TLfDI

Thüringer Landesbeauftragter
für den **Datenschutz** und die **Informationsfreiheit**

2018

1. Tätigkeitsbericht zum Datenschutz nach der DS-GVO

1. Tätigkeitsbericht zum Datenschutz nach der DS-GVO | 2018

TLfDI

1. Tätigkeitsbericht zum Datenschutz nach der DS-GVO

des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

Berichtszeitraum: 1. Januar 2018 bis 31. Dezember 2018
Zitiervorschlag: 1. TB DS-GVO LfDI Thüringen

Der 1. Tätigkeitsbericht DS-GVO steht im Internet unter der Adresse www.tlfdi.de zum Abruf bereit.

Erfurt, im Juni 2019

Dr. Lutz Hasse

Thüringer Landesbeauftragter für den Datenschutz
und die Informationsfreiheit

Inhaltsverzeichnis

Datenschutz

Vorwort

Dr. Lutz Hasse

Das aktuelle Berichtsjahr hat die Behörde des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ganz schon durcheinandergewirbelt. Das Wirksamwerden der Europäischen Datenschutz-Grundverordnung stellte alles andere in den Schatten. Von einem Tag auf den anderen galt es, neues Recht anzuwenden. Das war sowohl für die Unternehmen und Behörden in Thüringen eine Herausforderung als natürlich auch für meine Mitarbeiter und Mitarbeiterinnen, die zahllose Anfragen zu bearbeiten hatten. Der TLfDI sah sich in der Anlaufphase in erster Linie als Beratungspartner der verantwortlichen Stellen. Mit vielen Akteuren wurden gemeinsam Lösungen erarbeitet, den Übergang zu meistern. Ich finde, der Start ist ganz gut gelungen, erste Schritte sind gemacht. Jetzt gilt es, die begonnen Prozesse zu perfektionieren und weiter in die Tiefe zu gehen. Dafür wird auch die vom TLfDI durchgeführte Umfrage bei den Unternehmen und Kommunen eine gute Grundlage liefern.
In diesem Jahr ist das öffentliche Bewusstsein für die Gefahren der Verletzung des Schutzes von personenbezogenen Daten und der Missachtung von Sicherheitsvorkehrungen im Internet gestiegen. Der Guardian und die New York Times deckten auf, wie die Firma Cambridge Analytica die Profile von bis zu 87 Millionen Facebook-Nutzern ohne deren Zustimmung auswertete. Außerdem wurde im

September bekannt, dass die Daten von bis zu 50 Millionen Facebook-Nutzern gestohlen worden waren. Nicht nur Chancen, sondern auch eine große Gefahr birgt die Weiterentwicklung der Künstlichen Intelligenz (KI). Die Beobachtung dieser Prozesse wird auch künftig einen Schwerpunkt in der Tätigkeit des TLfDI darstellen. Genauso wichtig ist es, die Personen, um deren Daten es geht, fitter in Sachen Selbstdatenschutz zu machen. Gelingt dies weiterhin, ebenso wie die datenschutzkonforme Ausrichtung der Unternehmen, kann eine vorbildliche Umsetzung datenschutzrechtlicher Anforderungen in Unternehmen und bei Produkten ein echter Wettbewerbsvorteil für Thüringen werden.
Nach diesem kurzen Ausblick in die Zukunft erwartet Sie jetzt ein hoffentlich spannender Bericht über die Aktivitäten des letzten Jahres. Viel Spaß und nützliche Erkenntnisse beim Lesen wünscht Ihnen

Ihr

Dr. Lutz Hasse
Thüringer Landesbeauftragter für den Datenschutz
und die Informationsfreiheit

1. Schwerpunkte im Berichtszeitraum

© Minerva Studio - Eye close-up - fotolia.com

1.1 Schwerpunkte im Berichtszeitraum

Ohne Frage stellte die Rechtsänderung durch das Wirksamwerden der DS-GVO den TLfDI im Berichtszeitraum vor große Herausforderungen. Daneben bildete das Thema Medienkompetenz und der Datenschutz in Schulen und Bildungseinrichtungen einen weiteren Schwerpunkt.

Der aktuelle Berichtszeitraum war ganz maßgeblich davon geprägt, dass am 25. Mai 2018 die Datenschutz-Grundverordnung (DS-GVO) wirksam wurde. Zwar gab es zuvor einen zweijährigen Übergangszeitraum (siehe Beitrag 2.1), gleichwohl konzentrierten sich die mit der Umsetzung der neuen Rechtslage verbundenen Probleme auf das Jahr 2018. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) nahm an zahlreichen länderübergreifenden Sitzungen der Aufsichtsbehörden für den Datenschutz teil. Die Sitzungen dienten dazu, die bestehenden Orientierungshilfen an das neue Recht anzupassen und vor allem auch, neue Festlegungen zur Rechtslage zu treffen. Als Beispiel sind hier die Kurzpapiere der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) zu nennen, in denen bestimmte Aspekte der

neuen Rechtslage in kurzer und verständlicher Form dargelegt werden.
Daneben führte der TLfDI in diesem Jahr so viele Schulungen wie noch nie durch (siehe Beitrag 9.1), beantwortete zahlreiche Beratungsanfragen und erarbeitete neue Informationsmaterialien zu den verschiedenen Themenbereichen der DS-GVO.
Auch intern wurden die Mitarbeiter in der Anwendung des neuen Rechts geschult und die Verfahrensabläufe in der Behörde an die Vorgaben der DS-GVO angepasst. Nicht zuletzt war es wichtig, alle offenen Fälle, für die noch die alte Rechtslage galt, möglichst vor dem Wirksamwerden der DS-GVO abzuschließen.
Neben dieser Mammutaufgabe bestand ein weiterer Schwerpunkt der Tätigkeit des TLfDI darin, seine Funktion als Vorsitzender von zwei Arbeitskreisen der DSK auszufüllen. Thüringen hat den Vorsitz für den Arbeitskreis Schulen und Bildungseinrichtungen, der sich mit der datenschutzkonformen Ausgestaltung der Verwaltung in Schulen und Bildungseinrichtungen beschäftigt. Hier sind das digitale Lernen und die Anforderung an Cloud-Dienste sowie die Nutzung von mobilen Endgeräten wichtige Themen (siehe Beitrag 6.24). Der Arbeitskreis Datenschutz-/Medienkompetenz beschäftigt sich mit der Frage, wie den betroffenen Personen (vom Grundschul- bis zum Seniorenalter) ihre Rechte im Bereich des Datenschutzes nahegebracht werden können und wie ihnen eine kompetente, bewusste Mediennutzung möglich gemacht werden kann. Zu diesem Zweck ist der TLfDI auch Mitglied der Landeskooperation zur nachhaltigen Weiterentwicklung von Medienkompetenz. An dieser Kooperation sind neben dem TLfDI fünf Ministerien, das Lehrerfortbildungsinstitut und die Landesmedienanstalt beteiligt. In ihr werden Lösungsansätze für die Bereiche Schule/ Lehrerbildung, Erwachsene und Senioren sowie Jugendhilfe und Kindertagesstätten zur nachhaltigen Medienkompetenzentwicklung erarbeitet. Zum Zweck der besseren Verankerung von datenschutzrechtlichen Inhalten in der Lehrerausbildung und in den Lehrplänen der Schulen pflegt der TLfDI einen intensiven Kontakt zur Kultusministerkonferenz.

1.2 DS-GVO – ein Gedicht

Damals war's, vor langen Zeiten,
als es gab ein täglich Streiten
darum, wie er wohl ausseh'n muss,
europaweiter Datenschutz.

Denn zu beklagen damals war
ein Durcheinander sonderbar,
bei Antworten auf Fragen, schwere,
speziell zu der privaten Sphäre.

Europas Osten gab zum Besten
ein and'res Wissen als der Westen[1],
wenn es festzulegen galt,
die Richtung in dem Daten-Wald.

Die Norm, die Richtung festzulegen,
war von den Staaten auszulegen,
ungleich daher und eher schlecht,
war so das alte Daten-Recht.

Mit Richtlinie, der Euro-Norm,
lag so Europa nicht mehr vorn,
zu unterschiedlich je Region,
war deren Interpretation.

Einheitlich, so der Gedanke,
soll der Schutz der Daten sein,
kein europäisches Gezanke,
sondern verbindlich, klar und fein.

Viviane Reding, so der Name,
einer resoluten Dame,
man hört, sie will nicht länger warten,
mit der VO zum Schutz der Daten.

[1] Man hätte auch Norden/ Süden nennen können, was indes reimtechnisch schwierig gewesen wäre.

Unmittelbar soll sie nun gelten,
die Verordnung der EU,
verknüpfen alle Daten-Welten,
die Vorschrift hat das Zeug zum Coup.

Doch die Götter wollen Schweiß,
bevor hier winkt der große Preis,
und voller Mühen und auch Plagen,
ist der Weg zum großen Ziel,
und der Mut, es dann zu wagen,
verlangt von den Akteuren viel.

Von denen, die hier Lob verdienen,
heißt einer Albrecht – von den Grünen,
denn er konnt‘ es nicht erwarten,
endlich zu sein – im „Rausch der Daten“[2].

2018 dann, im Mai
da nimmt die Vorschrift ihren Lauf,
das Warten – es ist nun vorbei,
und Neues nimmt man gern in Kauf:

Die Portabilität der Daten,
das Recht auch auf Vergessensein,
Marktortprinzip – so gut geraten,
wie die Privatheit by Design.

Und keinen lässt so recht entspannen,
die Meldepflicht von Datenpannen,
zudem darf niemand sich vernetzen,
ohne die Folgen abzuschätzen,
und schon gar nicht wischt man weg,
die starke Bindung an den Zweck.

Praxisferner sind da schon,
die Pflichten zur Information,
und hoffentlich wird nicht zum Flop

[2] „Im Rausch der Daten“ ist ein sehr sehenswerter Film mit Jan Philipp Albrecht zur Entstehung der DS-GVO.

der legendäre One-Stop-Shop.

Verletzt man diese Normen nun,
muss man gründlich Buße tun,
zu zahlen sind bis zig Millionen,
denn Unrecht darf sich nicht mehr lohnen.

Hier lässt die Aufsicht Obacht walten,
ob die VO wird eingehalten –
und ganz vorbei kommt man doch nie
am Thüringer LfDI ;-)

2. Inkrafttreten der DS-GVO mit getroffenen Maßnahmen

© vege - Gesetze und Paragraphen - fotolia.com

2.1 Umsetzung der Datenschutz-Grundverordnung – Arbeit auch bei der Aufsichtsbehörde

Das Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO) stellt alle Verantwortlichen im Sinne des Gesetzes vor große Herausforderungen. Dies betraf den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) sogar doppelt, in seiner Rolle als Aufsichtsbehörde und auch als Verantwortlicher. Trotz dieser Doppelbelastung ist es der Aufsichtsbehörde gelungen, den Verantwortlichen zahlreiche Hilfestellungen zur Verfügung zu stellen.

Niemand kann eigentlich ernsthaft behaupten, die Datenschutz-Grundverordnung hätte ihn überraschend getroffen. Die Europäische Kommission legte am 25. Januar 2012 den ersten Vorschlag für eine „Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)“ (DS-GVO) vor. Danach hatte es pressewirksame und umfassende Debatten im Rahmen des europäischen Gesetzgebungsverfahrens gegeben. Es

fanden zahlreiche öffentliche Anhörungen im Europäischen Parlament statt, in denen viele Kritikpunkte geäußert worden waren. Daraus resultierend nahm das Europäische Parlament am 12. März 2014 die durch den Europa-Abgeordneten Jan Philipp Albrecht als Berichterstatter ausgearbeitete Verhandlungsposition mehrheitlich an. Im Juni 2015 einigten sich die EU-Justizminister auf einen Entwurf der EU-Datenschutz-Grundverordnung. Danach begann der sogenannte Trilog und es starteten die Abstimmungsverhandlungen zwischen Rat, Europäischem Parlament und Europäischer Kommission.
Im April 2016 beschloss der EU-Ministerrat die nun gültige und rechtskräftige Fassung; das EU-Parlament nahm die Regelungen am 14. April 2016 ebenfalls an. Die DS-GVO wurde am 4. Mai 2016 im Amtsblatt der Europäischen Union veröffentlicht. Nach Art. 99 Abs. 1 DS-GVO trat sie damit am 25. Mai 2016 in Kraft. Das Gesetz sieht allerdings in Art. 99 Abs. 2 eine zweijährige Übergangsfrist vor, weshalb die DS-GVO erst ab dem 25. Mai 2018 auch tatsächlich angewendet wurde.
Das Thema war damit seit 2012 in der öffentlichen Diskussion und spätestens mit dem Inkrafttreten am 25. Mai 2016 hätte sich jeder Verantwortliche an die Umsetzung der neuen Anforderungen machen müssen. Dafür hatte der europäische Gesetzgeber ganz bewusst einen Zeitraum von zwei Jahren vorgesehen. Was er nicht steuern konnte, war der menschliche Faktor. Eine Angelegenheit, die erst in zwei Jahren aktuell wird, erscheint angesichts anderer aktueller Probleme weit entfernt und neigt oft dazu vernachlässigt zu werden. Sie wird erst dann wieder angepackt, wenn die Frist fast verstrichen ist. Hinzu kommt, dass die Berichterstattung der Medien seit Ende 2017 nachdrücklich, unter Hinweis auf die drohenden Bußgelder von bis zu 20 Millionen Euro, auf die Umsetzungspflicht der DS-GVO zum 25. Mai 2018 hingewiesen hat.
All das stellte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) vor eine große Herausforderung. Zum einen musste er selbst als Verantwortlicher – denn auch beim TLfDI werden personenbezogene Daten verarbeitet – die erforderlichen Umsetzungs-Maßnahmen treffen. Zum anderen sah er sich mit einer wahren Flut von Beratungsanfragen konfrontiert, die der TLfDI trotz vier zusätzlicher Personalstellen in 2018 kaum bewältigen konnte. Dabei sollte die DS-GVO für die Verantwortlichen, die die bis dahin bestehenden gesetzlichen Anforderungen erfüllt hatten, keine umfassenden Neuerungen mit sich bringen. Allerdings mussten alle

Verfahren, bei denen personenbezogene Daten verarbeitet werden, im Hinblick auf den Anpassungsbedarf nach der DS-GVO überprüft werden. Dazu sollte zunächst der Ist-Zustand analysiert werden, um dann den entsprechenden Handlungsbedarf zu ermitteln. Folgende wichtige Neuerungen waren dabei zu beachten:
Es war zu prüfen, ob das neue Recht für alle Datenverarbeitungsprozesse eine Rechtsgrundlage bereitstellt. Sofern sich die Datenverarbeitung auf eine Einwilligung stützte, war zu prüfen, ob die gegenüber dem bisherigen Recht etwas konkreter formulierten Anforderungen des Art. 7 DS-GVO erfüllt sind. So darf beispielsweise die Erfüllung eines Vertrags nicht von einer Einwilligung in die Verarbeitung personenbezogener Daten abhängig gemacht werden, die für die Erfüllung des Vertrages nicht erforderlich ist (Kopplungsverbot). Dies ist beispielsweise der Fall, wenn bei einer Bestellung in einem Onlineshop die Bestellung davon abhängig gemacht wird, dass der Kunde seine Einwilligung in die Nutzung seiner Daten zu Werbezwecken erteilen muss.
Betroffenen Personen stehen nach der DS-GVO umfangreichere Rechte zu, die der Verantwortliche zu beachten hat. Dies betrifft vor allem die Informationspflichten nach Art. 13 und Art. 14 DS-GVO, aber auch das Auskunftsrecht nach Art. 15 DS-GVO und das neue Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO.
Die DS-GVO enthält spezifische Rahmenbedingungen für die Art und Weise, wie die Anforderungen der DS-GVO schon bei der Prozessgestaltung und bei den Voreinstellungen umzusetzen sind (Art. 25 DS-GVO: Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, Data Protection by design und Data Protection by default). Sie verpflichtet in Art. 5 Abs. 2 DS-GVO den Verantwortlichen zum Nachweis, dass personenbezogene Daten rechtmäßig verarbeitet werden (Rechenschaftspflicht). Deswegen sieht die DS-GVO an unterschiedlichen Stellen Dokumentationspflichten vor (z. B. für das Verzeichnis über Verarbeitungstätigkeiten in Art. 30 DS-GVO, für die Dokumentation von Datenschutzvorfällen in Art. 33 Abs. 5 DS-GVO oder für die Dokumentation von Weisungen im Rahmen der Auftragsverarbeitung in Art. 28 Abs. 3 Buchstabe a) DS-GVO). Nach Art. 37 Abs. 7 DS-GVO muss der Verantwortliche oder der Auftragsverarbeiter die Kontaktdaten des Datenschutzbeauftragten der zuständigen Aufsichtsbehörde melden. Ebenso ist der Aufsichtsbehörde die Verletzung des Schutzes personenbezogener Daten zu melden (Art. 33 Abs. 1 DS-GVO). Zu all diesen Pflichten müssen beim

Verantwortlichen die erforderlichen Prozesse implementiert werden. Auch eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO, die nun die Vorabkontrolle ersetzt, erfordert eine umfangreiche Dokumentation.

Bei der Umsetzung der notwendigen Maßnahmen wollten die Aufsichtsbehörden des Bundes und der Länder die Verantwortlichen nicht im Regen stehen lassen. Sie haben sich daher nach dem Inkrafttreten der DS-GVO in diversen Arbeitskreisen und zu zahlreichen Terminen getroffen, um den Verantwortlichen konkrete Hilfestellungen bei der Umsetzung anzubieten. Dabei sind die Kurzpapiere der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder entstanden, die auch auf der Internetseite des TLfDI unter https://www.tlfdi.de/tlfdi/europa/europaeischedsgvo/index.aspx veröffentlicht wurden. Sie dienten als erste Orientierung und Vorbereitung zur bevorstehenden, praktischen Anwendung der DS-GVO, insbesondere für den nicht-öffentlichen Bereich (Unternehmen). Konkrete Hinweise erwiesen sich deswegen als schwierig, weil die DS-GVO auch für die Aufsichtsbehörden ein neues Recht darstellte. Zudem gab es zu diesem Zeitpunkt noch keine Erfahrungswerte in der Umsetzung und auch keine Richtlinien (guidelines) der Europäischen Union; auch eine Rechtsprechung existiert zu den relativ unbestimmten Rechtsbegriffen noch nicht. Daher waren ein intensiver Dialog und ein tiefes Eintauchen in die Rechtsmaterie erforderlich.

Auch auf Ebene des Landes erarbeitete der TLfDI Informationsmaterialien und zahlreiche Muster wie z. B. für die Meldung von Datenpannen oder zur Meldung des Datenschutzbeauftragten. Der Verunsicherung bei den Verantwortlichen versuchte der TLfDI in zahlreichen Schulungen und Informationsveranstaltungen entgegenzuwirken (siehe Beiträge 5.8 und 9.1).

Zusammenfassend lässt sich feststellen, dass der Start in die Datenverarbeitung nach der DS-GVO in Thüringen zwar etwas holperig war, ein größeres Debakel aber ausblieb. Dies nicht zuletzt deswegen, weil der TLfDI den Verantwortlichen mit allen in seiner Macht stehenden Mitteln beratend zu Seite gestanden hat.

2.2 Zahlen, Daten, Fakten: Ausbau der statistischen Erfassung beim TLfDI

Mit dem Wirksamwerden der DS-GVO sind die Posteingänge beim TLfDI massiv gestiegen. Der TLfDI wird künftig vermehrt mit statistischen Auswertungen arbeiten, nachdem ein entsprechendes Verfahren implementiert ist.

Die Datenschutz-Grundverordnung (DS-GVO) regelt die Aufgaben und Befugnisse der Aufsichtsbehörde in Art. 57 und 58 umfassend. Danach hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) neue Aufgaben und auch weitergehende Befugnisse als bisher (siehe 5.27). Aufgrund dessen und auch wegen der umfangreichen Medienberichterstattung zur DS-GVO (siehe 2.1) sind die Posteingänge beim TLfDI erheblich gestiegen. Dies mag die folgende Grafik verdeutlichen:

Es gab im Berichtszeitraum einige Presseanfragen zu statistischen Werten. Die Aufsichtsbehörde ist gesetzlich nicht verpflichtet, Statistiken zu führen. Auch der anzufertigende Tätigkeitsbericht *kann* nach Art. 59 DS-GVO z. B. eine Liste enthalten, die die Arten von gemeldeten Verstößen und getroffenen Maßnahmen dokumentiert. Die

Nachfrage solcher statistischen Veröffentlichungen ist immer größer geworden, so dass der Bereich der Statistik beim TLfDI künftig ausgeweitet werden soll. Für den Berichtszeitraum des vorliegenden Tätigkeitsberichts liegen folgende Zahlen vor:

Im Jahr 2018 gab es 22.188 Posteingänge. Seit dem Wirksamwerden der DS-GVO gab es 353 an den TLfDI gerichtete Beschwerden. Dabei muss betont werden, dass diese Zahl nur die Beschwerden im Sinne des Gesetzes erfasst, die die Voraussetzungen des Art. 77 DS-GVO erfüllen. Es handelt sich dabei um schriftlich eingegangene Beschwerden, die eine natürliche Person eingereicht hat, die von der in Rede stehenden Datenverarbeitung persönlich betroffen ist. Darüber hinaus gab es, wie auch die Zahl der Posteingänge zeigt, zahlreiche sonstige Eingaben, die nicht den Tatbestand der Beschwerde nach Art. 77 DS-GVO erfüllen. Sie wurden bislang noch nicht gesondert statistisch erfasst. Besonders umfangreich war die Zahl der an den TLfDI gerichteten Beratungsanfragen, die nicht gesondert gezählt wurden.
Im Berichtszeitraum gingen 78 Meldungen nach Art. 33 DS-GVO zu Datenschutzverletzungen ein (siehe 5.23 zu weiteren Einzelheiten).

Konkrete Zahlenangaben zu Maßnahmen nach Art. 58 DS-GVO, die im Berichtszeitraum getroffenen wurden, können noch nicht gemacht werden. Die Zahl der getroffenen Maßnahmen ist noch relativ überschaubar, weil der TLfDI nach dem Wirksamwerden der DS-GVO den Schwerpunkt seiner Tätigkeit zunächst auf die Sensibilisierung der Öffentlichkeit und die Beratung im Einzelfall gerichtet hat.
Der TLfDI erarbeitet derzeit ein Konzept zur besseren statistischen Erfassung seiner vielfältigen Aufgaben auch mit Blick auf die internationalen Verfahren, die auf EU-Ebene durchgeführt werden.

3. Die „Entstehung“ des neuen ThürDSG

© andyller – Datenschutz (Anwalt, Datenschutzbeauftragter)

3.1 Das neue Thüringer Datenschutzgesetz – kein „großer Wurf“ trotz vielfacher Kritik

Was lange währt, wird nicht immer gut: Obwohl die Thüringer Landesregierung von Juni 2017 bis Januar 2018 an ihrem Gesetzentwurf zur Anpassung des Thüringer Landesrechts an die EU Datenschutz-Grundverordnung und an die EU-Richtlinie für Inneres und Justiz (kurz: JI-Richtlinie) gearbeitet hatte, erreichte den Thüringer Landtag ein stark verbesserungsbedürftiger Gesetzentwurf. Leider wurden dann auch im parlamentarischen Beratungsverfahren längst nicht alle Verbesserungsvorschläge des TLfDI berücksichtigt. Das neue Thüringer Datenschutzgesetz, das am 15. Juni 2018 in Kraft getreten ist, ist daher immer noch verbesserungswürdig.

I. Frühe Einbindung des TLfDI

Bereits im Vorbereitungsverfahren, der sogenannten Ressortabstimmung der Ministerien, zur Anpassung des Thüringer Landesrechts an die am 25. Mai 2018 zur Anwendung gelangte EU Datenschutz-Grundverordnung und die EU-Richtlinie Inneres und Justiz (kurz: JI-Richtlinie), beteiligte das Thüringer Ministerium für Inneres und

Kommunales (TMIK) den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) an dem Entstehungsprozess des neuen Gesetzentwurfs (siehe dazu auch den Beitrag aus dem 12. Tätigkeitsbericht zum Datenschutz, Nr. 3.6, Seite 59 ff.).

II. Chance für Verbesserungen

Die Verbesserungsvorschläge des TLfDI nahm das TMIK nicht an, was in seinem Gesetzentwurf zur 2. Ressortabstimmung im Herbst 2017 ersichtlich wird und zu dem auch der TLfDI im Oktober 2017 umfangreich Stellung bezogen hatte. Hierbei kritisierte der TLfDI erneut die von ihm geforderten, aber letztlich nicht umgesetzten Vereinfachungen des Rechts für öffentliche Stellen, die am Wettbewerb teilnehmen, sowie die weiterhin fehlende unbefristete Bestellung von behördlichen Datenschutzbeauftragten. Zudem wehrte sich der TLfDI gegen das vorgesehene Verbot der Ersatzvornahme für den TLfDI. Der Begriff der Ersatzvornahme bedeutet, dass die Vornahme einer geschuldeten Handlung anstelle des Handlungspflichtigen von der Behörde durchgeführt wird; dabei anfallende Kosten trägt jedoch der Handlungspflichtige. In diesem Zusammenhang wies der TLfDI darauf hin, dass es gerade in Fällen von Datenschutzverstößen, in denen ein sehr hohes Risiko für die Rechte und Freiheiten der betroffenen Personen besteht oder im Falle einer Verweigerungshaltung öffentlicher Stellen Anordnungen des TLfDI zu befolgen, dem TLfDI möglich sein müsste, eine solche Ersatzvornahme selbst vorzunehmen oder vornehmen zu lassen.

Aber nicht nur die Anpassung des Thüringer Datenschutzgesetzes an die Datenschutz-Grundverordnung, auch dessen Anpassung an die JI-Richtlinie wurde vom TLfDI kritisch gesehen. Während die JI-Richtlinie in Art. 47 Abs. 2 regelt, dass die Mitgliedstaaten ihren Datenschutz-Aufsichtsbehörden für den Fall von Datenschutzverstößen wirksame Abhilfebefugnisse einräumen (wie z. B. Anordnungen oder Verbote zu verhängen), sah der Gesetzentwurf der Thüringer Landesregierung für den TLfDI lediglich vor, die bisherige Beanstandungsmöglichkeit von Datenschutzverstößen beizubehalten. Das Fazit des TLfDI lautete daher für diese Neuregelung: “nicht EU-rechtskonform“.

III. Stellungnahme

Kurz vor der endgültigen Verabschiedung des Gesetzentwurfs für ein neues Thüringer Datenschutzrecht erhielt der TLfDI im Rahmen der

sogenannten Kabinettanhörung die Möglichkeit, zum dritten Mal seine Kritik und Einwendungen zu allen datenschutzrechtlichen Änderungen im Gesetzentwurf für ein Thüringer Datenschutz-, Anpassungs- und Umsetzungsgesetz EU vorzubringen. Wie es der Titel dieses Artikelgesetzentwurfs bereits signalisierte, war nun nicht nur das neue Thüringer Datenschutzgesetz Bestandteil des Gesetzentwurfs, sondern in anderen Artikeln der Novelle (daher der Begriff „Artikelgesetz“) sah die Landeregierung z. B. die Änderung des Polizeiaufgabengesetzes, des Thüringer Informationsfreiheitsgesetzes oder die Änderung des Thüringer Pressegesetzes vor. Die Aufgabe des TLfDI war dabei zu prüfen, ob alle vorgesehenen Gesetzesänderungen auch die Vorgaben der Datenschutz-Grundverordnung und der JI-Richtlinie dahingehend erfüllen. Quintessenz vorab: Die Anpassung des Thüringer Landesrechts an die europäische Rechtslage war immer noch stark verbesserungsbedürftig. Ein wesentlicher Kritikpunkt des TLfDI war nach wie vor, dass der Vollzug und die schnelle Umsetzung der Abhilfebefugnisse bei Datenschutzverstößen, die in Art. 58 Abs. 2 Datenschutz-Grundverordnung aufgelistet sind, nicht im neuen Thüringer Datenschutzgesetz geregelt war.
Der TLfDI empfahl daher dringend die Überarbeitung der entsprechenden Regelungen mit dem Ziel, dass die Vorschriften des Thüringer Verwaltungszustellungs- und Vollstreckungsgesetzes (ThürVwZVG), insbesondere die der Ersatzvornahme, auch für die Ausübung der Befugnisse des TLfDI Anwendung finden sollten.
Weiterhin regte der TLfDI aufgrund seiner bisherigen Praxiserfahrungen an, dass künftig im neuen Thüringer Datenschutzgesetz der datenschutzrechtliche Status von Landtagsabgeordneten im Rahmen ihrer parlamentarischen Mandatsausübung klar geregelt ist. Der TLfDI sprach sich dabei für eine Regelung aus, bei der Landtagsabgeordnete mit einer öffentlichen Stelle gleichgesetzt werden würden und deren parlamentarische Tätigkeit somit nicht unter den Anwendungsbereich des Bundesdatenschutzgesetzes (BDSG) fällt. Darüber hinaus sollte die vom TLfDI vorgeschlagene Regelung unmissverständlich zum Ausdruck bringen, dass der Ältestenrat des Thüringer Landtags, und nicht der TLfDI, die zuständige Aufsichtsstelle für die Beachtung und Einhaltung der datenschutzrechtlichen Regelungen ist.
Aber nicht nur zu den Neuregelungen des Thüringer Datenschutzgesetzes, auch zu den Änderungen im Polizeiaufgabengesetz (PAG) merkte der TLfDI Änderungsbedarf an. So kritisierte er beispiels-

weise, dass die Aufhebung des datenschutzrechtlichen Auskunftsanspruchs im PAG nun eine Kette von Verweisen zum neuen Thüringer Datenschutzgesetz nach sich zieht und demnach „nicht anwenderfreundlich“ sei, weil wissbegierige Bürger nun in zwei Gesetzen, und nicht wie bisher nur in einem Gesetz nachschauen müssen.
Weiterhin empfahl der TLfDI, auch für den verdeckten Einsatz von technischen Mitteln zur Anfertigung von Bildaufzeichnungen gemäß § 34 Abs. 4 Satz 1 PAG eine richterliche Anordnung zu verlangen, sodass die Polizei künftig nur dann verdeckt Videos zur Gefahrenabwehr erstellen kann, wenn zuvor eine Richterin oder ein Richter dies angeordnet hat. Das Zwischenfazit nach der dritten Stellungnahme des TLfDI gegenüber der Landesregierung fiel ernüchternd aus: Die meisten Anregungen und Empfehlungen des TLfDI wurden vom zuständigen Ministerium für Inneres und Kommunales nicht in den Gesetzentwurf übernommen.

IV. Verbesserungsversuch, nun beim Landtag

Nachdem die Thüringer Landesregierung im 2. Kabinettdurchgang Anfang Januar 2018 den Gesetzentwurf „Thüringer Gesetz zur Anpassung des Allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Thüringer Datenschutz-Anpassungs- und -Umsetzungsgesetz EU“ beschlossen hatte, leitete sie diesen zur parlamentarischen Beratung an den Thüringer Landtag weiter. Der Landtag überwies den genannten Gesetzentwurf in der Drucksache 6/4943 nach erster Beratung in den Ausschuss für Inneres und Kommunales zur weiteren Beratung. Im Rahmen des schriftlichen Anhörungsverfahrens trug der TLfDI vor den Osterfeiertagen 2018 zum vierten Mal seine datenschutzrechtlichen Bedenken gegen das neue Thüringer Datenschutzgesetz vor. Dabei ging der TLfDI insbesondere auf folgende Aspekte ein:

a. Ausdrücklich wies der TLfDI darauf hin, dass die von der Landesregierung noch einmal geänderte Regelung des § 7 Abs. 1 Thüringer Datenschutzgesetz-Entwurfs (ThürDSG-Entwurfs) EU-rechtswidrig sei, weil sie zum einen in Satz 2 eine unnötige „Pirouette“ für den TLfDI vorsah: Der TLfDI sollte, wenn er einen Verstoß bei der Verarbeitung personenbezogener Daten festgestellt hatte, dies dem Verantwortlichen mitteilen und darüber hinaus die zuständige oberste Landesbehörde und die Aufsichtsbehörde darüber zu unterrichten. Insbesondere die Verständigung

der beiden letztgenannten Behörden war und ist in der Datenschutz-Grundverordnung aber gar nicht vorgesehen. Zum anderen fehlte dem TLfDI nach eigener Auffassung in § 7 Abs. 4 ThürDSG-Entwurf nach wie vor eine effektive Befugnis gegenüber öffentlichen Stellen, zur vorübergehenden Beschränkung von Verarbeitungen personenbezogener Daten, Zwangsmittel gemäß des ThürVwZVG, insbesondere eine Ersatzvornahme, geltend zu machen.

b. Der TLfDI monierte ferner, dass es gemäß Art. 58 Abs. 5 Datenschutz-Grundverordnung den Datenschutzaufsichtsbehörden auch gestattet werden müsse, gegebenenfalls ein gerichtliches Verfahren gegen Datenschutzverstöße aus der Datenschutz-Grundverordnung zu betreiben – ein solche Regelung sei aber derzeit nicht im ThürDSG-Entwurf enthalten. Anders und gut, so der TLfDI, sei dies zum Beispiel in § 19 Abs. 5 Satz 2 des neuen Hessischen Datenschutzgesetzes geregelt worden.

c. Ebenfalls zum vierten Mal wies der TLfDI auf eine notwendige Entfristung der Amtszeit des behördlichen Datenschutzbeauftragten hin.

d. Erneut kritisierte der TLfDI deutlich die geplante Regelung in § 6 Abs. 2 ThürDSG-Entwurf, wonach er bei Datenschutzverstößen, die unter den Anwendungsbereich der JI-Richtlinie fallen, lediglich ein Beanstandungsrecht und keine Befugnis erhalten sollte Anordnungen oder Verbote zu erlassen. Der TLfDI sah diese Regelung im Gesetzentwurf der Landesregierung als „nicht europarechtskonform“ an.

e. Verbesserungsbedarf erkannte der TLfDI auch bei der geplanten Neufassung von § 11a des Thüringer Pressegesetzes (TPG). Der Gesetzentwurf der Landesregierung hatte von der Möglichkeit, gemäß Art. 85 Datenschutz-Grundverordnung, von diesem Regelungsinstrument abzuweichen und das sogenannte Presseprivileg unverändert zu belassen nicht in ausreichendem Umfang Gebrauch gemacht. Für den TLfDI war es aber wichtig, dafür Sorge zu tragen, dass die Presse auch weiterhin nicht unter die Datenschutzaufsicht des TLfDI fällt, sondern es bei einer Selbstregulierung der Presse auf Grundlage von Pressekodex und Beschwerdeordnung des Deutschen Presserats bleiben sollte, das sogenannte Presseprivileg). Dementsprechend unterbreitete der TLfDI einen entsprechenden Formulierungsvorschlag zur Änderung des § 11a TPG.

f. Schließlich schlug der TLfDI vor, § 2 Abs. 3 des Thüringer Sicherheitsüberprüfungsgesetzes so zu ergänzen, dass sich auch die Person des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit zur Ausübung seines Amtes keiner Sicherheitsüberprüfung nach dem Thüringer Sicherheitsüberprüfungsgesetz unterziehen sollte. Als Begründung für diese Änderung führte der TLfDI an, dass die Person des Landesbeauftragten in Anwendung von Art. 51 Abs. 1 Datenschutz-Grundverordnung in der Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen sei.

Der Innen- und Kommunalausschuss des Thüringer Landtags und letztlich die Landtagsabgeordneten sind den Vorschlägen des TLfDI letzten Endes nur bedingt gefolgt: Während die vom TLfDI vorgeschlagenen Änderungen unter b., c., e. und f. berücksichtigt wurden, schafften es die unter a. und d. genannten Änderungsvorschläge des TLfDI nicht, in der Beschlussempfehlung des Innen- und Kommunalausschusses (Drucksache 6/5722) berücksichtigt zu werden. Ebenso wurden auch weitere datenschutzrechtliche Vorschläge des TLfDI zur Änderung der Thüringer Kommunalordnung, zur Änderung des Thüringer Kommunalwahlgesetzes und nicht zuletzt zur Änderung des Polizeiaufgabengesetzes nicht von den Fraktionen des Thüringer Landtags aufgegriffen.

Deshalb gilt hier eine alte Regel aus dem Fußball entsprechend: Nach dem Gesetzentwurf ist vor dem Gesetzentwurf….

4. Datenschutz und Informationsfreiheit – zwei Seiten einer Medaille

© Marco2811 - Datenschutz

Zwei Themen, eine Person: Wie der Name schon sagt, ist der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) neben dem Datenschutz auch für den Bereich der Informationsfreiheit zuständig. Diese Personalunion hat sich bundesweit bewährt. Datenschutz und Informationsfreiheit sind zwei Seiten einer Medaille, die zusammen betrachtet und beurteilt werden müssen.

Der Thüringer Landesbeauftragte für den Datenschutz übt bereits seit Ende des Jahres 2012 zugleich auch das Amt des Landesbeauftragten für die Informationsfreiheit aus. Diese Personalunion hat sich bewährt. Das Argument der wenigen Kritiker, dass sich einerseits der Schutz der Daten und andererseits die Preisgabe von Daten zugunsten der Informationsfreiheit konträr gegenüberstünden, kann der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wie auch seine Beauftragten-KollegInnen in den anderen Bundesländern nicht bestätigen. Vielmehr handelt es sich bei der Informationsfreiheit und dem Datenschutz um zwei Seiten einer Medaille, die gemeinsam betrachtet und bewertet werden müssen und ge-

rade deshalb von ein und derselben Institution wahrgenommen werden sollten. Denn der Anspruch auf den Zugang zu Informationen endet dort, wo der Schutz personenbezogener Daten beginnt – wer soll das besser beurteilen können als der Landesdatenschutzbeauftragte? Darüber hinaus ergibt sich auch aus der Datenschutz-Grundverordnung (DS-GVO) selbst, dass die Aufgabengebiete Datenschutz und Informationsfreiheit vom TLfDI weiterhin wahrgenommen werden können und dürfen:

- Aus Art. 57 DS-GVO, der die Aufgaben für die Aufsichtsbehörden im Datenschutz regelt, ergibt sich kein Ausschlussgrund, der einer Übertragung weiterer Befugnisse entgegensteht.
- Zu keinem anderen Ergebnis gelangt man, wenn man Art. 58 Abs. 6 DS-GVO (Befugnisse der Aufsichtsbehörden) zu Grunde legt, da diese Regelung nur gewährleisten will, dass die Befugnisse der Aufsichtsbehörden zur Zusammenarbeit und Kohärenz mit den anderen Aufsichtsbehörden nicht durch die Ausübung zusätzlicher Befugnisse beeinträchtigt wird. Durch die weitere Wahrnehmung der Aufgaben des TLfDI im Bereich der Informationsfreiheit sind diese Befugnisse aus Art. 58 DS-GVO, wie z. B. die Durchführung von Datenschutzüberprüfungen gemäß Art. 58 Abs. 1 Buchstabe b) DS-GVO oder die Verwarnungsmöglichkeit der Aufsichtsbehörde gemäß Art. 58 Abs. 2 Buchstabe b) DS-GVO nicht beeinträchtigt.

In der bisherigen Praxis konnte der TLfDI nicht feststellen, dass es bei seiner Arbeit zu Konflikten zwischen dem Datenschutz und der Informationsfreiheit gekommen ist. Gemäß § 12 des Thüringer Informationsfreiheitsgesetzes (ThürIFG) kann sich jeder, der sich in seinem Recht auf Informationszugang verletzt sieht, an den Landesbeauftragten für die Informationsfreiheit wenden. Als Schlichtungsstelle kann der TLfDI darauf hinwirken, dass ein Informationszugang durch die informationspflichtigen Stellen gewährt wird und entgegengesetzte Interessen in einen Ausgleich gebracht werden. Stellt der TLfDI Verstöße gegen das Thüringer Informationsfreiheitsgesetz fest, kann er nach § 12 Abs. 3 ThürIFG deren Behebung in angemessener Frist fordern und sie gegebenenfalls beanstanden. Jedoch bestehen keine Weisungs-, Abänderungs- oder Aufhebungsbefugnisse. Dazu muss der Antragssteller selbstständig den Rechtsweg beschreiten.

Seit dem Wirksamwerden der DS-GVO steht der Datenschutz natürlich wesentlich größer im Vordergrund als die Informationsfreiheit.

Deshalb sind auch in diesem Bereich wesentlich mehr Eingaben zu verzeichnen als im Bereich der Informationsfreiheit.
Einen Aufwind könnte Thüringen durch ein Thüringer Transparenzgesetz erfahren, das sich derzeit im Gesetzgebungsverfahren befindet. Auch nach diesem Gesetzentwurf der Landesregierung soll der Landesdatenschutzbeauftragte weiterhin in Personalunion die Aufgaben des Informationsfreiheitsbeauftragten wahrnehmen. Damit bringt auch die Thüringer Landesregierung grundsätzlich zum Ausdruck, dass sie an der doppelten Aufgabenwahrnehmung durch den TLfDI festhält.

5. Themengebiete

© Spencer- 3D Man Office - fotolia.com

Aufgrund der neuen Rechtslage ist es nicht mehr so leicht, zwischen dem öffentlichen und dem nicht-öffentlichen Bereich eine scharfe Trennlinie zu ziehen. Viele Bestimmungen gelten für beide Bereiche, die Unterschiede sind nicht mehr so groß wie nach dem alten Recht. Deswegen und auch, weil den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum sehr viele Fragen grundsätzlicher Art erreichten, ist dieser Tätigkeitsbericht anders als bisher in die Bereiche „Themengebiete“ und „Fälle“ unterteilt. Letztere beruhen auf konkreten, vom TLfDI bearbeiteten Fällen. Die Beiträge unter dieser Rubrik enthalten eher allgemeine Abhandlungen zu bestimmten Rechtsfragen oder Themengebieten. Dabei ist dieser Bereich so aufgebaut, dass zunächst die Beiträge aufgeführt sind, die eindeutig dem öffentlichen Bereich zuzuordnen sind. Es folgen für beide Bereiche geltende Ausführungen und abschließend finden sich Beiträge ausschließlich zum nicht-öffentlichen Bereich.

5.1 Die DS-GVO und die parlamentarische Tätigkeit von Landtagsabgeordneten: auch datenschutzrechtlich „zwei Paar Schuhe“

In den vergangenen vier Jahren musste sich der Thüringer Landesbeauftragte immer wieder mit der Frage beschäftigen, ob Abgeordnete des Thüringer Landtags entweder als öffentliche Stelle unter den Anwendungsbereich des Thüringer Datenschutzgesetzes oder als nicht-öffentliche Stelle unter den Anwendungsbereich des Bundesdatenschutzgesetzes fallen. Im Rahmen der Anpassung des Thüringer Datenschutzrechtes an die Vorgaben der Datenschutz-Grundverordnung (DS-GVO) war es deshalb aus der Sicht des TLfDI höchste Zeit, diese datenschutzrechtliche Streitfrage abschließend zu klären. Die bisher gefundene Lösung überzeugt jedoch nur teilweise, auch weil eine abschließende Regelung noch gar nicht existiert.

Unterfällt die parlamentarische Tätigkeit von Abgeordneten des Thüringer Landtags dem Anwendungsbereich des Thüringer Datenschutzgesetzes (ThürDSG) oder dem des Bundesdatenschutzgesetzes (BDSG)? Diese spannende Streitfrage hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) in den vergangenen vier Jahren mehrfach bei Datenschutz-Beschwerden von Bürgern über das parlamentarische Handeln von Abgeordneten des Thüringer Landtags zu entscheiden. Als parlamentarisches Handeln stufte der TLfDI dabei Handlungen von Landtagsabgeordneten ein, die in Ausübung ihres Mandats in der Öffentlichkeit, gegenüber der Presse oder in sozialen Netzwerken unternommen wurden. Als Beispiel sei hier der Twitter-Eintrag eines Landtagsabgeordneten genannt, der zwei Bilder von Unterschriftsbögen gegen die Gemeindegebietsreform der Thüringer Landesregierung postete, auf denen sowohl der Name als auch die Adresse der Unterzeichner zu sehen gewesen ist.
Der TLfDI stieß bei der Frage, welche Rechtsgrundlage für die datenschutzrechtliche Bewertung von parlamentarischen Tätigkeiten der Landtagsabgeordneten anzuwenden ist, auf zwei unterschiedliche Auffassungen in der Fachliteratur.
Eine Literaturmeinung vertrat die Rechtsauffassung, dass der „einzelne Abgeordnete […] grundsätzlich im Hinblick auf seine Fremdbestimmung und öffentlich-rechtlicher Aufgabenbindung freie Mandatswahrnehmung [...] als nicht-öffentliche Stelle nach § 2 Abs. 4 Satz 1

BDSG anzusehen“ sei (so Dammann in: Simitis, BDSG, § 2, Rdnr. 29). Demzufolge wäre also dieser Ansicht nach ein mögliches Fehlverhalten von Landtagsabgeordneten auf der Grundlage des BDSG zu sanktionieren.
Demgegenüber kam eine andere Literaturmeinung in der gleichen Rechtsfrage zu folgendem Ergebnis: „Andere öffentlich-rechtlich organisierte Einrichtungen sind der Bundespräsident, der Bundestag und der Bundesrat sowie die Fraktionen, parlamentarische Gruppen und Abgeordnete, wenn sie im Rahmen ihrer Mandatsausübung mit personenbezogenen Daten umgehen“ (Hanloser in: Wolf/Brink, Datenschutzrecht in Bund und Ländern, 1. Auflage 2013, § 2 BDSG, Rdnr. 50).
Auf Grundlage der letztgenannten Auffassung gelangte auch der TLfDI zu dem Ergebnis, dass die Abgeordneten des Thüringer Landtags als öffentliche Stellen im Sinne von § 2 Abs. 1 Thüringer Datenschutzgesetz alte Fassung (ThürDSG -alt-) auch unter den Anwendungsbereich von § 2 Abs. 5 Satz 3 und Satz 4 ThürDSG -alt- fielen. Allerdings hatte dies zur Folge, dass für die Kontrolle zur Einhaltung des Datenschutzes bei Abgeordneten im Rahmen ihrer parlamentarischen Tätigkeit nicht der TLfDI, sondern gemäß ThürDSG der Ältestenrat des Landtags zuständig war.
Dementsprechend empfahl der TLfDI im Frühjahr 2018, im Rahmen der Anpassung des Thüringer Datenschutzrechts an die Vorgaben der Datenschutz-Grundverordnung, die Aufnahme einer hinreichend klaren Regelung in das neue Thüringer Datenschutzgesetz. Aus dieser Regelung sollte hervorgehen, dass Landtagsabgeordnete bei der Ausübung ihrer parlamentarischen Tätigkeit der Datenschutz-Grundverordnung und dem ThürDSG unterfielen; für die Ausübung der datenschutzrechtlichen Kontrolle sollte aber nicht der TLfDI, sondern weiterhin der Ältestenrat zuständig sein.
Die Mehrheit im Thüringer Landtag hat sich jedoch dann für einen dritten Weg entschieden, wie sich aus Nr. I. 1. d) der Beschlussempfehlung in der Drucksache 6/5722 ergibt. Folgende Regelung in § 2 Abs. 6 Satz 3 und Satz 4 ThürDSG wurde mit Hilfe dieser Beschlussempfehlung in das neue Thüringer Datenschutzgesetz eingefügt und trat am 15. Juni 2018 in Kraft (siehe dazu das Gesetz- und Verordnungsblatt für den Freistaat Thüringen, Nr. 6 2018, Seite 229 ff.):

Die Verarbeitung personenbezogener Daten bei der Wahrnehmung parlamentarischer Aufgaben durch den Landtag sowie der parlamentarischen Tätigkeit der Abgeordneten einschließlich der Fraktionen unterliegt nicht den Bestimmungen dieses Gesetzes. Der Landtag erlässt insoweit eine seiner verfassungsrechtlichen Stellung entsprechende Datenschutzordnung.

Damit regelten die Abgeordneten des Thüringer Landtags, dass das Thüringer Datenschutzgesetz und damit auch die Datenschutz-Grundverordnung keine Anwendung auf ihre parlamentarische Tätigkeit finden. Ferner gilt die Datenschutz-Grundverordnung auch nicht unmittelbar für das Parlamentsrecht, weil dieses gemäß Art. 2 Abs. 2 Buchstabe a) Datenschutz-Grundverordnung gerade nicht in den Anwendungsbereich des Unionsrechts fällt.
Spannend bleibt somit abzuwarten, wie eine Ausgestaltung einer Datenschutzordnung für die parlamentarische Tätigkeit von Abgeordneten des Thüringer Landtags vorgenommen wird. Denn bis zum Redaktionsschluss dieses Tätigkeitsberichts hatte der TLfDI noch keine Kenntnis vom dem Inhalt einer solchen Datenschutzordnung.

5.2 Die Datenschutz-Grundverordnung und das neue Thüringer Pressegesetz: Wer kontrolliert wen?

Obwohl Art. 85 Abs. 1 und Abs. 2 Datenschutz-Grundverordnung Möglichkeiten vorsehen, das Recht auf Schutz personenbezogener Daten mit dem Recht auf Meinungsfreiheit, insbesondere im journalistischen Bereich, in Einklang zu bringen, gab es im Rahmen der Beratung über das Thüringer Gesetz zur Anpassung des Allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Thüringer Datenschutz-Anpassungs- und -Umsetzungsgesetz EU) sowohl auf Seiten der Landesregierung als auch bei Journalistenverbänden Zweifel, wie weit diese Ausnahmeregelungen gehen sollen. Der TLfDI hat sich mit guten Argumenten dafür ausgesprochen, dass das bisherige Recht der Presse zur Selbstregulierung durch Pressecodex und Beschwerdeordnung des deutschen Presserats unberührt bleiben sollte. Dies sah auch der Thüringer Landtag so und änderte § 11a Satz 6 und 7 des Thüringer Pressegesetzes entsprechend.

Anfang Januar 2018 übermittelte die Thüringer Landesregierung dem Thüringer Landtag den Gesetzentwurf „Thüringer Gesetz zur Anpassung des Allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680“ (Landtags-Drucksache 6/4943). Bestandteil dieses sogenannten Artikel-Gesetzes (siehe Beitrag 3.1 „Das neue Thüringer Datenschutzgesetz – kein ‚großer Wurf‘ trotz vierfacher Kritik“) war unter anderem in Art. 22 auch die Änderung von § 11a des Thüringer Pressegesetzes (TPG). In einer unübersichtlichen Regelung bestimmte Satz 4 des § 11a TPG-Entwurfs, welche Kapitel und Artikel aus der Datenschutz-Grundverordnung bei einer Datenverarbeitung unter anderem zu journalistischen Zwecken nicht oder nur eingeschränkt Anwendung finden sollten. In der Gesetzesbegründung zu § 11a TPG (siehe Landtags-Drucksache 6/4943, Seite 72 ff.) erläuterte die Landesregierung zwar ausführlich Herkunft und Entwicklung des sogenannten Medienprivilegs, beantwortete aber die Frage, wer die Fachaufsicht über datenschutzrechtliche Verstöße von Journalisten innehat, nur sehr knapp. Das Medienprivileg im Datenschutzrecht nahm bereits vor Inkrafttreten der Datenschutz-Grundverordnung die ausschließlich journalistische-redaktionelle und literarische Verarbeitung personenbezogener Daten weitestgehend von den Datenschutzbestimmungen aus.

Aufgrund dieser Unklarheit im Gesetzentwurf der Landesregierung waren sowohl Vertreter von Journalistenverbänden als auch von Medienunternehmen verunsichert und wandten sich Anfang 2018 ratsuchend an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Parallel dazu suchte auch die Thüringer Staatskanzlei in derselben Angelegenheit das Gespräch mit dem TLfDI, um eine Lösung zu dieser Streitfrage zu finden.

Der TLfDI stellte zunächst klar, dass auch für ihn die Pressefreiheit ein sehr hohes, schützenswertes Gut ist, dass nicht mithilfe der Datenschutz-Grundverordnung ausgehebelt werden darf (siehe TLfDI Pressemitteilung vom 16. März 2018: „Datenschutzgrundverordnung versus Pressefreiheit findet mit Dr. Hasse nicht statt“ https://www.tlfdi.de/mam/tlfdi/presse/180316_pressemitteilung_des_tlfdi.pdf).

Nach Prüfung der einschlägigen Regelungen und insbesondere des Gutachtens von Prof. Dr. Matthias Cornills vom August 2017 („Das datenschutzrechtliche Medienprivileg unter Behördenaufsicht? – Der unionsrechtliche Rahmen für die Anpassung der medienrechtlichen Bereichsausnahmen“: in § 9c, § 57 RStV-E und den Landespressegesetzen an die EU-Datenschutzgrundverordnung“) teilte der TLfDI seine Rechtsauffassung zur Frage der Datenschutz-Aufsicht im Journalismus dem Thüringer Landtag im Rahmen des parlamentarischen Anhörungsverfahrens zum Gesetzentwurf in der Drucksache 6/4943 mit. Der TLfDI wies zunächst darauf hin, dass gemäß Art. 85 Abs. 2 Datenschutz-Grundverordnung für den Bereich der journalistischen Datenverarbeitung die Vorgaben des vierten Kapitels der Datenschutz-Grundverordnung – Regelungen zu unabhängigen Aufsichtsbehörden – in ihrer Anwendung ausgeschlossen sind. Dieser Ausschluss müsste, so der TLfDI, dann aber auch für die Regelungen des achten Kapitels der Datenschutz-Grundverordnung gelten, in dem die Rechtsbehelfe, die Haftung und die Sanktionen enthalten sind. Darüber hinaus sei das achte Kapitel ohne die darin vorausgesetzten Aufgabenzuweisungen und Befugnisse der unabhängigen Aufsichtsbehörden aus dem sechsten Kapitel gar nicht vollzugsfähig. Zu dieser Ansicht gelangte auch Prof. Cornills auf Seite 59 seines Gutachtens. Aufgrund dieser Erkenntnis schlug der TLfDI eine Neufassung des Wortlauts von § 11a TPG vor, die dafür sorgen sollte, dass das bisherige datenschutzrechtliche Presseprivileg auch nach Anwendung der Datenschutz-Grundverordnung ab dem 25. Mai 2018 weiterhin Bestand haben sollte. Aufgrund dessen wäre auch eine Datenschutzkontrolle von Journalisten durch den TLfDI ausgeschlossen. Bei diesem Vorschlag für eine Neufassung orientierte sich der TLfDI am Wortlaut des Hessischen Gesetzes zur Anpassung des Hessischen Datenschutzrechts (Drucksache 19/5728) und hier am Vorschlag zur Neufassung von § 10 Satz 3 Hessisches Pressegesetz.
Der Thüringer Landtag nahm diese Anregungen des TLfDI im Rahmen seiner parlamentarischen Beratung des Gesetzentwurfs in der Drucksache 6/4943 auf und ging sogar noch einen Schritt weiter: In § 11a Satz 8 des neuen TPG, das am 15. Juni 2018 in Kraft getreten ist, heißt es nun besonders klar: „Die Selbstregulierung der Presse durch den Pressekodex und die Beschwerdeordnung des Deutschen Presserates bleiben[!] unberührt.“

5.3 Thüringer E-Government-Gesetz

Die Digitalisierung der Gesellschaft ist auch für die öffentliche Verwaltung in Thüringen eine Herausforderung und gleichzeitig eine Chance, Verwaltungsabläufe mit den Bürgern effektiver zu gestalten. Um eine Akzeptanz in der Bevölkerung zu erlangen, bedarf es dabei auch eines EU-konformen Datenschutzes. Im parlamentarischen Verfahren zum Erlass des Thüringer E-Government-Gesetzes wurde der TLfDI frühzeitig beteiligt.

Das Thüringer E-Government-Gesetz (ThürEGovG) vom 10. Mai 2018 wurde im Gesetz- und Verordnungsblatt für den Freistaat Thüringen in Nr. 5 vom 23. Mai 2018 (Berichtigung in Nr. 7 vom 5. Juli 2018) veröffentlicht. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde im Gesetzgebungsverfahren beteiligt und inhaltlich um Stellungnahme gebeten. Dieser Bitte ist der TLfDI gerne nachgekommen. So nahm der TLfDI im Rahmen des Anhörungsverfahrens im Juni 2017 gegenüber dem Thüringer Finanzministerium und im Februar 2018 gegenüber dem Haushalts- und Finanzausschuss des Thüringer Landtags jeweils Stellung.
Das ThürEGovG regelt die Einführung elektronischer Verfahren und die elektronische Abwicklung von Dienstleistungen der öffentlichen Verwaltung in Thüringen.
Ziel des Gesetzes ist, durch den Einsatz von digitalen Informations- und Kommunikationstechniken die, Durchführung von internen und externen Prozessen zur Information, Kommunikation und Transaktion zu vereinfachen, beispielsweise zwischen der Verwaltung und Bürgern oder juristischen Personen.
So werden unter anderen die Einführung von Servicekonten, die Möglichkeit der zentralen Identifikationsmöglichkeit und die Einführung der elektronischen Akte im ThürEGovG geregelt. Um alle Vorhaben des ThürEGovG umsetzen zu können, soll auch die Gewinnung, Bindung und Entwicklung von IT-Fachkräften in der Landesverwaltung auf Grundlage eines gemeinsamen Personalentwicklungskonzepts der obersten Landesbehörden erfolgen.
Mit der Änderung des Grundgesetzes im Juli 2017 erhielt der Bund durch Art. 91c die Gesetzeskompetenz zur Ausgestaltung des Zugangs zu den Verwaltungsleistungen von Bund und Ländern, mit dem

Ziel, dadurch in Deutschland ein moderneres E-Government umzusetzen. Im August 2017 folgte bereits das Onlinezugangsgesetz (OZG). Dieses verpflichtet unter anderem den Bund und die Länder, bis spätestens zum Ablauf des Jahres 2022 ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten. Diese Portale sind zu einem Verbund zu verknüpfen.
Um die Identität eines Nutzers vor Inanspruchnahme elektronischer Dienstleistungen zu überprüfen, regelt das OZG zudem, welche Daten bei der Registrierung erhoben werden dürfen. Der TLfDI berichtete darüber in Punkt 17.1 seines 12. Tätigkeitsberichtes. Mit dem ThürEGovG wurden nun für Thüringen die Rechtsgrundlagen für den elektronischen Zugang zur Verwaltung (§ 6) und die Einrichtung von Servicekonten (§ 7) geschaffen.

I. Servicekonten

Das ThürEGovG regelt in § 8 Abs. 2, dass die Bereitstellung des Servicekontos gemäß § 7 Abs. 1 behördenübergreifend und zentral von einer Stelle erfolgt, die einem dafür geeigneten und zuständigen Ministerium untersteht. Ziel sei laut Begründung zum Gesetzentwurf, dass für jeden Bürger und jede juristische Person in der Regel nur ein Servicekonto notwendig sei. Mit diesem Servicekonto, in Verbindung mit einer elektronischen Identitätsprüfung, können dann sämtliche, angebotene, elektronische Verwaltungsleistungen auf kommunaler Ebene, wie auch auf Landesebene genutzt werden. Gemeinde und Gemeindeverbände mit bereits bestehenden Service- oder Bürgerkonten, die in ihrem Funktionsumfang mindestens dem des zentralen Servicekontos des Landes entsprechen und mit diesem möglichst nahtlos zusammenarbeiten, werden von der Regelung nicht erfasst.
Der TLfDI wies darauf hin, dass insbesondere Bürgerinnen und Bürgern die Möglichkeit eingeräumt werden muss, sowohl einzelne im permanenten Servicekonto dauerhaft gespeicherte, personenbezogenen Daten als auch das Konto selbst löschen zu lassen. Weiterhin besteht entsprechend der Datenschutz-Grundverordnung (DS-GVO) ein Widerspruchsrecht, auf das hinzuweisen ist, da die genannte Einwilligung unter die Voraussetzungen des Art. 7 in Verbindung mit Art. 4 Nr. 11 DS-GVO fällt. Nach Art. 7 Abs. 3 Satz 1 DS-GVO hat die betroffene Person das Recht, ihre Einwilligung jederzeit zu widerrufen. Nach dem Widerruf wird die künftige Verarbeitung von personenbezogenen Daten rechtswidrig. Alle bereits vorhandenen Daten müssen gelöscht oder anonymisiert werden.

Bezüglich der Servicekonten hatte auch die 91. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) bereits im April 2016 die Entschließung „Datenschutz bei Servicekonten“ verabschiedet. Die DSK wies darauf hin, dass dabei das Verbot einer Vorratsdatenspeicherung zu unbestimmten Zwecken sowie das grundrechtliche Prinzip der informationellen Gewaltenteilung zu beachten sind. Der TLfDI berichtete darüber in Punkt 17.1 des 12. Tätigkeitsberichts.

II. Servicekonten-Identitätsprüfung

Diese zentrale Stelle für das Servicekonto fungiert gleichzeitig auch als Identifizierungsdiensteanbieter. So ist geregelt, dass die elektronische Identifizierung anhand einer einmaligen Abfrage der Identitätsdaten erfolgen kann. Ein dauerhaftes Speichern der Identitätsdaten ist nur mit Einwilligung des Nutzers möglich. Weiterhin bedarf es einer Einwilligung des Nutzers, wenn zu seiner Identifizierung erforderliche Daten aus einem bereits bestehenden Servicekonto bei der für das Servicekonto zuständigen Stelle elektronisch abgerufen werden. Festgelegt ist, dass die Einwilligung den datenschutzrechtlichen Anforderungen entsprechen muss. Entsprechend der Begründung zum Gesetzentwurf muss also vor jeder Verwendung von der betroffenen Person die entsprechende datenschutzrechtliche Einwilligung für die konkrete Anwendung erteilt werden, damit die Stammdaten verarbeitet werden können. Eine pauschale Einwilligung wäre aus Sicht des TLfDI auch schon nach der Datenschutz-Grundverordnung (DS-GVO) europarechtswidrig.

Wer für Dritte Dienstleistungen zur Identifizierung anhand von Personalausweisen und ähnlichen Dokumenten zur Identifizierung erbringt, muss zudem über ein entsprechendes Berechtigungszertifikat von der zuständigen Behörde des Bundes verfügen (§ 21b Personalausweisgesetz).

Aus Sicht des TLfDI ist ein zentraler Identifizierungsdiensteanbieter in Thüringen zu begrüßen. So hat der TLfDI bereits im August 2015 gegenüber dem Thüringer Innenministerium und Thüringer Finanzministerium bezüglich des Verfahrens iKfZ (internetbasierte Fahrzeug-Zulassung) empfohlen, mittelfristig bei der einheitlichen Stelle gemäß § 71a Thüringer Verwaltungsverfahrensgesetz, eine zentrale Anwendungsmöglichkeit bezüglich der elektronischen Identifikationsüberprüfung anzubieten.

III. Elektronische Aktenführung

Gemäß § 16 ThürEGovG haben die Behörden des Landes spätestens ab dem 1. Januar 2023 ihre Akten elektronisch in einem zentralen Verfahren zu führen.

Soweit Behörden des Landes ihre Akten elektronisch führen, ist die elektronische Akte dann ab dem 1. Januar 2024 führend. Dies bedeutet theoretisch dann auch die Verabschiedung der Papierakte. Bei der Übertragung in elektronische Dokumente ist dabei nach dem Stand der Technik sicherzustellen, dass die elektronischen Dokumente mit den Papierdokumenten bildlich und inhaltlich übereinstimmen und das nachvollzogen werden kann, wann und durch wen die Unterlagen übertragen wurden. Im Thüringer Archivgesetz (ThürArchivG) vom 29. Juni 2018 wurde flankierend geregelt, dass das Thüringer Landesarchiv für die Archivierung elektronischer Unterlagen ein Digitales Magazin unterhält (§ 8 Abs. 5 ThürArchivG).

Der TLfDI wies in seiner Stellungnahme gegenüber dem Haushals- und Finanzausschuss des Thüringer Landtags darauf hin, dass aus Sicht des TLfDI durchaus Behörden oder Teilbereiche von Behörden nicht dem zentralen Verfahren angeschlossen werden können. Denkbar ist solch ein Fall beispielsweise, wenn das zentrale Verfahren nicht die Anforderungen erfüllt, die aus datenschutzrechtlicher Sicht an personenbezogene Daten mit hohem Schutzbedarf zu stellen sind. Letzteres kann beispielsweise eine Verschlüsselung der Daten erfordern, und zwar nicht nur bei der Datenübertragung, sondern eben auch bei Datenspeicherung.

Weiterhin sollte klargestellt werden, dass jede öffentliche Stelle trotz elektronischer Aktenführung nach einem einheitlichen Verfahren Verantwortlicher im Sinne von Art. 24 Abs. 1 DS-GVO bleibt. Dies hat zur Folge, dass jeder Verantwortliche für die personenbezogenen Daten, die in seinen Verantwortungsbereich fallen, eigenständige technische und organisatorische Maßnahmen festzulegen hat.

In Bezug auf den Geltungsbereich des Gesetzes empfahl der TLfDI weiterhin zu prüfen, ob die Regelung in § 1 Abs. 4 ThürEGovG bezüglich des TLfDI nicht im Hinblick auf Art. 52 DS-GVO europarechtswidrig ist. Danach handelt jede Aufsichtsbehörde nach Art. 51 DS-GVO bei der Erfüllung Ihrer Aufgaben und bei der Ausübung ihrer Befugnisse völlig unabhängig. Damit ist es nicht zu vereinbaren, wenn dem TLfDI durch das Land ein bestimmtes Verfahren vorgeschrieben wird. Es ist daher unverständlich, dass nur der Thüringer

Landtag und der Landesrechnungshof, mit Ausnahme des § 1 Abs. 7 ThürEGovG, nicht vom Geltungsbereich des Gesetzes erfasst sind.

Unabhängig davon nimmt der TLfDI selbstverständlich seine Beratungspflicht war und ist seit Februar 2017 auch beim Projekt „Zentrales DMS“ beratend im zentralen Steuerungsgremium tätig. Dieses Steuerungsgremium befasst sich hauptsächlich mit organisatorischen Fragestellungen bezüglich des Dokumentenmanagement-Systems (DMS). Der TLfDI ist dabei als Anwender und im Rahmen seiner datenschutzrechtlichen Funktion als Aufsichtsbehörde mit mehreren Personen vertreten. Über die im Projekt erzielten Ergebnisse wird der TLfDI in seinem nächsten Tätigkeitsbericht informieren.

5.4 Das neue Thüringer Archivgesetz

Im Gesetzgebungsverfahren wurde der TLfDI frühzeitig beteiligt. Mit dem neuen Thüringer Archivgesetz werden nicht nur die Aufgaben der Archive klar definiert und Regelungen zu Schutzfristen überarbeitet. Es wird auch geregelt, dass das Landesarchiv für die Archivierung elektronischer Daten nach § 3 Abs. 1 und 3 ein Digitales Magazin unterhält.

Das neue Thüringer Archivgesetz (ThürArchivG) vom 29. Juni 2018 wurde im Gesetz- und Verordnungsblatt Nr. 8, Ausgabe vom 26. Juli 2018, veröffentlicht. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde bereits im September 2017 von der Thüringer Staatskanzlei diesbezüglich beteiligt und um Stellungnahme gebeten. Dieser Bitte ist der TLfDI gerne nachgekommen.
Im März 2018 wurde der TLfDI dann im Rahmen des Anhörungsverfahrens zum neuen ThürArchivG vom Ausschuss für Europa, Kultur und Medien des Thüringer Landtags zur mündlichen Anhörung in die öffentliche Sitzung im April 2018 eingeladen. Ziel der Anhörung war es, die Auffassung des TLfDI zum vorliegenden Gesetzentwurf zu erfahren und dem TLfDI Fragen zu stellen.
Im Anhörungsverfahren konnte vom TLfDI mitgeteilt werden, dass die Anregung des TLfDI mit der Einfügung des Satzes 1 in § 17 Abs. 2 des Thüringer Archivgesetz-Entwurfs bereits berücksichtigt wurde. Nach § 17 Abs. 2 Satz 1 ThürArchivG gilt die Schutzfrist nach

Abs. 1 Satz 1 nicht für solche Unterlagen, die bereits bei ihrer Entstehung zur Veröffentlichung bestimmt waren oder für Unterlagen, für die vor der Übergabe an das Landesarchiv bereits ein Zugang oder eine Veröffentlichung nach anderen gesetzlichen Vorschriften vorlag. Denn die Schutzfristen des Abs. 1 können nicht für die Unterlagen gelten, für die vor einer Übergabe an das öffentliche Archiv bereits ein Zugang oder einer Veröffentlichung nach dem Thüringer Informationsfreiheitsgesetz vorlag. Diese Ergänzung war aus der Sicht des TLfDI notwendig, weil insbesondere § 11 Abs. 2 Thüringer Informationsfreiheitsgesetz (ThürIFG) regelt, dass Informationen auch unabhängig von einem Antrag nach § 5 Abs. 1 ThürIFG über das Internet oder sonst in öffentlich zugänglicher Weise zugänglich gemacht werden können.
Gemäß § 3 Abs. 1 und 3 ThürArchivG ist auch geregelt, dass das Landesarchiv für die Archivierung elektronischer Daten zukünftig ein Digitales Magazin unterhält. Bezüglich der technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten und bei der elektronischen Erfassung von Archivgut (digitale Übergabe von zur Archivierung bestimmter Unterlagen) gemäß § 15 ThürArchivG in Verbindung mit § 8 Abs. 6 ThürArchivG ist die Beratung zum Datenschutz durch den TLfDI von der Projektorganisation „Digitales Magazin“ des Thüringer Landesarchivs bereits vorgesehen.

5.5 Schulungsveranstaltung für Thüringer Schulleiter

Die Schulleiter und Schulleiterinnen sollten aus der Fortbildungsveranstaltung des TLfDI mitgenommen haben, dass die Datenschutz-Grundverordnung den Schulen einige Änderungen hauptsächlich im Bereich der Informationspflichten, der Gestaltung von Einwilligungen sowie Auftragsverarbeitungsverträgen bringt. Ein Grund zur Panik besteht in keinem Fall. Vieles bleibt im Schulbetrieb beim Alten.

Um den großen Unsicherheiten zu begegnen, die im Zusammenhang mit der Geltung der Datenschutz-Grundverordnung (DS-GVO) in den Schulen entstanden sind, hatte sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bereits Ende 2017 an Herrn Minister Holter vom Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) gewandt und dort die Durchführung von Fortbildungsveranstaltungen zum Inhalt der DS-GVO und

deren Bedeutung für die Schulen vorgeschlagen. Um möglichst flächendeckend alle derzeit 824 in staatlicher Trägerschaft befindlichen Schulen zu erreichen, schlug der TLfDI vor, jeweils eine Veranstaltung in jedem Zuständigkeitsbereich der fünf staatlichen Schulämter durchzuführen. Es war also mit durchschnittlich jeweils 165 teilnehmenden Schulleiterinnen und Schulleitern zu rechnen.
Nachdem eine längere Zeit ohne eine Reaktion auf den Vorschlag des TLfDI vergangen war, wandte sich dieser im März 2018 erneut an das TMBJS mit der Bitte um konkrete Vorschläge zu möglichen Terminen und Veranstaltungsorten. Die Aufgabe zur Abstimmung von Terminvorschlägen sowie der passenden Örtlichkeiten wurde vom Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien übernommen. In den letzten beiden Septemberwochen war es dann soweit. Der TLfDI und zwei seiner für den Bildungsbereich zuständigen Mitarbeiter standen dann für jeweils zwei Stunden den Schulleiterinnen und Schulleitern zur Verfügung, wobei zunächst ein Vortrag zum „Datenschutz in der Schule“ hinsichtlich der Auswirkungen der DS-GVO auf die schulische Arbeit gehalten wurde. Anschließend hatten die Schulleiter und Schulleiterinnen Gelegenheit Fragen zu stellen. Wenn in einigen Fällen die Sachverhalte nicht unmittelbar beantwortet werden konnten, wurden die Fragenden gebeten, sich nochmals schriftlich an den TLfDI zu wenden.
Die Stimmung im Auditorium wurde vom TLfDI je nach Schulamtsbezirk als höchst unterschiedlich wahrgenommen. Es gab Veranstaltungen, bei denen die Zuhörer engagiert und mit Interesse für die Materie den Vortrag verfolgten und interessante schulfachliche Fragen stellten. An anderen Terminen herrschte eine als erregt zu bezeichnende Stimmung unter den Teilnehmern, die die verschiedenen Informationspflichten, die die DS-GVO den Schulen mittlerweile auferlegt, mit Unmutsbekundungen quittierten. Der TLfDI wies die Teilnehmer an verschiedenen Stellen mehrfach darauf hin, dass viele datenschutzrechtliche Regelungen bereits vor der Geltung der DS-GVO auf die gleiche Weise umzusetzen waren. Wie auch bisher dürfen personenbezogene Daten verarbeitet werden, soweit dies zur Erfüllung der gesetzlichen Aufgaben der Lehrkräfte oder der Schulen erforderlich ist. Damit sind Benotungen von Lernenden und die Zeugnisausgabe selbstverständlich wie in der Vergangenheit möglich. Der TLfDI wird alle offenen Fragen der Schulen beantworten beziehungsweise

hat dies bereits gegenüber einigen staatlichen Schulämtern bereits getan und wird die Antworten auf seiner Internetseite veröffentlichen (FAQ-Liste).

5.6 Evaluation des Kurses Medienkunde – Vermutungen des TLfDI bestätigt

Die Evaluation des Kurses Medienkunde an Thüringer Schulen ist abgeschlossen. Unter anderem wird die Einführung eines regulären Unterrichtsfaches „Medienkunde“ empfohlen. Die Ergebnisse bestätigen die Vermutungen und Handlungserfordernisse, die der TLfDI seit Langem öffentlich vertritt.

Medienbildung in der Schule tut not. Das gilt nicht erst, seitdem Facebook, WhatsApp und „Insta“ das Miteinander von Jugendlichen prägen wie kein anderes Medium zuvor. Thüringen hatte das früh erkannt und schon 2001 einen Kurs Medienkunde für die Klassenstufen 5 bis 7 an Thüringer Schulen eingeführt. Unser Freistaat war damals Protagonist in der Bundesrepublik. Später wurde der Kurs erweitert bis zur 10. Klassenstufe. Ein Kursplan legt fest, was inhaltlich in Eigenregie der Schule umgesetzt werden soll. Wichtigstes Merkmal: Medienkunde ist kein Unterrichtsfach, das in der Stundentafel verankert ist. Vielmehr legt jede Schule für sich fest, welche medienbezogenen Kompetenzen in welchem regulären Unterrichtsfach „integrativ“ erreicht werden sollen. Das klappt in der einer Schule besser, in der anderen weniger gut, wie der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) aus vielen Gesprächen mit Lehrern und Schülern weiß. Auch auf seine Anregung hin beauftragte das Bildungsministerium eine landesweite Evaluation des Kurses. Ein Team der TU Ilmenau um Prof. Dr. Wolling prüfte ab Mitte 2016 in den Schulen und befragte dabei Lehrer und Experten. Der TLfDI war auch beteiligt und informierte darüber in seinem 12. Tätigkeitsbericht. Seit Anfang 2018 sind die Evaluationsergebnisse von Prof. Wolling unter https://www.db-thueringen.de/receive/dbt_mods_00034913 veröffentlicht.

Ergebnis: Die Befürchtungen des TLfDI wurden (leider) umfänglich bestätigt. Ein bezeichnendes Ergebnis unter anderen: Der integrative Ansatz hat sich grundsätzlich bewährt, jedoch sollte zusätzlich ein reguläres Unterrichtsfach Medienkunde eingeführt werden. Das entspricht genau einem Vorschlag des TLfDI, den er seit Langem immer wieder in die öffentliche Diskussion eingebracht hatte. Hier wäre z. B. Platz für die Sensibilisierung von Schülerinnen und Schülern für (ihren!) Privatsphärenschutz und den Erwerb einer entsprechenden Medienkompetenz. In einer datengetriebenen Lebenswelt ist Selbstdatenschutz mehr denn je Ausdruck von informationeller Selbstbestimmung. Wie stelle ich mein Smartphone ein, damit Apps nicht ungewollt meine persönlichen Daten in die Untiefen des Internets schießen? Wie stelle ich meinen Internetbrowser datenschutzfreundlich ein? Wie suche ich im Netz erfolgreich und trotzdem datensparsam? Welche Rechte habe ich als Bürger der EU, um auf den Umgang anderer mit meinen Daten Einfluss zu nehmen? Hier muss der Schritt vom Wissen zum Entscheiden hin zum Handeln können durch die Schule maßgeblich unterstützt werden. Anders als in Biologie, Kunsterziehung oder einem anderen Fach wäre hierfür in einem Fach Medienkunde genau der richtige Platz.
Neben dieser durchaus spektakulären Empfehlung, ein neues Unterrichtsfach einzuführen, wird im Evaluationsbericht unter anderem explizit auf die Notwendigkeit hingewiesen, die Vorbereitung der Lehrkräfte durch medienkompetenzbezogene Aus- und Fortbildung anzugehen und eine generelle Digitalisierung in den Schulen in den Blick zu nehmen. Auch der TLfDI sieht die Lehrerbildung als absoluten Schwerpunkt, der zügig vorangetrieben werden muss. Die Evaluationsergebnisse korrelieren weitgehend mit den Impulsen, die auch die Kultusministerkonferenz in ihrem Strategiepapier „Bildung in der digitalen Welt“ setzt. Erfreulicherweise hat das Thüringer Bildungsministerium im September 2018 mit Überlegungen zu einer „Digitalstrategie Thüringer Schule (DiTS)“ reagiert. Ein Unterrichtsfach Medienkunde/Informatik wird kommen! Eine Chance für Thüringen, hier endlich wieder Profil zu zeigen. Der TLfDI wird dabei sichtbare Spuren hinterlassen, auch was den nur zähen Prozess der Beseitigung der vom Evaluationsbericht aufgedeckten zahlreichen Defizite anbelangt.

5.7 Sie fragen, wir antworten: FAQs zur DS-GVO in den Thüringer Kommunen

Im Sommer 2018 richteten die Thüringer Kommunen in bisher ungekannter Anzahl Fragen zur Anwendung der Datenschutz-Grundverordnung (DS-GVO) an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Um möglichst viele dieser Fragen schnell und verständlich zu beantworten, lud der TLfDI gemeinsam mit dem Thüringer Gemeinde- und Städtebund und dem Thüringischen Landkreistag alle kommunalen Datenschutzbeauftragten sowie weitere interessierte Personen zu einer FAQ-Veranstaltung (FAQ = **f**requently **a**sked **q**uestions, übersetzt: häufig gestellte Fragen) am 21. August 2018 in die Stadthalle Apolda ein. Weitere praktische Tipps rund um das Thema Datenschutz in den Thüringer Kommunen finden Sie auf der Internetseite TLfDI- unter: https://www.tlfdi.de/tlfdi/datenschutz/kommunales/

Kurz nach der Anwendung der Datenschutz-Grundverordnung (DS-GVO) am 25. Mai 2018, häuften sich beim TLfDI die Posteingänge und Anfragen aus den Kommunen in bisher nicht gekannter Anzahl, wie die DS-GVO in allen erdenklichen Gebieten des von den Kommunen anzuwendenden Fachrechts zu berücksichtigen und auszulegen sei. Wie konnte der TLfDI diesen „Anfrageberg“ abbauen – angesichts der Tatsache, dass die Behörde nicht den benötigten Personalzuwachs zur Bewältigung der aus der DS-GVO resultierenden Mehraufgaben erhalten hatte? Der TLfDI entschloss sich daher, gemeinsam mit dem Thüringer Gemeinde- und Städtebund (GStB) und mit dem Thüringischen Landkreistag (LKT) eine sogenannte FAQ-Veranstaltung am 21. August 2018 in der Stadthalle in Apolda anzubieten; sie richtete sich an alle kommunalen Datenschutzbeauftragten und weiteren interessierten Personen. Im Vorfeld dieser Veranstaltung hatten alle interessierten Mitarbeiterinnen und Mitarbeiter der Thüringer Kommunen die Gelegenheit, ihre Fragen und Probleme rund um die DS-GVO an den GStB und den LKT zu senden, die diese dann gebündelt zur Klärung und Beantwortung an den TLfDI weiterleiteten. Eine Zusammenfassung aller in Apolda erörterten Fragen und Probleme zur Anwendung

der DS-GVO in den Kommunen findet sich in der Power-Point-Präsentation des TLfDI unter https://www.tlfdi.de/mam/tlfdi/vortrag_ds-gvo_in_kommunen_internetfassung_stand_28.08.2018.pdf .

Nachfolgend sollen die wichtigsten Fragen zur Anwendung der DS-GVO in den Thüringer Kommunen noch einmal zusammengefasst beantwortet werden:

Frage 1: Wo fangen wir an? Was ist am dringendsten umzusetzen? Worauf ist besonders zu achten?
Antwort: Der TLfDI riet dazu, folgende Schritte zur Anwendung der DS-GVO einzuschlagen:

- Bestellung eines Datenschutzbeauftragten, Veröffentlichung von dessen Kontaktdaten, Mitteilung an den TLfDI gemäß § 13 Thüringer Datenschutzgesetz (ThürDSG)
- Einführung und Anwendung der Informationspflichten gemäß Art. 13 und 14 DS-GVO, zu den Rechten der betroffenen Person und zu Löschkonzepten
- Festlegung der Rechtsgrundlagen und des Zwecks der Datenverarbeitung
- Erstellen von Verzeichnissen von Verarbeitungstätigkeiten für jedes Verfahren gemäß Art. 30 DS-GVO
- Erlass einer Datenschutzerklärung und einer Dienstanweisung zum Datenschutz für die Behörde
- Anpassung bestehender Verträge zur Auftragsverarbeitung
- Kommunale Satzungen auf die Vereinbarkeit mit der DS-GVO prüfen
- Anpassung sämtlicher Datenverarbeitungsprozesse und -strukturen an die DS-GVO.

Dem TLfDI war und ist klar, dass dies insbesondere in kleinen Thüringer Gemeinden nicht „über Nacht“ geschehen konnte und kann, auch weil der Schulungsbedarf groß und die Schulungsangebote landesweit alles andere als breit gefächert waren und sind.

Frage 2: Was, außer der Datenschutzerklärung, sollte auf der gemeindlichen Homepage noch veröffentlicht oder angepasst werden?

Antwort: Der TLfDI empfiehlt, folgende Informationen auf der Homepage zu veröffentlichen:

- Kontaktdaten des Datenschutzbeauftragten
- Beachtung der Informationspflichten nach § 40 ThürDSG für alle Fälle, in denen nicht die DS-GVO, sondern die JI-Richtlinie und damit die §§ 31 ff. ThürDSG Anwendung finden
- Bereitstellung von Informationen, die nach Art. 13 und 14 DS-GVO mitgeteilt werden müssen:
  - Name und Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters
  - die Zwecke und die Rechtsgrundlage der Datenverarbeitung
  - die Empfänger oder die Kategorien von Empfängern der personenbezogenen Daten
  - gegebenenfalls die Absicht, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln
  - Angabe der Dauer der Datenspeicherung
  - Hinweise auf das Auskunfts- und Beschwerderecht bei der Datenschutzaufsichtsbehörde
  - gegebenenfalls Hinweis auf eine gesetzliche oder vertragliche Regelung, die die Bereitstellung personenbezogener Daten vorschreibt und Hinweis auf mögliche Folgen einer Nichtbereitstellung sowie der Hinweis auf das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling

Frage 3: Wie und wann sind die Bürger über den Datenschutz zu informieren?
Antwort: Die Bürgerinnen und Bürger sind bei jeder Datenverarbeitung zu informieren,

- die unter die DS-GVO und das ThürDSG fällt, nämlich bei der Verarbeitung von personenbezogenen Daten,
- die gegebenenfalls spezialgesetzliche Regelungen berührt, z. B. § 82 SGB X,
- und zwar in präziser, transparenter, verständlicher, in leicht zugänglicher Form und in einer klaren einfachen Sprache (siehe Wortlaut von Art. 12 Abs. 1 Satz 1 DS-GVO),
- und zwar zum Zeitpunkt der Erhebung personenbezogener Daten des Betroffenen.

Eine Rechenschaftspflicht für die Einhaltung der transparenten Informationsgewährung besteht nach Art. 5 Abs. 2 DS-GVO; allerdings

bedeutet dies nicht, dass der Betroffene den Erhalt der Informationen zu unterschreiben hat.

Frage 4: Auf welche Formulare müssen Datenschutzhinweise abgedruckt werden? Gibt es hierfür Mustertexte?
Antwort: Der TLfDI wies darauf hin, dass es hierzu keine allgemeingültigen Regelungen gibt, auf welchen Formularen die Informationspflichten abgedruckt werden müssen. Wichtig sei aber, dass den Informationspflichten aus Art. 13 und 14 DS-GVO vom Verantwortlichen **zum Zeitpunkt der Erhebung personenbezogener Daten** einer betroffenen Person nachgekommen wird. Der TLfDI verwies in diesem Zusammenhang auf folgende Hinweise und Kurzpapiere:

- Verweis auf Hinweise zu den Informationspflichten zur Erhebung von personenbezogenen Daten
www.tlfdi.de/mam/tlfdi/datenschutz/hinweise_zu_den_informationen.pdf

- Hinweisblatt für die Behörde des TLfDI:
www.tlfdi.de/mam/tlfdi/datenschutz/informationen_zur_verarbeitung_von_personenbezogenen_daten_.pdf

- Kurzpapier Nr. 10 „Informationspflichten bei Dritt-und Direkterhebung“ www.tlfdi.de/mam/tlfdi/gesetze/dsk_kpnr_10_informationspflichten.pdf

Frage 5: In welcher Form muss informiert werden? Problematisch stellen sich die neuen Informationspflichten insbesondere bei sogenannten Massenbescheiden dar. Ist der Informationspflicht im Falle einer schriftlichen Kommunikation mit dem Bürger Genüge getan, wenn die Gemeinden in ihren Bescheiden einen

(Datenschutz-) Hinweis aufnehmen und dieser in Verbindung mit einem auf der Internetseite der jeweiligen Gemeinde hinterlegtem Informationsschreiben gebracht wird?
Antwort: Der TLfDI wies bei der Beantwortung dieser Frage auf Folgendes hin:

- Grundsätzlich ist ein allgemeiner Hinweis zu den Informationspflichten, die dann genauer auf der TLfDI-Internetseite näher erläutert und ausgeführt werden, nicht zulässig. Darauf hat der TLfDI auch noch einmal in seinem Schreiben vom 25. September 2019 an alle obersten Landesbehörden – die das Schreiben an die Kommunen weiterleiten sollten – hingewiesen. Danach sind die Voraussetzungen des Art. 12 DS-GVO dann nicht gegeben, wenn die betroffene Person, die einen Brief erhält, die übermittelte URL (also den Link) erst im Internet eingeben muss, um an die Informationen nach Art. 13 und Art. 14 DS-GVO zu gelangen. Die Angabe eines Links ist nach Auffassung des TLfDI nur dann zulässig, wenn es sich um Informationen handelt, die im Internet gegeben werden, beispielsweise über die Datenverarbeitung bei der Nutzung des Internetauftritts der jeweiligen Seite. Gleiches gilt, wenn mit dem Betroffenen per E-Mail kommuniziert wird, da in diesem Fall ohnehin die Nutzung des Internets erforderlich ist, um die E-Mail lesen zu können (und damit kein sogenannter Medienbruch, also ein Wechseln der Kommunikationsform) stattfindet. In diesem Zusammenhang verwies der TLfDI auf folgenden Hinweis:
https://www.tlfdi.de/mam/tlfdi/datenschutz/hinweise_zu_den_informationen.pdf

Frage 6: Bestehen gegenüber Steuer- und Abgabepflichtigen besondere Informationspflichten?
Antwort: Nein, es bestehen in diesen Fällen keine besonderen Informationspflichten. Der TLfDI wies in diesem Zusammenhang jedoch darauf hin, dass nicht mehr er, sondern der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit gemäß § 32h Abgabenordnung zuständig ist für die Aufsicht über die Finanzbehörden hinsichtlich der Verarbeitung personenbezogener Daten im Anwendungsbereich der Abgabenordnung.

Frage 7: Wie sind Bestandskunden zu informieren? Wie sind Neukunden zu informieren?
Antwort: Der TLfDI wies unter Beachtung des Wortlauts des Art. 13 Abs. 1 Satz 1 DS-GVO („zum Zeitpunkt der Erhebung dieser Daten“) darauf hin, dass den Informationspflichten bei Bestandskunden zum Zeitpunkt des erstmaligen Kontakts mit dem Kunden nach der endgültigen Anwendbarkeit der DS-GVO zum 25. Mai 2018 nachgekommen werden muss.
Die Informationspflichten bei Neukunden sind einzuhalten zum Zeitpunkt, an dem die personenbezogenen Daten des Neukunden erstmalig erhoben werden.

Frage 8: Gelten die Informationspflichten der DS-GVO für sämtliche Verwaltungsvorgänge, bei denen personenbezogene Daten genutzt werden (Ordnungsamt, Sondernutzungsanträge, Baumfällungen, Verfahren im Meldeamt, Standesamt)?
Antwort: Der TLfDI konnte diese Frage mit „grundsätzlich ja“ beantworten, wies aber auf folgende Ausnahmen hin: Die DS-GVO-Informationspflichten kommen nicht zur Anwendung,

- wenn die Verarbeitung personenbezogener Daten unter den Anwendungsbereich der JI-Richtlinie fällt und damit die §§ 31 ff. ThürDSG einschlägig sind. In diesem Fall richten sich die Informationspflichten nach § 40 ThürDSG (Allgemeiner Informationsanspruch)
- wenn ein Fall des Art. 13 Abs. 4 DS-GVO (Betroffener verfügt bereits über die Informationen) oder ein Fall des Art. 14 Abs. 5 DS-GVO (Betroffener verfügt über die Informationen, die Bereitstellung ist unmöglich oder unverhältnismäßig) vorliegt
- wenn ein Fall des § 20 Abs. 1 oder 2 ThürDSG vorliegt, wonach die Informationspflichten beschränkt werden können, z. B. bei Gefährdung der öffentlichen Sicherheit oder wenn die Daten ausschließlich zur Datensicherung oder Datenschutzkontrolle verarbeitet werden.

Frage 9: Ist eine Einwilligung der betreffenden Person notwendig, wenn ich eine gesetzliche Grundlage zur Datenverarbeitung habe, z. B. § 62 Personenstandsgesetz (PStG) – Auskunft aus dem Personenstandsregister?

Antwort: Soweit eine gesetzliche Grundlage für die Datenverarbeitung einschlägig ist, ist eine Einwilligung unnötig und somit nicht mehr erforderlich. Daher gilt: Der Mitarbeiter einer datenverarbeitenden öffentlichen Stelle hat immer erst nach einer gesetzlichen Grundlage für die Datenverarbeitung zu suchen. Erst wenn diese gesetzliche Grundlage oder ein weiterer Grund aus Art. 6 Abs. 1 DS-GVO, der eine Datenverarbeitung für zulässig erklärt, nicht gegeben ist, kommt die Einwilligung als Rechtfertigungsgrund für eine Datenverarbeitung in Frage. Die Einwilligung muss aber freiwillig erklärt werden; hierzu ist Erwägungsgrund 43 zu beachten.

Frage 12: Was ist beim Vorlesen von Heiratsanträgen bei einer Eheschließung mit Publikum künftig zu beachten? Inwieweit ist das Verlesen eines Heiratseintrags im Register, der alle maßgeblichen Daten der Eheschließenden, Zeit und Ort der Eheschließung sowie Angaben zum Recht der Namensführung enthält, datenschutzrechtlich nach Inkrafttreten der DS-GVO zu bewerten, insbesondere dann, wenn während der Zeremonie der Eheschließung mehr als 50 Personen anwesend sind und sich darunter auch keine direkte Verwandtschaft befindet?
Antwort: Zur Beantwortung dieser Frage wies der der TLfDI zunächst auf den Wortlaut des § 14 Abs. 1 Personenstandsgesetz (PStG) hin:

(1) Vor der Eheschließung sind die Eheschließenden zu befragen, ob sich seit der Anmeldung ihrer Eheschließung Änderungen in ihren die Ehevoraussetzungen ***betreffenden tatsächlichen Verhältnissen*** *ergeben haben und ob sie* ***einen Ehenamen bestimmen*** *wollen.*
Daraus und aus der Kommentierung von Gaaz/Bornhofen, Personenstandsgesetz, Handkommentar, 2. Auflage 2010 ergab sich für den TLfDI, dass sowohl die **Feststellung der Anwesenheit des Brautpaares** als auch die **Erklärungen zur Namensführung der Brautleute** unmittelbar vor der eigentlichen Trauungszeremonie durchzuführen sind (siehe Gaaz/Bornhofen, § 14, Rdnr. 15 bis 21). Folglich darf der Standesbeamte alle personenbezogenen Daten der künftigen Eheleute, die er während der Eheschließung zur Erfüllung seiner Verpflichtungen aus § 14 Abs. 1 PStG benötigt, gemäß dieser Rechtsgrundlage und in Verbindung mit Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO verarbeiten.

Davon zu unterscheiden war für den TLfDI die Frage, welche Personen zur Eheschließung in das dafür von der Gemeinde vorgesehene Trauzimmer einzulassen sind. Hierzu führt die Kommentierung von Gaaz/Bornhofen, a. a. O., Rdnr. 13, Folgendes aus:

Für die Trauung gilt der Grundsatz der Beteiligtenöffentlichkeit (vergleiche §§ 13, 29, 67 Verwaltungsverfahrensgesetz (VwVfG)) Grundsätzlich sollen neben dem Standesbeamten nur die Eheschließenden und eventuelle Zeugen anwesend sein. ***Auf Wunsch der Brautleute kann Verwandten und Freunden die Anwesenheit während der Trauung gestattet werden. Unbeteiligten Zuschauern ist der Zutritt zum Eheschließungsraum zu verwehren****.*

An dieser Stelle offenbart sich aus der Sicht des TLfDI die „Krux mit der DS-GVO“: Nur weil ein neues Datenschutz-Fachrecht vom EU Gesetzgeber geschaffen worden ist, bedeutet dies nicht, dass das nationale Recht, wie z. B. das PStG oder das VwVfG automatisch nicht mehr anzuwenden ist. Das Gegenteil ist der Fall: Bundes- und Landesrecht bleibt neben der DS-GVO und ThürDSG anwendbar, es ist jedoch im Zusammenhang mit den datenschutzrechtlichen Bestimmungen zu lesen. Leichter gesagt als getan....

Abschließend weist der TLfDI darauf hin, dass er auf seiner Homepage unter https://www.tlfdi.de/tlfdi/datenschutz/kommunales/ eine Vielzahl von Arbeitshilfen, Hinweisen und Vorschlägen zu datenschutzrechtlichen Problemen in der kommunalen Praxis abrufbar bereit hält. Dieses Serviceangebot soll auch weiter ausgebaut und aktualisiert werden, weil der TLfDI zusammen mit Vertretern des Thüringer Ministeriums für Inneres und Kommunales und den Kommunalen Spitzenverbänden in der Arbeitsgemeinschaft „Umsetzung der DS-GVO in den Kommunen“ kommunale Datenschutzprobleme aufbereitet. Ein laufender Prozess.

5.8 Datenschutz-Grundverordnung – neue Aufgaben? Die Öffentlichkeitsarbeit des TLfDI

Die Datenschutz-Grundverordnung (DS-GVO) definiert zahlreiche Aufgaben einer Datenschutz-Aufsichtsbehörde. Große Bedeutung hat dabei die Öffentlichkeitsarbeit, die regelmäßig über aktuelle Risiken bei der Verarbeitung personenbezogener Daten berichtet und betroffene Personen sowie Verantwortliche für Datenschutz-Themen sensibilisieren soll. In dieser Aufgabe sieht der TLfDI einen wesentlichen Schwerpunkt seiner Arbeit.

Die Datenschutz-Grundverordnung (DS-GVO) enthält in Art. 57 Abs. 1 eine umfangreiche Liste der Aufgaben der Aufsichtsbehörde. Direkt nach der Definition der primären Überwachungsaufgabe in Buchstabe a), findet sich an zweiter Stelle der Aufgabenliste, unter Buchstabe b), die Aufgabe, die „Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechtezusammenhang mit der Verarbeitung [zu] sensibilisieren und sie darüber aufzuklären." Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) versteht diese Aufgabe so, dass die Aufsichtsbehörde neben ihrer Überwachungsfunktion auch eine Beratungsfunktion hat. Aufgrund ihrer personellen Ausstattung ist die Thüringer Datenschutz-Aufsichtsbehörde nicht in der Lage, die Einhaltung datenschutzrechtlicher Vorschriften flächendeckend zu überwachen sowie proaktiv mögliche Verstöße zu verhindern beziehungsweise zu verfolgen. Ein wichtiges Instrument zur Einhaltung datenschutzrechtlicher Bestimmungen ist daher die Öffentlichkeitsarbeit; sie klärt über geltende Bestimmungen auf und zeigt im Einzelnen Wege zur rechtskonformen Ausgestaltung der Datenverarbeitung auf. Der Begriff „Öffentlichkeit" umfasst dabei sowohl die von der Datenverarbeitung betroffenen Personen als auch die Verantwortlichen und deren Auftragsverarbeiter, die bei der Datenverarbeitung die geltenden Bestimmungen des Datenschutzrechts einzuhalten haben. Beide Zielgruppen sollten die gesetzlichen Bestimmungen der DS-GVO kennen.
Für betroffene Personen ist es wichtig, dass sie ihre nach der DS-GVO definierten Rechte kennen. Die DS-GVO hat die neuen rechtlichen Regelungen erheblich erweitert. Den betroffenen Personen stehen laut Art. 13 und 14 DS-GVO nun umfangreiche Informationsrechte zur Verarbeitung ihrer personenbezogenen Daten zu. Auch das Aus-

kunftsrecht der betroffenen Personen wurde in Art. 15 DS-GVO erweitert. Es gibt weiterhin das Recht auf Berichtigung (Art. 16 DS-GVO) und das Recht auf Löschung (Art. 17 DS-GVO) sowie das Recht auf Einschränkung der Verarbeitung, davor Sperrung, (Art. 18 DS-GVO). Neu ist das Recht auf Datenübertragbarkeit, das betroffenen Personen das Recht einräumt, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten gängigen und maschinenlesbaren Format zu erhalten (Art. 20 DS-GVO). Weitere Informationen zu den Betroffenenrechten finden sich unter Beitrag 5.14.

Für die zweite Zielgruppe der Öffentlichkeitsarbeit, die Verantwortlichen und Auftragsverarbeiter, gibt es einige neue Anforderungen, bei denen noch gewisse Unsicherheiten bestehen. Der TLfDI erfüllt seine „Sensibilisierungsaufgabe“ auf vielfältige Weise. In diesem Zusammenhang sei zunächst auf die Veröffentlichungen auf der Internetseite des TLfDI unter https://www.tlfdi.de/tlfdi/europa/europaeische-dsgvo/index.aspx verwiesen. Dort finden sich Informationen zu den verschiedensten Themen im Zuge der Umsetzung der DS-GVO. Sie sind teilweise allgemeiner Natur, richten sich aber auch an spezielle Gruppen, wie beispielsweise Vereine und kleine Unternehmen. Daneben weist der TLfDI regelmäßig mithilfe von Pressemitteilungen auf aktuelle Informationen zur DS-GVO hin. Hierzu wird auf die Rubrik Pressemitteilungen auf der Internetseite des TLfDI unter https://www.tlfdi.de/tlfdi/presse/pressemitteilungen/ verwiesen. Ein wichtiges Standbein der Öffentlichkeitsarbeit waren im Berichtszeitraum die zahlreichen Informationsveranstaltungen, die der TLfDI abgehalten hat (siehe Beitrag 9.1). Schließlich gab es im Berichtszeitraum auch noch zwei Großveranstaltungen zu speziellen Themen. Hier konnten sich interessierte Personengruppen informieren und mit qualifizierten Fachleuten über anstehende Probleme diskutieren.

Der TLfDI sieht die Öffentlichkeitsarbeit auch weiterhin als eine wichtige Aufgabe an und wird sich im kommenden Berichtszeitraum erneut aktuellen Themen und

Dauerthemen des Datenschutzes widmen, um allen betroffenen Personen, Verantwortlichen und Auftragsverarbeitern mit entsprechenden Veröffentlichungen weitergehende Informationen zur Verfügung zu stellen sowie Schulungsveranstaltungen durchführen, soweit dies die personelle Kapazität erlaubt. Zudem wird der TLfDI selbstverständlich allen betroffenen Personen, Verantwortlichen sowie Auftragsverarbeitern in beratender Funktion zur Verfügung stehen.

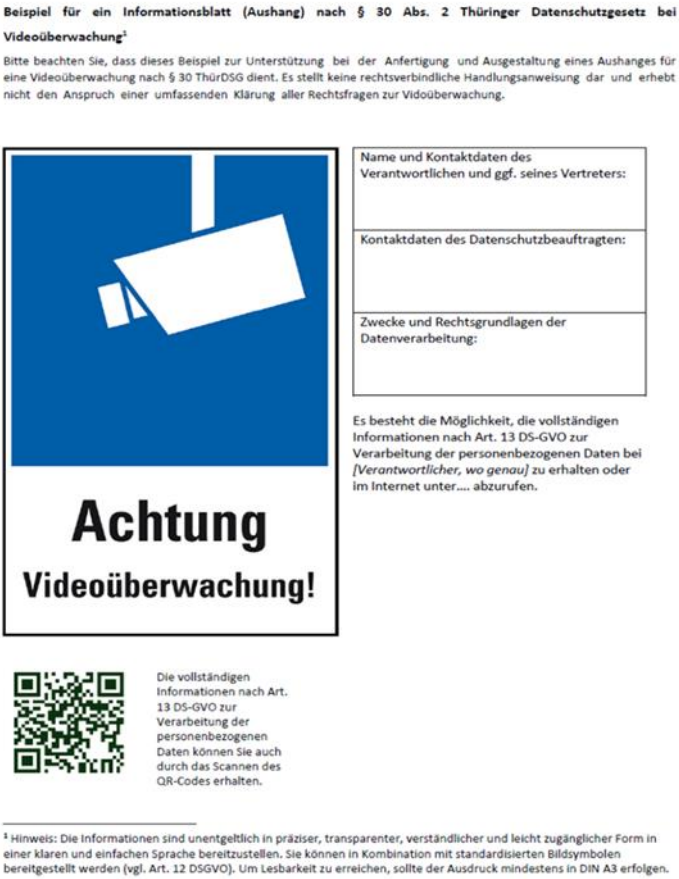
5.9 Videoüberwachung durch öffentliche Stellen nach dem neuen Thüringer Datenschutzgesetz

Die Zulässigkeit und die Voraussetzungen einer Videoüberwachung, die von öffentlichen Stellen eingesetzt wird, wird in § 30 des Thüringer Datenschutzgesetzes geregelt. Dabei sind insbesondere die neuen Informationspflichten zu beachten. Hinweisschilder zur Videoüberwachung müssen demnach leicht zugänglich und sichtbar angebracht werden und in einer verständlichen, klaren und einfachen Sprache ausformuliert sein.

Die Datenschutz-Grundverordnung (DS-GVO) regelt die Videoüberwachung nicht konkret. Die Videoüberwachung, die von öffentlichen Stellen eingesetzt wird, stellt demzufolge eine allgemeine Art der Datenverarbeitung gemäß Art. 6 Abs. 1 Buchstabe e) und Abs. 2 DS-GVO dar und wurde durch den Thüringer Gesetzgeber genauer geregelt. In diesem Zusammenhang passte der Gesetzgeber § 30 des Thüringer Datenschutzgesetzes (ThürDSG) in Bezug auf Zulässigkeit und Voraussetzungen einer Videoüberwachung an.
Eine mit der Hilfe optisch-elektronischer Einrichtungen beabsichtigte Videoüberwachung (Videobeobachtung oder -aufzeichnung) ist gemäß § 30 ThürDSG zulässig, wenn dies zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung öffentlicher Gewalt zum Schutz von Personen, die der überwachenden Stelle angehören oder sie aufsuchen (§ 30 Abs. 1 Nr. 1 ThürDSG) oder dem Schutz von Sachen, die der zu überwachenden Stelle oder den ihr angehörenden Personen gehören (§ 30 Abs. 1 Nr. 2 ThürDSG), erforderlich ist. Es dürfen jedoch keine Anhaltspunkte bestehen, dass schutzwürdige Interessen betroffener Person überwiegen.

Entscheidet sich die öffentliche Stelle für den Einsatz einer Videoüberwachung, muss sie insbesondere die gesteigerten Informationspflichten beachten. Es reicht zukünftig nicht mehr aus, lediglich mithilfe eines Symbols auf den Umstand der Videoüberwachung hinzuweisen. Das festgelegte Transparenzgebot (Art. 12 DS-GVO) in der Datenschutz-Grundverordnung erfordert, dass alle Informationen zur Verarbeitungstätigkeit dieser personenbezogenen Daten leicht zugänglich positioniert und verständlich in einer klaren und einfachen Sprache verfasst sind. Allerdings hat sich der Thüringer Gesetzgeber dafür entschieden, dass nicht sämtliche Informationen unmittelbar zur Verfügung gestellt werden müssen. Die verantwortliche öffentliche Stelle muss auf dem Hinweis zur Videoüberwachung (siehe unten Abbildung 1) Informationen zu sich als verantwortliche Stelle und ihrem Vertreter angeben; dazu gehören die Kontaktdaten des Datenschutzbeauftragten, die Zwecke der Datenverarbeitung und die Rechtsgrundlage für die Verarbeitung. Wichtig dabei ist, dass in dem Hinweis erwähnt wird, wo betroffene Personen weitere Informationen zur Verarbeitung ihrer personenbezogenen Daten erhalten können (z. B. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten, Speicherdauer, Rechte der Betroffenen).
Der TLfDI fertigte hierzu das nachfolgende Muster an, an dem sich die verantwortlichen Stellen orientieren können, wenn sie von der Videoüberwachung Gebrauch machen möchten. Unter folgendem Link ist das Hinweisschild zur Videoüberwachung nach Art. 13 DS-GVO auf der Internetseite des TLfDI als pdf-Datei abrufbar: https://www.tlfdi.de/mam/tlfdi/datenschutz/beispiel_fur_ein_informationsblatt.pdf

Abb.1:



Beispiel für ein Informationsblatt (Aushang) nach § 30 Abs. 2 Thüringer Datenschutzgesetz bei Videoüberwachung[1]

Bitte beachten Sie, dass dieses Beispiel zur Unterstützung bei der Anfertigung und Ausgestaltung eines Aushanges für eine Videoüberwachung nach § 30 ThürDSG dient. Es stellt keine rechtsverbindliche Handlungsanweisung dar und erhebt nicht den Anspruch einer umfassenden Klärung aller Rechtsfragen zur Vidoüberwachung.

Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters:
Kontaktdaten des Datenschutzbeauftragten:
Zwecke und Rechtsgrundlagen der Datenverarbeitung:

Es besteht die Möglichkeit, die vollständigen Informationen nach Art. 13 DS-GVO zur Verarbeitung der personenbezogenen Daten bei *[Verantwortlicher, wo genau]* zu erhalten oder im Internet unter.... abzurufen.

Die vollständigen Informationen nach Art. 13 DS-GVO zur Verarbeitung der personenbezogenen Daten können Sie auch durch das Scannen des QR-Codes erhalten.

[1] Hinweis: Die Informationen sind unentgeltlich in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitzustellen. Sie können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden (vgl. Art. 12 DSGVO). Um Lesbarkeit zu erreichen, sollte der Ausdruck mindestens in DIN A3 erfolgen.

5.10 Europa rückt näher zusammen – auch im Bereich des Datenschutzes

Das Ziel der Datenschutz-Grundverordnung ist es, eine einheitliche Anwendung des Rechts in den Europäischen Mitgliedsstaaten zu gewährleisten. Bei grenzüberschreitenden Datenverarbeitungen wurde

für den nicht-öffentlichen Bereich ein Kooperationsverfahren geschaffen, bei dem am Ende eine einheitliche Entscheidung aller beteiligten Datenschutz-Aufsichtsbehörden der europäischen Mitgliedsstaaten vorliegt. Im Rahmen dieses Kooperationsverfahrens arbeiten Datenschutz-Aufsichtsbehörden in der EU künftig enger miteinander, um in grenzüberschreitenden Fällen zu einer gemeinschaftlichen Einigung und Entscheidung zu gelangen. Sollte eine Einigung auf diesem Weg nicht möglich sein, kann mithilfe des Europäischen Datenschutzausschusses im Zuge des sogenannten Kohärenzverfahrens eine Entscheidung gefunden werden.

Bei grenzüberschreitenden, datenschutzrechtlich relevanten Sachverhalten bietet das sogenannte One-Stop-Shop-Verfahren (Art. 56, 60, 63 ff. der Datenschutz-Grundverordnung) eine Vereinfachung dahingehend, dass für Unternehmen nur die Datenschutz-Aufsichtsbehörde am Unternehmenshauptsitz zuständig ist. Das Unternehmen soll somit nicht mit mehreren Aufsichtsbehörden in Kontakt treten müssen. Eine von der Datenverarbeitung betroffene Person hingegen muss nun aber nicht mit der Aufsichtsbehörde am Unternehmenshauptsitz in Kontakt treten, sondern kann ihre Beschwerde über mögliche datenschutzrechtliche Verletzungen auch an die Aufsichtsbehörde ihres Wohnsitzes richten.
Das One-Stop-Shop-Verfahren ist gekennzeichnet durch eine federführende Datenschutz-Aufsichtsbehörde und möglichen betroffenen Datenschutz-Aufsichtsbehörden. Die federführende Aufsichtsbehörde ist die zuständige Aufsichtsbehörde am Sitz der Hauptniederlassung des Unternehmens. Sie fungiert als zentraler Ansprechpartner und kann datenschutzrechtliche Aufsichtsmaßnahmen durchführen. Eine betroffene Aufsichtsbehörde kennzeichnet, dass sich das betreffende Unternehmen entweder im Hoheitsgebiet des Mitgliedsstaats dieser Aufsichtsbehörde niedergelassen hat, die Verarbeitung erhebliche Auswirkungen auf betroffenen Personen mit Wohnsitz im Mitgliedsstaat dieser Aufsichtsbehörde hat oder haben kann oder wenn eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde (Art. 4 Nr. 22 Datenschutz-Grundverordnung). Sobald sich eine Aufsichtsbehörde als „betroffene Aufsichtsbehörde“ meldet, wird sie in dem weiteren Einigungsverfahren mit einbezogen.
Kommt es zwischen der federführenden Aufsichtsbehörde und der bzw. den betroffenen Aufsichtsbehörde(n) zur Einigung über die Vor-

gehensweise gegenüber dem Unternehmen, das die datenschutzrechtliche Verletzung begangen hat, ergeht ein Beschluss an die Hauptniederlassung des Unternehmens. Das Unternehmen hat dann nach Maßgabe des Beschlusses seine Verarbeitungsprozesse in allen EU-Niederlassungen anzupassen und mit der Datenschutz-Grundverordnung in Einklang bringen. Das Unternehmen teilt die getroffenen Maßnahmen der federführenden Aufsichtsbehörde mit. Die federführende Aufsichtsbehörde unterrichtet dann wiederum die betroffenen Aufsichtsbehörden.
Die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, unterrichtet den Beschwerdeführer über den Beschluss. Stellt sich heraus, dass eine Beschwerde unzulässig oder unbegründet ist, erlässt die Aufsichtsbehörde, an die sich der Beschwerdeführer gewandt hat, einen entsprechenden Beschluss. Das betroffene Unternehmen wird anschließend darüber informiert.
Wird keine Einigung zwischen der federführenden und den betroffenen Aufsichtsbehörden erzielt, kommt das sogenannte Kohärenzverfahren (Art. 63 bis 67 der Datenschutz-Grundverordnung) zur Anwendung. Dabei trifft der Europäische Datenschutzausschuss einen verbindlichen Beschluss. Ziel ist es auch hier eine einheitliche Anwendung der Datenschutz-Grundverordnung (DS-GVO) zu gewährleisten. Im Rahmen des Kohärenzverfahrens werden darüber hinaus auch gemeinsame Richtlinien und Stellungnahmen bestimmt.
In Fällen bei denen Unternehmen keine Niederlassungen in der Europäischen Union haben, aber Bürgern der Europäischen Union Waren und Dienstleistungen anbieten, greift nicht das One-Stop-Shop-Verfahren. Unternehmen ohne EU-Niederlassung haben nicht einen einzelnen Ansprechpartner, sondern müssen sich mit jeder Datenschutz-Aufsichtsbehörde in der Europäischen Union auseinandersetzen.
Um eine effektive Zusammenarbeit der Datenschutz-Aufsichtsbehörden in der EU zu fördern, wurde das Binnenmarkt-Informationssystem IMI eingerichtet. Damit wird es EU ansässigen Datenschutz-Aufsichtsbehörden erleichtert, die praktische Umsetzung des EU-Rechts sicherzustellen.
Seit der Einführung von IMI im Mai 2018 prüfte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) in bislang 597 Fällen, ob er betroffene oder federführende Aufsichtsbehörde war. In 62 Fällen hat sich der TLfDI als betroffene Aufsichtsbehörde gesehen. Eine Federführung lag noch nicht vor. Darüber hinaus hat sich der TLfDI bei EU-weiten Abstimmungen von

eingereichten Listen zur Datenschutz-Folgenabschätzung mit Stellungnahmen beteiligt.
Mit Anwendbarkeit der DS-GVO ist spürbar geworden, dass viele Entscheidungen und Abläufe einen immer stärkeren europäischen Kontext aufweisen. Da auch hier zukünftig noch eine Steigerung zu erwarten ist und die Aufgaben des TLfDI dementsprechend zunehmen werden, ist eine Personalaufstockung beim TLfDI auch insoweit angezeigt.

5.11 Positionsbestimmung zum TMG

Seit dem 25. Mai 2018 gilt die Datenschutz-Grundverordnung (DS-GVO). Gleichzeitig sollte eine e-Privacy-Verordnung (ePVO) in Kraft treten. Dies ist bisher nicht erfolgt. Auch das Telemediengesetz (TMG) wurde noch nicht an die DS-GVO angepasst. So gibt es nach wie vor Unstimmigkeiten in der Anwendbarkeit in Bezug auf das TMG. Der TLfDI wird rechtzeitig über neue Erkenntnisse informieren.

Am 4. Mai 2016 wurde die DS-GVO im Amtsblatt der Europäischen Union veröffentlicht. Sie ist seit dem 25. Mai 2018 anzuwenden.
Zeitgleich sollte auch eine neue EU-e-Privacy-Verordnung in Kraft treten, die die gültige EU-e-Privacy-Richtlinie ablösen sollte. Im Entwurf der Europäischen Kommission der EU-e-Privacy-Verordnung (der Verordnung über Privatsphäre und elektronische Kommunikation) vom 10. Januar 2017 hieß es dazu in der Begründung:

„Seit der letzten Überprüfung der e-Datenschutz-Richtlinie im Jahr 2009 haben sich jedoch wichtige technische und wirtschaftliche Entwicklungen auf dem Markt vollzogen. Anstatt herkömmliche Kommunikationsdienste zu nutzen, verlassen sich Verbraucher und Unternehmen zunehmend auf neue Internetdienste, die eine interpersonelle Kommunikation ermöglichen, z. B. VoIP-Telefonie, Sofortnachrichtenübermittlung (Instant-Messaging) und webgestützte E-Mail-Dienste. Solche Over-the-Top-Kommunikationsdienste („OTT-Dienste“) werden aber im Allgemeinen vom gegenwärtigen Rechtsrahmen der Union für die elektronische Kommunikation, einschließlich der e-Datenschutz-Richtlinie, nicht erfasst. Folglich hat die Richtlinie mit der technischen Entwicklung nicht Schritt gehalten, was zu

einem mangelnden Schutz der über solche neuen Dienste abgewickelten Kommunikation führt.“

Weiter wird ausgeführt:

„So hat beispielsweise die Einwilligungsvorschrift zum Schutz der Vertraulichkeit von Endeinrichtungen ihr Ziel verfehlt, denn Endnutzer werden aufgefordert, Verfolgungs-Cookies (Tracking-Cookies) zu akzeptieren, ohne dass sie deren Sinn verstehen, und in einigen Fällen werden Cookies sogar ohne ihre Einwilligung gespeichert. Die Einwilligungsvorschrift ist einerseits zu umfassend, weil sie auch Verfahren einschließt, die gar keine Gefahr für die Privatsphäre darstellen, und andererseits zu eng, weil sie einige Verfolgungstechniken (z. B. Verfolgung von Gerätekennungen), die ohne Zugriff/Speicherung im Gerät auskommen, nicht erfasst. Schließlich kann auch ihre Umsetzung für Unternehmen teuer sein.“

So sieht der Entwurf der EU-Kommission einer EU-e-Privacy-Verordnung vor, dass die Einwilligung für Cookies nach Art. 8 Abs. 1 Buchstabe b) auch schon in den passenden technischen Einstellungen einer Software, die den Zugang zum Internet ermöglicht, gegeben werden kann (Art. 9 Abs. 2). Ein denkbares Beispiel wäre z. B. eine Browsereinstellung für die Speicherung eines Warenkorbs beim Online-Shopping.
Im Entwurf der EU-Kommission wird in den Erwägungsgründen 23 und 24 allerdings auch kritisiert, dass die meisten weitverbreiteten Browser für Cookies die Standardeinstellung „Alle Cookies annehmen“ anbieten. Damit werden nicht nur Cookies vom Webseitenbetreiber selbst, sondern auch von Dritten ohne zusätzliche Einwilligung gesetzt, deren Dienste/Inhalte auf der Webseite eingebettet sind. Deshalb sollten Anbieter von Software, die das Abrufen und Darstellen von Informationen aus dem Internet erlauben, dazu verpflichtet sein, die Software so zu konfigurieren, dass sie die Möglichkeit bietet, zu verhindern, dass Dritte Informationen in der Endeinrichtung speichern. Entsprechend dem Erwägungsgrund 22 des Entwurfs sind als Endeinrichtungen z. B. Smartphones, Tablets oder Computer gemeint. Diese Einstellung, zu verhindern, dass Dritte Informationen in der Endeinrichtung speichern, wird häufig als „Cookies von Drittanbietern zurückweisen“ bezeichnet. Den Endnutzern sollte im Ergebnis

also eine Reihe von Einstellungsmöglichkeiten zur Privatsphäre angeboten werden, die vom höheren Schutz (z. B. „Cookies niemals annehmen“) über einen mittleren Schutz (z. B. „Cookies von Drittanbietern zurückweisen“ oder „Nur Cookies von Erstanbietern annehmen“) bis zum niedrigeren Schutz (z. B. „Cookies immer annehmen“) reicht. Solche Einstellungen zur Privatsphäre sollten in leicht sichtbarer und verständlicher Weise dargestellt werden, so die Forderung.
Ansonsten geht der Entwurf der e-Privacy-Verordnung, wie auch schon davor die e-Privacy-Richtlinie, davon aus, dass eine Einwilligung des Nutzers notwendig sei, also ein sogenanntes Opt-In zu erfolgen hat. Die Regelungen des derzeit gültigen Telekommunikationsgesetzes sehen aber immer ein Opt-Out vor, was bedeutet, dass der Nutzer nicht einwilligen muss, sondern widersprechen kann, wenn es um die Verarbeitung seiner personenbezogenen Daten geht.
Mehrfach hatte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) auf die Problematik in dieser Frage hingewiesen.
Die DSK hat deshalb am 26. April 2018 ein entsprechendes Positionspapier veröffentlicht und darauf hingewiesen, dass sich mit der Verzögerung des Gesetzgebungsverfahrens zur e-Privacy-Verordnung Fragen zur Anwendbarkeit des nationalen Rechts im Kontext der DS-GVO ergeben (siehe https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf). So habe der Gesetzgeber das TMG bisher nicht an die DS-GVO angepasst. Wegen des Anwendungsvorrangs der DS-GVO stelle sich juristisch daher die Frage, ob die datenschutzrechtlichen Regelungen des TMG weiterhin anwendbar seien.

Die DSK vertritt diesbezüglich die Auffassung, dass z. B. die §§ 12, 13, 15 TMG bei der Beurteilung der Rechtmäßigkeit von Reichweitenmessungen und des Einsatzes von Tracking-Mechanismen, die das Verhalten betroffener Personen im Internet nachvollziehbar machen, ab dem 25. Mai 2018 nicht mehr angewendet werden dürfen. Es bedarf jedenfalls beim Einsatz von Tracking-Mechanismen, die das Verhalten von

betroffenen Personen im Internet nachvollziehbar machen sowie bei der Erstellung von Nutzerprofilen einer vorherigen Einwilligung.
Das bedeutet, dass eine informierte Einwilligung im Sinne der DS-GVO, in Form einer Erklärung oder sonstigen eindeutig bestätigenden Handlung, vor der Datenverarbeitung eingeholt werden muss, also noch bevor Cookies platziert oder auf dem Endgerät des Nutzers gespeicherte Informationen gesammelt werden.
Das Positionspapier der DSK fand in der Öffentlichkeit große Resonanz, die allerdings nicht ungeteilt war. So hat beispielsweise der Bundesverband des Digitalverbands Deutschlands (Bitkom e. V.), der mehr als 2.600 Unternehmen der digitalen Gesellschaft vertritt, seine eigene Sichtweise zum Positionspapier der DSK veröffentlicht.
Eine Unterarbeitsgruppe der DSK befasst sich derzeit erneut mit dem Thema „Positionsbestimmung TMG“. Ziel ist es, in einem Konsultationsverfahren den jeweiligen Verbänden die Gelegenheit zu bieten, mit den Aufsichtsbehörden die dargelegten Auffassungen vertieft zu erörtern. Der TLfDI wird rechtzeitig informieren, sobald es aus Sicht des Datenschutzes neue Forderungen oder Erkenntnisse gibt.

5.12 Verantwortliche Stellen: Bestellung eines Datenschutzbeauftragten im Betriebs- und Personalrat?

Aufgrund der Anwendbarkeit der DS-GVO haben auch Personalräte in öffentlichen Stellen einen Datenschutzbeauftragten zu bestellen, Betriebsräte in Unternehmen nur dann, wenn es sich um einen Betrieb handelt, der mehr als 401 Arbeitnehmer beschäftigt.

Nach der Anwendbarkeit der Europäischen Datenschutz-Grundverordnung (DS-GVO) erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) einige Anfragen, ob der Personalrat öffentlicher Stellen oder der Betriebsrat eines Thüringer Unternehmens eigene Datenschutzbeauftragte bestellen müsse.
Mit der neuen Rechtslage ist nicht eindeutig festgelegt, ob Betriebs- und Personalräte als eigenständige Verantwortliche im Sinne der DS-GVO anzusehen sind. Sowohl für die eigene Verantwortlichkeit im Sinne der DS-GVO als auch für die Betrachtung der Vertretung als Teil des Arbeitsgebers finden sich gute Argumente, denn nach der DS-GVO können auch „andere Stellen“ Verantwortliche sein (Art. 4 Nr. 7 DS-GVO).

Personalräte und Betriebsräte sind nach Auffassung des TLfDI und einiger anderer Datenschutzaufsichtsbehörden in Deutschland verantwortliche Stellen nach Art. 4 Nr. 7 DS-GVO, weil sie aufgrund ihrer Stellung nach den Vorschriften des Personalvertretungsgesetztes beziehungsweise des Betriebsverfassungsgesetzes grundsätzlich allein über die gesetzlich vorgesehenen Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheiden. Auch nach altem Recht waren sie selbst für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich, wofür ihnen die dafür erforderliche Ausstattung zur Verfügung zu stellen war.

Die Pflicht zur Bestellung eines Datenschutzbeauftragten kann sich aus der DS-GVO oder dem nationalen Recht ergeben. Nach Art. 37 Abs. 1 DS-GVO ist auf jeden Fall ein Datenschutzbeauftragter zu benennen, wenn:

- die Verarbeitung von einer Behörde oder öffentlichen Stellen durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeiten handeln,
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, die aufgrund ihrer Art, ihres Umfangs und ihrer Zwecke eine umfangreiche, regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen oder
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 bestehen.

Weitere Ausführungen hierzu enthält das Kurzpapier der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder Nummer 12, dass unter https://www.tlfdi.de/mam/tlfdi/gesetze/dsk_kpnr_12_datenschutzbeauftragter.pdf abgerufen werden kann.

Im Ergebnis und auch aufgrund § 13 Thüringer Datenschutzgesetz (neu) müssen öffentliche Stellen einen Datenschutzbeauftragten bestellen. Nach Kenntnis des TLfDI vertreten mittlerweile mehrere bundesdeutsche Datenschutzaufsichtsbehörden die Rechtsauffassung, dass die Personalvertretung einer Dienststelle unter den Begriff des

Verantwortlichen im Sinn von Art. 4 Nr. 7 DS-GVO fällt. Begründet werden kann dies unter anderem durch Verweis auf § 68 Abs. 2 Satz 3 Thüringer Personalvertretungsgesetz (ThürPersVG). Demzufolge hat die Personalvertretung auch einen eigenen Datenschutzbeauftragten zu bestellen. Daher wäre aus Sicht des TLfDI einerseits der Regelungsgehalt des § 80 Abs. 1 ThürPersVG, nach dem die Personalvertretung verpflichtet ist, die Vorschriften über den Datenschutz einzuhalten und sich für deren Wahrung in der Dienststelle einzusetzen, entsprechend zu ergänzen. Damit jedoch der Personalvertretung andererseits keine „überbordenden" rechtlichen oder tatsächlichen Hürden bei der Besetzung des Amtes ihres (eigenen) Datenschutzbeauftragten auferlegt werden, sollte die gesetzliche Möglichkeit eingeräumt werden, dass der behördliche Datenschutzbeauftragte der Dienststelle in Personalunion auch das Amt des Datenschutzbeauftragten der Personalvertretung übernimmt, wenn dazu Einvernehmen zwischen Dienststelle und Personalvertretung besteht.
Der TLfDI hat daher im Rahmen seiner Stellungnahme an den Thüringer Landtag zur Änderung der personalvertretungsrechtlichen Vorschriften einen entsprechenden Änderungsvorschlag zu § 80 ThürPersVG unterbreitet.
Datenschutzbeauftragte in Unternehmen sind nach dem vom Bundesgesetzgeber genutzten Regelungsspielraum nach § 38 BDSG - zu bestellen, wenn:

- in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind oder
- Verarbeitungen vorgenommen werden, die einer Datenschutzfolgenabschätzung nach Art. 35 DS-GVO unterliegen oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt oder Meinungsforschung verarbeitet werden. In diesem Fall muss unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen ein DSB benannt werden.

Nach § 9 Betriebsverfassungsgesetz besteht der Betriebsrat ab 401 Arbeitnehmern aus 11 Mitgliedern. Trifft dies in einem Betrieb zu, ist zwingend ein Datenschutzbeauftragter auch für den Betriebsrat zu bestellen, wenn mindestens zehn Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

5.13 Europäischer Gerichtshof entscheidet, Fanpage-Betreiber sind auch gemeinsam mit Facebook verantwortlich für Datenverarbeitung

Der Europäische Gerichtshof (EuGH) hat in seinem Urteil vom 5. Juni 2018 die gemeinsame Verantwortung von Facebook und Fanpage-Betreibern bestätigt (EuGH C-210/16). Fanpage-Betreiber müssen künftig transparent darüber informieren, welche Daten zu welchem Zweck durch Facebook und die Fanpage-Betreiber verarbeitet werden.

Die Frage nach der Mitverantwortung von Betreibern von Facebook Fanpages beschäftigt seit vielen Jahren die Europäischen Gerichte. Selbst das Bundesverwaltungsgericht, das sich in einem Rechtsstreit damit befassen musste, setzte das Verfahren aus und richtete im Februar 2016 sechs Fragen zur Vorabentscheidung an den Europäischen Gerichtshof (EuGH). Auch der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) berichtete mehrfach darüber.
Dabei galt es unter anderem zu klären, inwiefern die Verantwortung von Betreibern einer Fanpage auf Facebook bei datenschutzrechtlichen Verstößen festzustellen ist. Im konkreten Fall ging es darum, dass Facebook mithilfe von Cookies Daten von Nutzern einer solchen Fanpage sammele ohne auf die Speicherung und Funktionsweise von angewendeten Cookies bzw. auf die nachfolgende Datenverarbeitung transparent hinzuweisen.
Der EuGH kam zum Ergebnis, dass der Betreiber einer auf Facebook unterhaltenen Fanpage zur Verarbeitung der personenbezogenen Daten der Besucher seiner Seite beiträgt und somit im vorliegenden Fall gemeinsam mit Facebook für diese Verarbeitung als Verantwortlicher einzustufen ist. Der Umstand, dass ein Betreiber einer Fanpage die 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.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder begrüßten das Urteil in ihrer Entschließung

vom 6. Juni 2018 (https://www.tlfdi.de/mam/tlfdi/datenschutz/entschliessungen/zwischenKonferenzen/entschliessung_dsk_fanpages_eugh_urteil_05_06_2018.pdf).

Das Urteil des EuGHs zur gemeinsamen Verantwortung von Facebook und den Betreibern einer Fanpage hat unmittelbare Auswirkungen auf die Seitenbetreiber. Diese können nicht mehr allein auf die datenschutzrechtliche Verantwortung von Facebook verweisen, sondern sind selbst mitverantwortlich für die Einhaltung des Datenschutzes gegenüber den Nutzenden ihrer Fanpage.

Weiterhin müssen Fanpagebetreiber nun Folgendes beachten:

- 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 trackt, 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 DS-GVO erfüllt.
- Für die Bereiche der gemeinsamen Verantwortung von Facebook und Fanpage-Betreibern ist in einer Vereinbarung festzulegen, wer von ihnen welche Verpflichtung der DS-GVO erfüllt. Diese Vereinbarung muss in wesentlichen Punkten den Betroffenen zur Verfügung gestellt werden, damit diese ihre Betroffenenrechte wahrnehmen können.

Gegenüber Thüringer Behörden positionierte sich der TLfDI wie folgt:

Sie werden daher gebeten zu prüfen, ob Sie die Informationspflichten nach der DS-GVO in Bezug auf die Fanpage gegenüber den betroffe-

nen Personen erfüllen können. 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.
Daher müssen Sie dafür sorgen, dass Facebook ihnen die Informationen zur Verfügung stellt, die zur Erfüllung der genannten Informationspflichten benötigt werden. Dies betrifft alle in Art. 13 DS-GVO genannten Informationen. Auch muss mit Facebook eine Vereinbarung nach Art. 26 DS-GVO geschlossen werden.
Angesichts der sehr deutlichen Entscheidung des EUGH rate ich dazu, die Fanpage zu deaktivieren. Sofern Sie davon Abstand nehmen, sollten Sie zumindest an den Verantwortlichen herantreten, um die nach Art. 13 DS-GVO erforderlichen Informationen zu erlangen und die nach Art. 26 DS-GVO notwendige Vereinbarung schließen zu können.
Der TLfDI ist im Dialog mit Thüringer Behörden, um die Anforderungen der DS-GVO an die gemeinsame Verantwortlichkeit umzusetzen. Er wird über die Ergebnisse berichten.

5.14 Betroffenenrechte nach der Datenschutz-Grundverordnung

Die DS-GVO stärkt die Rechte der von der Datenverarbeitung betroffenen Personen ganz maßgeblich. Sie enthält ein Zusammenspiel aus bereits bekannten und auch aus neuen Rechten, die im Folgenden dargestellt werden.

Das Kapitel III der Datenschutz-Grundverordnung (DS-GVO) enthält die „Rechte der betroffenen Personen“. Eines der wesentlichen Ziele bei der Neuregelung des europäischen Datenschutzrechts war der Ausbau der Betroffenenrechte. Es handelt sich dabei um Rechte, die die betroffenen Personen gegenüber dem für die Verarbeitung Verantwortlichen geltend machen können.

I. Grundsätzliches

Art. 12 DG-GVO regelt zunächst grundsätzlich die Modalitäten für die Ausübung der Rechte betroffener Personen. Diese Rahmenregelungen gelten für alle Betroffenenrechte. Art. 12 DS-GVO enthält

zum einen allgemeine Transparenzregeln und zum anderen Verfahrensregeln zu den Betroffenenrechten.
Zunächst wird klargestellt, dass alle Informationen, die sich auf die Verarbeitung beziehen, in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ zur Verfügung gestellt werden müssen. Der Grundsatz der Transparenz (Art. 5 Abs. 1 Buchstabe a) DS-GVO) setzt voraus, dass die von der Datenverarbeitung Betroffenen verstehen, wer auf welche Weise und zu welchem Zweck ihre Daten verarbeitet. Dies stellt die Verantwortlichen vor große Schwierigkeiten, denn komplexe Datenverarbeitungssysteme lassen sich oftmals nicht mit einigen knappen Worten erklären.
Der Verantwortliche ist verpflichtet, den betroffenen Personen die Ausübung ihrer Rechte so leicht wie möglich zu machen, Art. 12 Abs. 2 DS-GVO. Er muss nur dann nicht tätig werden, wenn er tatsächlich nicht in der Lage ist, die betreffende Person, die den Antrag stellt, zu identifizieren. Der Betroffene hat grundsätzlich einen Anspruch darauf, innerhalb eines Monats nach Eingang seiner Anträge, vom Verantwortlichen eine Antwort zu erhalten. Diese Frist kann maximal um zwei weitere Monate verlängert werden, wenn es sich um sehr schwierige Sachverhalte handelt. Wird der Verantwortliche innerhalb der genannten Frist nicht tätig, muss er innerhalb eines Monats nach Eingang des Antrags Gründe dafür mitteilen und auch über die Möglichkeit informieren, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen. Alle Mitteilungen und Maßnahmen müssen durch den Verantwortlichen unentgeltlich zur Verfügung gestellt werden. Allenfalls bei exzessiven Anträgen kann ein angemessenes Entgelt verlangt werden. In derartigen Fällten kann der Verantwortliche sich auch weigern, tätig zu werden. Er hat aber den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.
Eine wesentliche Neuerung des Datenschutzrechts stellen die Informationspflichten des Art. 13 und 14 DS-GVO dar. Streng genommen handelt es sich bei ihnen nicht um Rechte der betroffenen Personen, sondern um Pflichten des Verantwortlichen. Da sie aber der Information des Verantwortlichen dienen, damit dieser seine Rechte angemessen ausüben kann, stellen sie mittelbar gleichwohl wichtige Rechte des Betroffenen dar.

II. Informationspflichten

Art. 13 DS-GVO verpflichtet Verantwortliche, bestimmte Informationen zur Datenverarbeitung von betroffenen Personen aktiv, das heißt ohne besondere Aufforderung, zur Verfügung zu stellen. Diese Informationspflicht besteht, wenn der Verantwortliche personenbezogene Daten bei der betroffenen Person erhebt oder wenn er beabsichtigt, die erhobenen Daten zu einem anderen Zweck als den Erhebungszweck weiter zu verarbeiten. Die Informationen, die der Verantwortliche geben muss, sind in Art. 13 Abs. 1 Buchstabe a) bis f) aufgezählt. Es handelt sich um sehr vielfältige und umfassende Informationen zur Datenverarbeitung:

- den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters
- gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
- gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln.

Da diese andererseits in einer einfachen und leicht verständlichen Sprache gegeben werden müssen (vergleiche Art. 12 DS-GVO), stellt diese Regelung eine große Herausforderung in der Praxis dar.

Eine Informationspflicht besteht auch, wenn der Verantwortliche die Information nicht bei der betroffenen Person selbst erhebt, sondern wenn die Daten auf eine andere Weise, beispielsweise bei einer anderen Person, erhoben werden. Das gilt auch für den Fall, dass die Daten dem Verantwortlichen übermittelt werden. Hier enthält Art. 14 Abs. 1 Buchstabe a) bis f) DS-GVO einen umfangreichen Katalog der Informationen, die der betroffenen Person gegeben werden müssen. Diese Informationen entsprechen den nach Art 13 DS-GVO zu übermittelnden Daten. Zusätzlich sind nach Abs. 2 der Bestimmung folgende Informationen zur Verfügung zu stellen:

- die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer
- wenn die Verarbeitung auf Art. 6 Abs. 1 Buchstabe f) beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden

- das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie ein Recht auf Berichtigung, Löschung, auf Einschränkung der Verarbeitung, ein Widerspruchsrecht gegen die Verarbeitung sowie das Recht auf Datenübertragbarkeit
- wenn die Verarbeitung auf Art. 6 Abs. 1 Buchstabe a) oder Art. 9 Abs. 2 Buchstabe a) beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4.

Ausnahmen bestehen dann, wenn die betreffende Person bereits über die Information verfügt oder die Erteilung dieser Informationen sich als unmöglich erweist und einen unverhältnismäßigen Aufwand erfordern würde. Letzteres Kriterium ist allerdings sehr eng auszulegen, um den Schutz der Betroffenen hinreichend zu gewährleisten. Eine Ausnahme besteht auch dann, wenn die personenbezogenen Daten dem Berufsgeheimnis oder einer sonstigen Geheimhaltungspflicht unterliegen und vertraulich behandelt werden müssen.

III. Auskunftsanspruch

Um sicherzustellen, dass die betroffenen Personen auch alle Informationen erhalten, die sie benötigen, ergänzt Art. 15 DS-GVO mit dem Auskunftsrecht der betroffenen Person die Informationspflichten. Nach dieser Bestimmung besteht ein allgemeiner Auskunftsanspruch über verarbeitete personenbezogene Daten und bestimmte Metadaten zu dieser Datenverarbeitung. Der Anspruch ist grundsätzlich voraussetzungslos. Der betroffenen Person muss mitgeteilt werden, ob überhaupt Daten über sie verarbeitet werden. Sofern dies nicht der Fall ist, muss eine Negativauskunft erteilt werden. Weiterhin müssen die Verarbeitungszwecke genannt werden und die Kategorien der personenbezogenen Daten, die verarbeitet werden. Auch Empfänger und Kategorien von Empfängern sind den Betroffenen mitzuteilen sowie – falls

möglich – die geplante Speicherdauer. Darüber hinaus muss der Betroffene über seine Rechte aufgeklärt werden sowie gegebenenfalls über die Herkunft seiner personenbezogenen Daten.
Eine wichtige Bestimmung ist die neue Regelung über das Profiling. Wenn es eine automatisierte Entscheidungsfindung beim Verarbeiter gibt, muss nicht nur über diese Tatsache informiert werden, sondern auch eine aussagekräftige Information darüber gegeben werden, welche Logik hinter der Entscheidung liegt, Art. 14 Abs. 2 Buchstabe g) DS-GVO.

IV. Berichtigung

Wie bisher haben betroffene Person das Recht, vom Verantwortlichen eine Berichtigung ihrer personenbezogenen Daten zu verlangen, wenn diese unrichtig sind. Dies entspricht dem Grundsatz der Datenrichtigkeit in Art. 5 Abs. 1 Buchstabe d) DS-GVO. Der Anspruch betrifft allerdings nur Daten, die objektiv oder unbestritten unrichtig sind, beispielsweise, weil ein Name falsch geschrieben wurde oder ein Wohnort nicht stimmt. Wenn Streit über die Richtigkeit eines bestimmten Datums besteht, führt dies nicht automatisch zum Berichtigungsanspruch.

V. Löschung

Auch im bisherigen Recht gab es das Recht auf Löschung. Die neue Regelung in Art. 17 DS-GVO ist jedoch weitergehend. Der Anspruch richtet sich auf unverzügliche Löschung der betreffenden Daten. Grundsätzlich muss in folgenden Fällen gelöscht werden:

- bei Wegfall der Notwendigkeit der Zweckerfüllung
- beim Widerruf einer Einwilligung
- beim Widerspruch gegen die Verarbeitung
- bei ihrer Unrechtmäßigkeit
- bei einer Rechtspflicht zur Löschung
- oder bei der Erhebung personenbezogener Daten eines Kindes in Bezug auf angebotene Internetdienste.

Dieser grundsätzlichen Löschpflicht stehen fünf Ausnahmen in Art. 17 Abs. 3 DS-GVO gegenüber. Nicht zu löschen ist, wenn:

- die Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung erforderlich ist,
- wenn die Verarbeitung zur Erfüllung einer Rechtspflicht oder Erfüllung öffentlicher Aufgaben dient (z. B., wenn bereichsspezifische Aufbewahrungspflichten bestehen),

- wenn es ein öffentliches Interesse an der Verarbeitung im Bereich der öffentlichen Gesundheit geht,
- wenn die Verarbeitung zu Archivzwecken, Forschungszwecken und statistischen Zwecken oder für die Geltendmachung und Ausübung von Rechtsansprüchen erforderlich ist.

Eine Löschung muss aber nicht nur auf Antrag der betroffenen Person erfolgen. Nach Art. 17 DS-GVO ist der Verantwortliche auch zur Löschung verpflichtet, wenn die gesetzlichen Voraussetzungen erfüllt sind. Nach § 35 Bundesdatenschutzgesetz kann von einer Löschung abgesehen werden, wenn sie bei automatisierten Datenverarbeitung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist und das Interesse der betroffenen Person an der Löschung als gering anzusehen ist. Es wird im Einzelfall jeweils zu prüfen sein, ob diese Bestimmung europarechtskonform ist.
Die Überschrift zu der Vorschrift des Art. 17 DS-GVO trägt auch den Zusatz „Recht auf Vergessenwerden“. Dies hat den Hintergrund, dass das Internet eigentlich nichts vergisst und der betroffenen Person gleichwohl die Möglichkeit gegeben werden soll, dafür zu sorgen, dass bestimmte Daten nun „vergessen werden“ können. Um dem Recht auf Vergessenwerden im Netz mehr Geltung zu verschaffen wurde der Verantwortliche, der die personenbezogenen Daten öffentlich gemacht hat, verpflichtet, die Löschpflicht allen Empfängern mitzuteilen. Dass tatsächlich im world-wide-web alle zu löschenden Daten erfasst werden, ist allerdings unrealistisch. Aber immerhin.

VI. Einschränkung der Verarbeitung

Art. 18 DS-GVO regelt das Recht auf Einschränkung der Verarbeitung. Begrifflich entspricht die Einschränkung der Verarbeitung der bisher bekannten „Sperrung“. Es geht dabei darum, dass Daten zwar nicht gelöscht, aber auch nicht mehr anderweitig verarbeitet werden sollen. Dieses Recht hat die betroffene Person in vier Fallkonstellationen:

- wenn die Richtigkeit der Daten bestritten wird, ihre Unrichtigkeit aber nicht bewiesen ist,
- wenn die Verarbeitung unrechtmäßig ist und die betroffene Person nach der Einschränkung der Verarbeitung die Löschung ablehnt,

- wenn die Daten vom Verantwortlichen nicht mehr benötigt werden, die betroffene Person sie aber zur Verfolgung von Rechtsansprüchen benötigt, sind die Daten nicht zu löschen, sondern in der Verarbeitung einzuschränken,
- wenn die betroffene Person Widerspruch gegen die Verarbeitung nach Art. 21 Abs. 1 DS-GVO eingelegt hat. Nach der Einschränkung der Verarbeitung dürfen die Daten nur noch mit Einwilligung der betroffenen Person verarbeitet werden oder soweit dies zur Verfolgung von Rechtsansprüchen erforderlich ist oder aus Gründen eines wichtigen öffentlichen Interesses.

Korrespondierend zur Regelung der Berichtigung, Löschung oder Einschränkung der Verarbeitung postuliert Art. 19 DS-GVO die Pflicht des Verantwortlichen, allen Empfängern personenbezogener Daten offenzulegen, dass es eine Löschung, Berichtigung oder Einschränkung der Verarbeitung dieser personenbezogenen Daten gegeben hat. Diese Pflicht entfällt nur, wenn sie unmöglich ist oder mit einem unverhältnismäßig hohen Aufwand verbunden ist. Die betroffene Person ist über die Empfänger dieser Mitteilungen zu unterrichten.

VII. Datenübertragbarkeit (Portabilität)

Neu ist das Recht auf Datenübertragbarkeit in Art. 20 DS-GVO. Dieses Recht soll der betroffenen Person eine bessere Kontrolle über die eigenen Daten ermöglichen. Betroffene sind demnach berechtigt, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt haben, in einem strukturierten, gängigen maschinenlesbaren und interoperablen Format zu erhalten und sie anderen Verantwortlichen zu übermitteln. Der Anspruch richtet sich nur auf solche Daten, die die betroffene Person selbst bereitgestellt hat. Außerdem gilt der Anspruch nur im Fall einer Einwilligung, wenn die Verarbeitung mit Hilfe automatisierter Verfahren erfolgt. Der Anspruch ist ausgeschlossen, wenn für die Verarbeitung die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt. Allerdings besteht dieser Anspruch nur, soweit dies technisch machbar ist, Art. 20 Abs. 2 DS-GVO. Nach Erwägungsgrund 68 sollte der Verantwortliche durch diese Regelung dazu aufgefordert werden, interoperable Formate zu entwickeln, die die Datenübertragbarkeit ermöglichen. Es wird sicherlich noch einige Zeit brauchen, bis alle Datenverarbeitungssysteme eine derartige Datenübertragbarkeit ermöglichen.

VIII. Widerspruch gegen die Datenverarbeitung

Art. 21 DS-GVO gibt der betroffenen Person das Recht, jederzeit der Verarbeitung sie betreffender, personenbezogener Daten zu widersprechen. Der Widerspruch ist nur gegen Verarbeitungen möglich, die aufgrund des Art. 6 Abs. 1 Satz 1 Buchstabe e) oder f) erfolgen. Dies betrifft Fälle, in denen die Wahrnehmung einer dem Verantwortlichen übertragenen Aufgabe die Datenverarbeitung erfordert, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, oder, im Bereich der nicht-öffentlichen Stellen, die Aufgabe der Datenverarbeitung zur Wahrung berechtigter Interessen dient. Dies bedeutet allerdings nicht, dass die betroffene Person es immer in der Hand hat, ob ein Verantwortlicher ihre Daten verarbeiten darf oder nicht. Die Ausübung des Widerspruchsrechts setzt voraus, dass die betroffene Person Gründe geltend machen kann, die sich aus ihrer besonderen Situation ergeben. Es muss daher im Fall der betroffenen Person eine atypische Konstellation vorliegen, bei der ihren Interessen besonderes Gewicht beigemessen werden muss. Die Folge der Ausübung eines berechtigten Widerspruchs ist, dass die entsprechende Verarbeitung zu beenden ist. Der Verantwortliche kann gegen den Widerspruch zwingende, schutzwürdige Gründe für die Verarbeitung geltend machen und wenn diese die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen oder die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient, ist die Verarbeitung gleichwohl rechtmäßig.

IX. Profiling

Die Regelung in Art. 22 DS-GVO „Automatisierte Entscheidung im Einzelfall einschließlich Profiling“ soll den Einzelnen davor schützen, dass eine ihn betreffende Entscheidung allein auf Grundlage einer automatisierten Bewertung seiner Persönlichkeitsmerkmale ergeht. Die Regelung gibt der betroffenen Person das Recht, dass Entscheidungen, die für sie eine rechtliche Wirkung entfalten, oder sie in ähnlicher Weise erheblich beeinträchtigen, nicht ausschließlich aufgrund einer automatisierten Datenverarbeitung getroffen werden. Dieses Verbot gilt allerdings dann nicht, wenn die Entscheidung für den Abschluss oder die Erfüllung eines Vertrages erforderlich ist, sie aufgrund einer besonderen Rechtsvorschrift zulässig ist oder wenn die betroffene Person ausdrücklich eingewilligt hat.

X. Recht auf Beschwerde

Ein weiteres Betroffenenrecht ist schließlich das Recht auf Beschwerde nach Art. 77 DS-GVO. Danach kann sich jede betroffene Person an eine Aufsichtsbehörde in dem Mitgliedsstaat ihres persönlichen Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes wenden, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DS-GVO verstößt. Die Aufsichtsbehörde wiederum ist verpflichtet, einer Beschwerde angemessen nachzugehen und den Beschwerdeführer binnen drei Monaten über das Ergebnis oder zumindest den Zwischenstand ihrer Prüfung zu informieren. Kommt die Aufsichtsbehörde dieser Pflicht nicht nach, kann der Beschwerdeführer Klage gegen die Aufsichtsbehörde einreichen. Dies gilt selbstverständlich auch, wenn er mit dem Ergebnis der Prüfung der Aufsichtsbehörde nicht einverstanden ist. Dieses Beschwerderecht bei der Aufsichtsbehörde steht neben den anderen Rechten, etwa der Möglichkeit, gerichtlich gegen Verantwortliche und Auftragsverarbeiter vorzugehen oder Schadenersatz zu verlangen bzw. Strafantrag zu stellen.

XI. Was kann der Einzelne sonst noch tun?

Die Preisgabe personenbezogener Daten stellt für die Betroffenen immer ein gewisses Risiko dar. Dies gilt ganz besonders, wenn diese Daten digital erfasst und verarbeitet werden. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat Hinweise zur „digitalen Selbstverteidigung“ erarbeitet, die Sie unter https://www.tlfdi.de/mam/tlfdi/info/digitale_selbstverteidigung_05-2018_web.pdf finden. Dort werden Sie nach kurzen Hinweisen auf die Gefahrenlagen mit Tipps versorgt, wie Sie Ihren digitalen Schutz erhöhen können. Mit dort enthaltenen weiterführenden Links können Sie sich tiefgreifender informieren. Die Broschüre ist auch in Anhang dieses Berichtes zu finden.

Fazit:

Insgesamt enthalten die Regelungen zu den Betroffenenrechten in der DS-GVO Bekanntes. Die Rechte auf Auskunft und Löschung wurden inhaltlich erweitert und das gesamte Verfahren wurde in formeller

Hinsicht konkretisiert. Gänzlich neu ist das Recht auf Datenübertragbarkeit. Die Anforderungen an Inhalt und Form der zu gebenden Informationen sind in der DS-GVO deutlich strenger gestaltet. Damit bringen die neuen Transparenz- und Informationsvorschriften spürbare Unterschiede zum bisher geltenden Recht mit sich und verbessern den Schutz des Grundrechts der informationellen Selbstbestimmung.

5.15 Informationspflichten für Verantwortliche – Nachweis durch Unterschrift?

Die Informationspflicht nach Art. 13 der Datenschutz-Grundverordnung (DS-GVO) dient der Erfüllung des Grundsatzes einer transparenten Verarbeitung von personenbezogenen Daten. Sie besteht grundsätzlich dann, wenn der Verantwortliche personenbezogene Daten direkt bei der betroffenen Person erhebt. Eine Pflicht zur Gegenzeichnung für den Erhalt der Informationspflichten durch den Betroffenen sieht die Datenschutz-Grundverordnung jedoch nicht vor.

Gerade nach Wirksamwerden der DS-GVO kam es beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zu vielen Nachfragen hinsichtlich der Umsetzung der DS-GVO. Insbesondere die Informationspflichten sorgten für eine hohe Anfragezahl.
So erreichte den TLfDI unter anderem die Frage, ob sich die verantwortliche Stelle den Erhalt der Informationen nach Art. 13 der DS-GVO von der betroffenen Person gegenzeichnen lassen muss.
Art. 5 Abs. 2 der DS-GVO normiert die Rechenschaftspflicht des Verantwortlichen. Zum einen hat der Verantwortliche für die Einhaltung der Grundsätze des Art. 5 Abs. 1 der DS-GVO zu sorgen. Zum anderen muss der Verantwortliche die Einhaltung der Grundsätze nach Art. 5 Abs. 1 DS-GVO nachweisen können. Zu den in Art. 5 Abs. 1 Buchstabe a) DS-GVO aufgeführten Grundsätzen zählt auch die Transparenzverpflichtung, die durch die Bereitstellung der Informationen nach Art. 13 DS-GVO abgedeckt wird. Art. 5 Abs. 2 DS-GVO schreibt nicht vor, in welcher Form der Nachweis erfüllt werden muss. Eine Gegenzeichnung ist somit nicht zwingend. Es sollte jedoch zumindest eine (schriftliche) Dokumentation erfolgen aus der, zu Nachweiszwecken hervorgeht, dass die Informationsplichten erfüllt wurden.

5.16 Benennung eines Datenschutzbeauftragten (DSB): Voraussetzungen und Anforderungen an den Beauftragten für den Datenschutz

Datenschutzbeauftragte werden auf Grundlage des Art. 37 Abs. 1 der Datenschutz-Grundverordnung (DS-GVO) und des § 38 Bundesdatenschutzgesetz (BDSG) benannt. Zum Datenschutzbeauftragten (DSB) können Mitarbeiter des Verantwortlichen oder externe Fachkräfte benannt werden. Dabei darf kein Interessenskonflikt bestehen. Die Kontaktdaten des DSB müssen dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) schriftlich gemeldet werden.

Die Benennungsvoraussetzungen für Datenschutzbeauftragte finden sich in Art. 37 Abs. 1 der DS-GVO. Darüber hinaus hat sich der Gesetzgeber entschlossen im Rahmen einer Öffnungsklausel, nationale Regelungen zum DSB zu erlassen. Daher ist neben den Regelungen der DS-GVO bei der Beurteilung, ob eine Benennungspflicht besteht, auch § 38 BDSG zu beachten.
Der Verantwortliche und der Auftragsverarbeiter müssen nach Art. 37 Abs. 1 Buchstabe b) und c) DS-GVO auf jeden Fall einen DSB benennen, wenn die Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, die aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche, regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen oder die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 der DS-GVO besteht.

I. Besondere Kategorien und die Verarbeitung sensibler Daten

Zu den besonderen Kategorien von Daten zählen gemäß Art. 9 Abs. 1 der DS-GVO in Verbindung mit Art. 4 Nr. 15 der DS-GVO auch sensible bzw. sensitive Daten in Form von Gesundheitsdaten. Gemäß Art. 4 Nr. 15 der DS-GVO sind „Gesundheitsdaten personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“.

Verantwortliche sowie Auftragsverarbeiter im Gesundheitsbereich (z. B. Ärzte oder Apotheker) müssen nach Art. 37 Abs. 1 Buchstabe c) der DS-GVO einen Datenschutzbeauftragten benennen, wenn „die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9“ besteht.

II. Datenschutzbeauftragte und die Verarbeitung (sensibler) personenbezogener Daten als Kerntätigkeit

Erwägungsgrund 97 Satz 2 stellt fest, dass sich der Begriff der Kerntätigkeit auf die Haupttätigkeit und nicht auf die Verarbeitung personenbezogener Daten als Nebentätigkeit bezieht. Nach allgemeiner Auffassung muss die Datenverarbeitung eine essentielle Maßnahme zum Erreichen der Ziele des Verantwortlichen bzw. Auftragsverarbeiters darstellen. Das Erstellen von Gehaltsabrechnungen und IT-Support sind oft häufige Beispiele für datenschutzrelevante Kerntätigkeiten oder Kerngeschäfte einer nicht-öffentlichen bzw. öffentlichen Einrichtung. Trotz ihrer Notwendigkeit oder Unverzichtbarkeit werden solche Tätigkeiten gemeinhin eher als Nebenfunktionen und nicht als eigentliche Kerntätigkeit betrachtet.
Der Begriff der Kerntätigkeit steht in Wechselwirkung zum Umfang der Tätigkeit, sodass eine Gesamtbetrachtung vorgenommen werden muss. In der Literatur (Bergt, Kühling/Buchner, DS-GVO, Art. 37, Randnummer 24) wird beispielsweise bei der Bewertung der Tätigkeit von Ärzten als Kerntätigkeit folgendes vertreten:

Ziel der Tätigkeit von Ärzten ist es, Menschen gesund zu machen. Um aber herauszufinden, wie das Leiden eines Patienten zu bekämpfen ist – oder ob, im Fall von Vorsorgeuntersuchungen, überhaupt ein Problem besteht-, ist eine umfassende Untersuchung und Beobachtung des Patienten erforderlich, typischerweise auch regelmäßig über einen längeren Zeitraum [....] Die Kerntätigkeit von Ärzten liegt damit in der Verarbeitung sensibler Daten.

Diese Argumentation gilt analog auch für Apotheker, da auch hier die Diagnostik und Beratung über die Einnahme von Medikamenten im Vordergrund steht, sodass auch hier die Kerntätigkeit in der Verarbeitung sensibler Daten liegt. So auch der Beschluss der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 26. April 2018 „Datenschutzbeauftragten-Bestellpflicht nach Art. 37

Abs. 1 Buchstabe c) Datenschutz-Grundverordnung bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs“.
Maßgeblich bei der Bewertung der Erforderlichkeit eines Datenschutzbeauftragten ist, ob eine Verarbeitung sensibler personenbezogener Daten umfangreich im Sinne des Art. 37 Abs. 1 Buchstabe c) der DS-GVO ist. In Erwägungsgrund 91 zur DS-GVO ist in Bezug auf die Datenschutz-Folgenabschätzung ebenfalls von einer „umfangreichen Verarbeitung“ die Rede. Darin heißt es:
„Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogener Daten Patienten oder Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufs oder Rechtsanwalts erfolgt“.
Der Begriff „Gesundheitsberuf“ ist im Sinne der Aufzählung nach § 203 Abs. 1 Strafgesetzbuch (StGB) auszulegen und umfasst die in § 203 Abs. 1 Nr. 1, 2, 4 und 5 StGB aufgezählten Berufsbilder. Am 26. April 2018 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) die Entschließung „Datenschutzbeauftragten-Bestellpflicht nach Art. 37 Abs. 2 Buchstabe c) DS-GVO bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs“ veröffentlicht: https://www.tlfdi.de/tlfdi/datenschutz/datenschutzkonferenz/bundesund-laender/95/. Darin wird ausdrücklich festgehalten, soweit ein einzelner Arzt, Apotheker oder sonstiger Angehöriger eines Gesundheitsberufs eine Praxis, Apotheke oder ein Gesundheitsberufsunternehmen betreibt und mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind, besteht eine gesetzliche Verpflichtung zur Benennung eines DSB.

Bei Angehörigen eines Gesundheitsberufs, die ihre Tätigkeit in einer Berufsgemeinschaft (Praxisgemeinschaft) ausüben und weitere Ärzte, Apotheker beschäftigen, ist dann nicht von einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten im Sinne des Art. 37 Abs. 2 Buchstabe c) DS-GVO auszugehen, wenn in einer Praxisgemeinschaft weniger als zehn Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind.

Wenn bei der Verarbeitung personenbezogener Daten ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zu erwarten ist, ist eine Datenschutz-Folgenabschätzung vorgeschrieben, Art. 35 Abs. 1 DS-GVO. Damit ist immer zwingend ein Datenschutzbeauftragter zu benennen, auch wenn weniger als zehn Personen mit der Verarbeitung personenbezogener Daten besonderer Kategorien beschäftigt sind.

III. Benennungsvoraussetzungen nach BDSG

Das BDSG enthält darüber hinaus in § 38 Sonderregelungen zur DS-GVO in Bezug auf die Benennung des Datenschutzbeauftragten. Danach ist ein DSB immer dann zu benennen, wenn der Verantwortliche oder der Auftragsverarbeiter in der Regel mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt oder sie mit einer Datenverarbeitung beauftragt, die einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO unterliegen. Weiterhin muss ein Datenschutzbeauftragter benannt werden, wenn personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Markt- oder Meinungsforschung verarbeitet werden. Unternehmen können darüber hinaus jederzeit freiwillig einen Beauftragten für den Datenschutz benennen.

IV. Anforderungen an den Datenschutzbeauftragten

Gemäß Art. 37 Abs. 5 der DS-GVO wird der Datenschutzbeauftragte auf Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, dass er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt. Eine weitere Grundlage für die Benennung eines Datenschutzbeauftragten ist die Fähigkeit, Aufgaben gemäß Art. 39 der DS-GVO erfüllen zu können; der DSB übt dabei seine Pflichten und Aufgaben in vollständiger Unabhängigkeit aus. Diese Unabhängigkeit ist auch dann zu gewährleisten, wenn keine Pflicht zur Benennung eines Datenschutzbeauftragen besteht, sich der Verantwortliche aber aus freien Stücken dazu entschließt.
Ein Kandidat muss die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen. Bei der Einschätzung der Zuverlässigkeit sind sowohl subjektive Faktoren (persönliche Eigenschaften) als auch objektive Faktoren (mögliche Interessenskollisionen) zu berücksichtigen. Beide Kriterien sind bei der Benennung eines

Datenschutzbeauftragten gleichgewichtig entscheidend. Eine Interessenskollision ist dann nicht gegeben, wenn zwischen dem Verantwortlichen und dem DSB eine klare Trennung besteht. Bei internen betrieblichen Datenschutzbeauftragten ist hierbei darauf zu achten, dass der Datenschutz mit der primären Verpflichtung vereinbar ist. Eine Vereinbarkeit ist immer dann zu verneinen, wenn die Haupttätigkeit eine Führungs- oder Leitungsposition im Unternehmen darstellt, mit der Verarbeitung personenbezogener Daten verbunden ist oder sich auf diese auswirkt. Insbesondere darf er als DSB in seiner Kontrollfunktion nicht in die Situation kommen sich selbst kontrollieren zu müssen. Interessenkonflikte können immer dann auftreten, wenn der DSB gleichzeitig Aufgaben wahrnimmt in den Bereichen:

- Personal,
- Justitiariat/Recht,
- Automatisierte Datenverarbeitung (ADV) / Informationstechnik (IT) oder
- Organisationseinheiten mit besonders umfangreicher oder sensitiver Verarbeitung von personenbezogenen Daten wahrnimmt bzw.
- Geheimschutzbeauftragter oder
- Vorsitzender des Personalrats ist.

Der Datenschutzbeauftragte muss unabhängig von seinem Arbeitsstatus im Unternehmen seine Pflichten und Aufgaben in vollständiger Unabhängigkeit ausüben können. Nach Art. 37 Abs. 2 der DS-GVO darf eine Unternehmensgruppe einen gemeinsamen Datenschutzbeauftragten ernennen, sofern von jeder Niederlassung aus der DSB leicht erreicht werden kann.

Bei der Auswahl einer geeigneten Schulung des DSB ist auch darauf zu achten, wie hoch der Schutzbedarf für die vom Verantwortlichen oder vom Auftragsverarbeiter verarbeiteten personenbezogenen Daten ist. Das erforderliche fachliche Niveau des DSB sollte sich insbesondere nach den durchgeführten Datenverarbeitungsvorgängen und dem erforderlichen Schutz für die vom Verantwortlichen oder vom Auftragsverarbeiter verarbeiteten personenbezogenen Daten richten. Dabei ist der datenschutzrechtliche Schutzumfang maßgeblich.

Wegen der Aufgaben nach Art. 39 der DS-GVO kann es erforderlich sein, dass der DSB sektorspezifische Spezialkenntnisse besitzt, da ansonsten die Befähigung zur Erfüllung der genannten Aufgaben nicht möglich sein könnte. Gerade bei der Übernahme der Betreuung von Unternehmen als externer Beauftragter muss daher zwingend geprüft

werden, ob überhaupt die für das anfragende Unternehmen notwendige, individuelle Eignung gegeben ist.

V. Juristische Personen als Datenschutzbeauftragte?

Juristische Personen können nach der DS-GVO nicht explizit als Datenschutzbeauftragte benannt werden. Ob und unter welchen Voraussetzungen juristische Personen als DSB benannt werden können, steht unter den Aufsichtsbehörden noch zur Diskussion. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) vertritt die Auffassung, dass juristische Personen nicht als externe DSB benannt werden können. Bei der Benennung des Datenschutzbeauftragten liegt der Fokus, wie oben beschrieben, auf den individuellen Fähigkeiten des DSB. Daher ist es zwar möglich, dass die Person des Datenschutzbeauftragten bei einer juristischen Person angestellt ist, jedoch ist eine Zuordnung einer bestimmten natürlichen Person zum jeweiligen betreuten Unternehmen notwendig, da auch eine wahllose Vertretung nicht der DS-GVO entspricht. Es kann daher nur eine bestimmte Person benannt werden. Diese Person ist dann aber auch bei der Meldung des DSB mitzuteilen.
Problematisch bei der Benennung einer juristischen Person zum DSB ist, dass die Funktion des Datenschutzbeauftragten durch eine unbestimmte Personengruppe mit gegebenenfalls wechselndem Personenbestand wahrgenommen würde.

VI. Modalitäten zur Benennung eines Datenschutzbeauftragten

Sofern ein Unternehmen oder auch ein Einzelhändler verpflichtet ist, einen DSB zu benennen, muss eine Meldung des ernannten DSB nach Art. 37 Abs. 7 der DS-GVO an den TLfDI als Aufsichtsbehörde erfolgen. Hierzu ist unter https://www.tlfdi.de/tlfdi/europa/europaeischedsgvo/index.aspx ein Formular zur Meldung des Datenschutzbeauftragten bereitgestellt. Dieses soll von den Verantwortlichen für die Anmeldung und die Ummeldung des DSB genutzt werden.

Soweit keine Pflicht zur Benennung eines DSB vorliegt, unterstützt und begrüßt der TLfDI freiwillige Bemühungen durch die Verantwortlichen. Im Falle einer freiwilligen Benennung eines DSB unterliegen dessen Benennung, Stellung und Aufgabenbereich den gleichen Anforderungen wie

bei einer Benennung nach gesetzlichen Benennungspflicht (Art. 37 bis 39 DS-GVO). Der im nicht-öffentlichen Bereich geltende Abberufungs- und Kündigungsschutz des DSB nach § 38 Abs. 2 des BDSG gilt jedoch nur, wenn seine Benennung verpflichtend ist.
Die Benennung eines DSB erfolgt aufgrund seiner beruflichen Qualifikation und insbesondere wegen seines Fachwissens, dass er auf dem Gebiet des Datenschutzrechts und der Datenpraxis besitzt, Art. 37 Abs. 5 der DS-GVO. Weiterhin muss er fähig sein, die Erfüllung seiner Aufgaben nach Art. 39 der DS-GVO zu gewährleisten. Der DSB hat nach Art. 39 der DS-GVO die Aufgabe das Unternehmen bei der Durchführung der Datenschutzbestimmungen zu unterstützen, zu beraten und die Einhaltung der Normen zu überwachen. Es ist Aufgabe des Verantwortlichen oder des Auftragsverarbeiters, sicherzustellen und nachweisen zu können, dass die Datenverarbeitung im Einklang mit den Maßgaben der DS-GVO erfolgt. Für die Einhaltung der datenschutzrechtlichen Bestimmungen ist der Verantwortliche oder der Auftragsverarbeiter zuständig. Verstöße gegen die Vorschriften zur Benennung eines Datenschutzbeauftragten können vom TLfDI mit einem Bußgeld geahndet werden. Dabei würde sich ein etwaiges Bußgeldverfahren gegen den Verantwortlichen richten, der der Benennungspflicht nach Art. 37 Abs. 5 DS-GVO unterliegt.

5.17 Wirksame Einwilligungen nach altem Datenschutzrecht? Was Verantwortliche und Betroffene beachten müssen

Erteilte Einwilligungen nach altem Datenschutzrecht gelten weiterhin, wenn sie den Anforderungen der Datenschutz-Grundverordnung (DS-GVO) entsprechen. Ist dies nicht der Fall, muss der Verantwortliche die Einwilligung dem vorgegebenen Standard der DS-GVO anpassen und die Einwilligung erneut von der betroffenen Person einholen. Gelingt es dem Verantwortlichen nicht, die Einwilligung der betroffenen Person nach gültigem Standard der DS-GVO einzuholen, ist die Datenverarbeitung nicht rechtmäßig und muss eingestellt werden.

Viele Anfragen, die beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eingegangen sind, beschäftigten sich mit der Frage, ob Einwilligungen, die vor dem 25. Mai 2018 erteilt wurden, weiterhin rechtsgültig sind oder erneut Einwilligungen eingeholt werden müssen. Seit diesem Stichtag gilt

nämlich die Europäische Datenschutz-Grundverordnung (DS-GVO). Sie hat das bis dahin geltende Bundesdatenschutzgesetz-alt (BDSG-alt) abgelöst.
Einwilligungen, die vor dem 25. Mai 2018 eingeholten wurden, gelten fort, sofern sie den Bedingungen der Datenschutz-Grundverordnung entsprechen (Erwägungsgrund 171, Satz 3 DS-GVO). Die Bedingungen für eine gültige Einwilligung sind im Tätigkeitsbericht unter Punkt 5.24 ausführlich beschrieben. Bisher rechtswirksam erteilte Einwilligungen erfüllen grundsätzlich die Bedingungen der Datenschutz-Grundverordnung; einige Einwilligungen könnten jedoch unwirksam sein. Ob eine wirksam erteilte Einwilligungen im Rahmen der DS-GVO vorliegt, ist vom Verantwortlichen sorgfältig zu prüfen anhand der beschriebenen Voraussetzungen im Tätigkeitsbericht unter Punkt 5.24 und der Leitlinien des Europäischen Datenschutzausschusses (Guidelines on Consent). Daher ist es wichtig, dass die Verantwortlichen ihre Arbeitsprozesse und Aufzeichnungen vor dem 25. Mai 2018 genau überprüft haben, um sicherzustellen, dass bestehende Einwilligungen die Standards der DS-GVO einhalten und die Datenverarbeitungen somit rechtmäßig erfolgt.
Die DS-GVO setzt bei der Einholung von Einwilligungen neue Maßstäbe und definiert hierzu neue Anforderungen. Verantwortliche müssen daher Ihre Abläufe zur Einholung von Einwilligungen ändern, statt einfach nur die Datenschutzbestimmungen neu zu beschreiben.
Der Verantwortliche muss nach neuer Rechtslage nachweisen können, dass er eine gültige Einwilligung für die beabsichtigte Datenverarbeitung vom Betroffenen eingeholt hat. Ist das dem Verantwortlichen nicht möglich, liegt keine Einwilligung vor, die den Standards der DS-GVO entspricht. Selbst „vermutete Einwilligungen“, die durch bereits vorausgefüllte oder vorab angekreuzte Kästchen erteilt wurden, sind nicht mit der Datenschutz-Grundverordnung vereinbar. Diese Einwilligungen müssen folglich erneuert werden.
Darüber hinaus müssen die Vorgänge und IT-Systeme gegebenenfalls überprüft werden, um nachzuweisen, dass dem Verantwortlichen eine Einwilligung vorliegt. Dabei ist zu berücksichtigen, dass für jeden Verarbeitungszweck die entsprechend verarbeiteten Daten detailliert und exakt genannt werden (z. B. Telefonnummer, Geburtsdatum, E-Mail-Adresse usw.). Allein die Angabe von Datenkategorien zum Zweck der Verarbeitung ist zu allgemein gehalten und entspricht nicht den Vorgaben der DS-GVO.

Weiterhin soll es der betroffenen Person nach Art. 7 Abs. 3 der DS-GVO möglich sein, die Einwilligung jederzeit zu widerrufen. Informationen zum Widerruf einer Einwilligung, eine sogenannte Widerrufsbelehrung, müssen der betroffenen Person vor der tatsächlichen Abgabe der Einwilligung bereitgestellt werden. Dabei muss der Widerruf genauso einfach sein wie die Erteilung der Einwilligung. Das bedeutet, dass der betroffenen Person der Widerruf auf demselben Weg ermöglicht werden muss wie die Erteilung der Einwilligung. Dazu hat der Verantwortliche eventuell seine Arbeitsprozesse entsprechend anzupassen.
Einwilligungen sind ferner unwirksam, wenn ein Verstoß gegen die Freiwilligkeit, insbesondere gegen das Kopplungsverbot (Art. 7 Abs. 4 DS-GVO), vorliegt. Sinn und Zweck des Kopplungsverbots ist das generelle Freiwilligkeitsgebot, das Betroffene davor schützt, zwangsweise in eine Datenverarbeitung einzuwilligen, um ein damit verbundenes Leistungsangebot in Anspruch nehmen zu können. Erteilte Einwilligungen zur Datenverarbeitung von Kategorien personenbezogener Daten sind unwirksam, wenn sie zur Erfüllung des Vertragszwecks nicht erforderlich sind.
Wenn ein Verantwortlicher zu dem Ergebnis kommt, dass die nach altem Recht erteilte Einwilligung den Anforderungen der Datenschutz-Grundverordnung nicht entspricht, muss er Maßnahmen ergreifen, um diese Anforderungen einzuhalten. Dem Verantwortlichen ist zu empfehlen, die Einwilligung nach dem Standard der DS-GVO zu erneuern. Wenn dem Verantwortlichen das nicht gelingt, ist eine Datenverarbeitung nach Art. 6 Abs. 1 Buchstabe a) der DS-GVO nicht rechtmäßig und muss eingestellt werden.

5.18 Erweiterte Informationspflichten: Anfragen zur Umsetzung in der Praxis

Dieser Beitrag beschäftigt sich mit der Erteilung von Informationen nach Art. 13 und 14 der Datenschutz-Grundverordnung (DS-GVO), warum diese nicht unterzeichnet werden müssen und wie der Verantwortliche auch ohne das Aufbewahren sämtlicher Informationen seiner Nachweispflicht zur Erteilung der Information nachkommen kann. Die Umsetzung und die Hürde der Nachweispflicht schien im Berichtszeitraum für Unternehmer, Handwerksberufe und Vereine neben dem Alltagsgeschäft ein fast unüberwindbarer Aufwand.

Viele nicht-öffentliche Stellen (Unternehmen), die sich mit Beratungsbedarf an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wandten, waren der Auffassung, dass sie nun für sämtliche Datenverarbeitungen eine Einwilligungserklärung betroffener Personen benötigten. Sie vermischten dabei inhaltlich die Einwilligungserklärung nach Art. 6 Abs. 1 Buchstabe a) der DS-GVO und die zu erteilenden Informationen nach Art. 13 und 14 der DS-GVO miteinander. Die Einwilligungserklärung (siehe Beitrag 5.24) stellt eine Rechtsgrundlage für die Datenverarbeitung dar. Die Informationspflichten sind als Transparenzpflicht nach Art. 5 Abs. 1 Buchstabe a) DS-GVO durch den Verantwortlichen zu erfüllen. Es wird im Rahmen der Informationen nach Art. 13 und 14 gerade dargestellt zu welchen Zwecken und auf welcher Rechtsgrundlage die Datenverarbeitung bei dem Verantwortlichen erfolgt. Jedoch stellt das Versenden der Informationen keine Einholung der Einwilligung betroffener Personen dar, auch nicht, wenn diese Informationen von den Betroffenen unterzeichnet werden sollen.
Nach Art. 5 Buchstabe a) DS-GVO müssen personenbezogene Daten „auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden“. Eben diese Transparenzanforderungen aus Art. 5 der DS-GVO werden in den Art. 12 ff. der DS-GVO näher konkretisiert.
Die Informationspflichten nach Art. 13 und 14 der DS-GVO sind Verlängerungen der Transparenzforderung der Datenschutz-Grundverordnung und sind neben dem Vorliegen einer Rechtsgrundlage zu erfüllen.
Die Informationspflichten bilden die Basis für die Ausübung der Betroffenenrechte nach Art. 15 ff. der DS-GVO. Nur sofern Betroffene wissen, dass personenbezogene Daten über sie verarbeitet werden, können sie ihre Rechte ausüben. Die Informationspflichten der DS-GVO gehen weit über die bisherige Rechtslage hinaus und müssen, sofern keine Ausnahmevorschrift eingreift, beachtet werden.
Die Informationsverpflichtungen des Verantwortlichen gegenüber betroffenen Personen werden in der DS-GVO in Abhängigkeit davon geregelt, ob personenbezogene Daten direkt bei der betroffenen Person (Direkterhebung, Art. 13 DS-GVO) oder bei Dritten (Dritterhebung, Art. 14 DS-GVO) erhoben werden.

I. Informationspflichten bei der Direkterhebung

Um eine faire und transparente Verarbeitung von personenbezogenen Daten sicherzustellen, sind bei der Direkterhebung der betroffenen Person die nach Art. 13 Abs. 1 und Abs. 2 DS-GVO aufgeführten Informationen mitzuteilen und zur Verfügung zu stellen. Die einzelnen Informationen, die zu erteilen sind, ergeben sich unmittelbar aus dem Gesetz; die Angaben müssen vom Verantwortlichen entsprechend auf das jeweilige Unternehmen oder die jeweilige Vereinigung angepasst werden. Aus diesem Grund werden vom TLfDI keine Muster für ein solches Informationsblatt für nicht-öffentliche Stellen bereitgestellt. Von den Aufsichtsbehörden des Bundes und der Länder wurde zu den Informationspflichten das Kurzpapier Nr. 10: „Informationspflichten bei Dritt- und Direkterhebung“ erstellt, das über die wichtigsten zu beachtenden Punkte Auskunft gibt. Nach Art. 13 der DS-GVO sind unter anderem der Name des Verantwortlichen, Kontaktdaten des Datenschutzbeauftragten (falls vorhanden), Zwecke der Verarbeitung, sowie Rechtsgrundlage und berechtigtes Interesse anzugeben; falls die Verarbeitung auf Art. 6 Buchstabe f) gestützt wird, auch die Speicherdauer, die Betroffenenrechte etc. Bei der Erhebung der personenbezogenen Daten sollten die zu erteilenden Informationen bei anwesenden Personen direkt ausgehändigt oder auf einen Aushang oder eine Auslage verwiesen werden. Bei nicht anwesenden Personen sollten die zu erteilenden Informationen unmittelbar nach der Erhebung postalisch oder auf elektronischem Postweg, je nach vorheriger Kommunikation mit der betroffenen Person, zur Verfügung gestellt werden.

II. Informationspflichten bei Dritterhebung

Bei der Dritterhebung werden die personenbezogenen Daten auf andere Weise als bei der betroffenen Person erhoben, z. B. erfolgt die Erhebung aus allgemein zugänglichen Quellen oder aufgrund einer Datenübermittlung eines anderen Verantwortlichen oder sonstigen Dritten.
Wie bei Art. 13 der DS-GVO ergeben sich die entsprechenden Angaben unmittelbar aus Art. 14 Abs. 1 und Abs. 2 DS-GVO, die ebenfalls auf das entsprechende Unternehmen und dessen Struktur angepasst werden müssen. Daher wird auch vom TLfDI kein Muster für die In-

formationspflichten bereitgestellt und auf das o. g. Kurzpapier verwiesen. Art und Inhalt der mitzuteilenden Informationen entsprechen im Wesentlichen denen bei der Direkterhebung.
Da die betroffene Person im Gegensatz zur Direkterhebung nicht an der Datenerhebung mitgewirkt hat und somit auch keine Kenntnis darüber haben kann, welche personenbezogenen Daten erhoben wurden, ist der Verantwortliche verpflichtet, dem Betroffenen diese Kategorien verarbeiteter personenbezogenen Daten (z. B. Name, Adresse, Geburtsdatum, E-Mail, Telefonnummer, Bankverbindung etc.) mitzuteilen. Diese Angaben müssen so konkret sein, dass der betroffenen Person deutlich wird, zu welchen Folgen die Verarbeitung führen kann. Zudem ist nach Art. 14 Abs. 2 der DS-GVO die Datenquelle, also diejenige Stelle, von der ein Verantwortlicher die Daten erhalten hat, zu nennen oder ob es sich um eine öffentlich zugängliche Quelle handelt. Sofern die Daten aus mehreren Quellen stammen und die Herkunft nicht mehr eindeutig identifiziert werden kann, muss dennoch eine allgemeine Information gegeben werden.
Der Zeitpunkt für die zu erteilende Information ergibt sich bei der Dritterhebung aus Art. 14 Abs. 3 der DS-GVO. Danach ist der Verantwortliche verpflichtet nach Erhebung der Daten die Informationen nachträglich innerhalb einer angemessenen Frist mitzuteilen. Diese Frist darf aber den Zeitraum eines Monats nicht überschreiten. Die Monatsfrist stellt dabei eine Maximaldauer dar und sollte nicht pauschal angesetzt werden. Sofern die Daten zur Kommunikation mit der betroffenen Person verwendet werden, sollten die Informationen spätestens zum Zeitpunkt der ersten Kontaktaufnahme mitgeteilt werden. Falls die Daten einem anderen Empfänger weitergegeben werden sollen, müssen die Informationen spätestens zum Zeitpunkt der ersten Offenlegung erteilt werden.
Die Informationspflichten nach Art. 13 und 14 der DS-GVO sind im Fall einer Zweckänderung sowohl bei der Direkt- als auch bei der Dritterhebung neben der Information über die geänderte Zweckbestimmung erneut zu erfüllen. Eine Übermittlung an einen Dritten ist häufig auch eine Zweckänderung, sodass schon aus diesem Grund vor der Übermittlung die betroffene Person erneut zu informieren ist.

III. Ausnahmen von den Informationspflichten

Nach Art. 13 Abs. 4 und Art. 14 Abs. 5 der DS-GVO bestehen keine Informationspflichten, wenn die betroffene Person bereits über die

mitzuteilenden Informationen verfügt. Das bedeutet auch, dass die betroffene Person von dem Verantwortlichen nicht erneut informiert werden muss, sondern eine einmalige Information ausreicht, sofern keine Zweckänderung oder eine Übermittlung an Dritte erfolgt.
Ferner besteht bei der Dritterhebung keine Informationspflicht, wenn sich die Informationserteilung als z. B. unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde, die Daten einem Berufsgeheimnis unterliegen (z. B. entfällt bei Erhebung von therapeutisch bedeutsamen Gesundheitsdaten über die Familienangehörigen des Patienten die Informationspflicht nach Art. 14 DS-GVO gegenüber diesen Personen) oder die Erlangung durch Rechtsvorschrift ausdrücklich geregelt ist.
Weitere Beschränkungen der Informationspflichten ergeben sich aus §§ 32 und 33 des Bundesdatenschutzgesetzes (BDSG). § 32 BDSG regelt dabei die Beschränkung der Informationspflichten hinsichtlich einer beabsichtigten Weiterverarbeitung durch den Verantwortlichen. Die Informationen des Art. 13 Abs. 1 und Abs. 2 DS-GVO werden von diesen Beschränkungen nicht erfasst. § 33 BDSG regelt weitere Beschränkungen der Informationspflichten im Rahmen von Art. 14 DS-GVO.

IV. Form der Informationspflicht

Nach Art. 12 Abs. 1 der DS-GVO sind die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in klarer und einfacher Sprache zu übermitteln. Grundsätzlich sind die Informationen so bereitzustellen, dass die betroffene Person sie im Zusammenhang mit der Datenerhebung ohne Medienbruch entgegennehmen kann. Werden die personenbezogenen Daten beispielsweise mit einem schriftlichen oder elektronischen Formular erhoben, müssen die Informationen grundsätzlich auf diesem Formular bereitgestellt werden. Eine elektronische Informationserteilung muss leicht zu finden sein z. B. durch einen Link der darauf verweist, einen deutlich erkennbaren Button oder QR-Code, zudem können auch Bildsymbole, sogenannte Icons, eingesetzt werden. Bei anwesenden Personen sollte nicht auf Informationen im Internet, sondern auf einen Aushang bzw. einer Auslage im Geschäft hingewiesen werden. Das Aushändigen eines Flyers oder einer Informationsbroschüre bzw. eines Informationsblattes ist ebenfalls möglich.

V. Nachweis der Informationspflichten

Besonders in diesem Bereich wurden viele Fragen von Verantwortlichen an den Thüringer Landesbeauftragten für Datenschutz und Informationsfreiheit gerichtet. Aus Art. 5 Abs. 2 GS-GVO ergibt sich, dass der Verantwortliche für die Einhaltung des Art. 5 Abs. 1 DS-GVO verantwortlich ist und dass er dessen Einhaltung nachweisen können muss. Beim TLfDI wurde daher angefragt, ob alle ausgegebenen Informationsblätter von den Betroffenen unterzeichnet und dann aufbewahrt werden müssten. Dies war nach dem 25. Mai 2018 aufgrund der Unklarheiten in Bezug auf die Auslegung des Gesetzes der wohl sicherste Weg für Verantwortliche, aber wohl auch der umständlichste und aufwendigste. Das Gesetz sieht nicht vor, dass die Erteilung der Information von betroffenen Personen bestätigt werden müsste. Die betroffene Person muss die Möglichkeit haben, diese Informationen zur Kenntnis zu nehmen und danach umfassend ihre Betroffenenrechte ausüben zu können. Es ist daher ausreichend, wenn Unternehmen oder sonstige nicht-öffentliche Stellen ein Verfahren in ihren Geschäftsablauf integriert haben, das sicherstellt, dass die betroffenen Personen zu den in der DS-GVO geforderten Zeitpunkten diese Informationen erhalten. Sofern beispielsweise beim ersten Betreten des Geschäfts die Informationen an die Kunden ausgehändigt werden (mittels Flyer, Informationsbroschüre oder Informationsblatt) oder auf den entsprechenden Aushang verwiesen wird, reicht diese Vorgehensweise als Nachweis für die Erfüllung der Informationspflicht gegenüber den betroffenen Personen aus. Bei erstmaligen schriftlichen Kontakt, ist es zudem möglich die Information in einem Antwortschreiben beiliegend zur Verfügung zu stellen.

VI. Folgen eines Verstoßes

Ein Verstoß gegen die Informationspflichten kann von der Aufsichtsbehörde nach Art. 83 Abs. 5 Buchstabe b) der DS-GVO mit einer Geldbuße geahndet werden.

5.19 Impressum und Datenschutzerklärung: Transparenz und Datenschutzhinweise für Webseitenbetreiber

Die Impressumspflicht und die Pflicht, auf die Verarbeitung personenbezogener Daten hinzuweisen, gab es schon vor der DS-GVO. Neu ist in der DS-GVO geregelt, dass die Datenschutzhinweise nun präziser, transparenter und verständlich formuliert sein müssen. Im Übrigen sind die Bußgelder, falls die Vorgaben nicht umgesetzt werden, nun höher.

Immer wieder erreichen den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) Anfragen zur Internetseiten-Gestaltung, insbesondere welche Informationen im Impressum aufzunehmen sind und welche Informationen nach der DS-GVO in die Datenschutzhinweise aufgenommen werden müssen.
Grundsätzlich ist zwischen der Impressumspflicht und den Datenschutzhinweisen nach der DS-GVO zu unterscheiden.
Die Impressumspflicht ist in § 5 und § 6 Telemediengesetz (TMG) geregelt. Sie existierte bereits vor der DS-GVO. So muss beispielsweise der Dienstanbieter neben den Kontaktdaten auch die Handelsregisternummer und die Umsatzsteuer-Identifikationsnummer angeben. Bei Aktiengesellschaften, Kommanditgesellschaften auf Aktien und Gesellschaften mit beschränkter Haftung, die sich in Abwicklung oder Liquidation befinden, sind auch hierüber Angaben zu machen. Das TMG verlangt übrigens auch in § 5 Abs. 1, dass die Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten sind. Mit der unmittelbaren Erreichbarkeit haben manche Internetseiten-Betreiber allerdings ihre Schwierigkeiten. Oft ist das Impressum schwer und umständlich auf der entsprechenden Internetseite zu finden.
Zudem kann es spezialgesetzliche Regelungen geben, die weitere Angaben oder Informationen erfordern. So müssen Online-Shop-Betreiber z. B. auch § 36 und § 37 des Gesetzes über die alternative Streitbeteiligung in Verbrauchersachen (VSBG) beachten. Dies bedeutet z. B. auch, dass für Streitbeilegungsverfahren die Verbraucherschlichtungsstelle anzugeben ist.
Die Pflicht, Datenschutzhinweise auf der Internetseite zu veröffentlichen ist auch nicht neu. Auch vor der DS-GVO mussten die Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Er-

hebung und Verwendung personenbezogener Daten in allgemein verständlicher Form unterrichtet werden. Dies bedeutet, schon vor dem 25. Mai 2018 musste auf den Einsatz von Cookies, den Einsatz von Website-Analysetools usw. hingewiesen werden (§ 13 TMG).
Neu ist mit der DS-GVO, dass die Datenschutzhinweise nun präziser, transparent und verständlich formuliert sein müssen (Art. 12 DS-GVO).
Wie präzise die Datenschutzhinweise sein müssen, regelt insbesondere Art. 13 DS-GVO. Der Verantwortliche hat also geeignete Maßnahmen zu treffen, um der betroffenen Person alle Informationen gemäß den Art. 13 und 14 und alle Mitteilungen gemäß den Art. 15 bis 22 und Art. 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere auch für Informationen, die sich speziell an Kinder richten. Richten sich Online-Angebote gezielt an Kinder, ist also eine kindgerechte Sprache zu verwenden. Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch (Art. 12 Abs. 1 DS-GVO, Erwägungsgrund 39). Beispielsweise auch auf der Website, wenn sie für die Öffentlichkeit bestimmt sind. Dies gilt insbesondere dann, wenn die große Zahl der Beteiligten und die Komplexität der dazu benötigten Technik es der betroffenen Person schwermachen, zu erkennen und nachzuvollziehen, ob, von wem und zu welchem Zweck ihre personenbezogenen Daten erfasst werden, wie etwa bei der Werbung im Internet (Erwägungsgrund 58). Beim Abruf einer Webseite werden verschiedene Daten übermittelt. Dazu gehören die IP-Adresse, der verwendete Webbrowser, das genutzte Betriebssystem, die eingestellte Sprache, gegebenenfalls Informationen zur Position des Gerätes, installierte Browsererweiterungen, Bildschirmgrößen, die Zeitzone und Advertising-ID's. Daneben speichern Webseiten kurze textuelle Informationen im Browser, als Cookies bezeichnet, ab. Über diese Daten versuchen Werbetreibende Personen bzw. Personengruppen zu identifizieren. Sind Dienste eines Werbetreibenden auf verschiedenen Websites integriert oder wird erfasst, wie oft eine Werbeanzeige von Personen einer bestimmten Personengruppe eine Werbeanzeige anklicken, können Personen bzw. Personengruppen nachverfolgt und Profile über Interessen und Vorlieben gebildet werden. Dies erlaubt eine gezielte personalisierte Werbung.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) haben zudem verschiedene Kurzpapiere erstellt. Diese sollen zur Orientierung bei der praktischen Umsetzung der DS-GVO dienen. Hinweise zu Informationspflichten bei der Dritt- und Direkterhebung enthält das Kurzpapier Nr. 10, das über den Link https://www.tlfdi.de/mam/tlfdi/gesetze/dsk_kpnr_10_informationspflichten.pdf abrufbar ist.

5.20 Geteilte Verantwortung: Die DS-GVO und das neue Konzept der Auftragsdatenverarbeitung

Im Berichtszeitraum erreichten den Thüringer Landesbeauftragten für Datenschutz und Informationsfreiheit (TLfDI) zahlreiche Anfragen rund um die Inkraftsetzung der Datenschutz-Grundverordnung (DS-GVO) zum 25. Mai 2018. So beschäftigte viele Anfragesteller der Umgang mit bereits bestehenden vertraglichen Verhältnissen zur Auftragsdatenverarbeitung. Sie baten den TLfDI um Auskunft darüber, ob bestehende vertragliche Verhältnisse zur Auftragsdatenverarbeitung fortgelten und was im Rahmen der Umsetzung zu beachten sei. Weiterhin wurde immer wieder um entsprechenden Mustervorlagen für einen Vertrag zur Auftragsverarbeitung gebeten. Dabei war vielen Unternehmen auch unklar, ob überhaupt ein Vertrag zur Auftragsverarbeitung mit anderen Unternehmen abgeschlossen werden muss, oder ob die Übermittlung der Daten auf eine Rechtsgrundlage gestützt werden kann.

Der Begriff des Auftragsverarbeiters wird in Art. 4 Nr. 8 DS-GVO definiert. Danach ist Auftragsverarbeiter eine natürliche oder juristische Person, eine Behörde bzw. Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Dem Auftragsverarbeiter stehen fortan nur noch bestimmte Entscheidungsspielräume in Bezug auf die Mittel der Verarbeitung zur Verfügung. Die Entscheidung über die „Mittel“ der Verarbeitung beinhaltet einerseits technische und organisatorische Fragen, deren Entscheidung problemlos auf den Auftragsverarbeiter delegiert werden kann

(z. B. welche Hardware oder Software verwendet wird) und andererseits wesentliche Elemente, welche den Kern der Rechtmäßigkeit der Verarbeitung betreffen, z. B. welche Daten verarbeitet werden, wie lange sollen diese verarbeitet werden oder wer hat Zugang hierzu. Diese Entscheidungen bleiben ausschließlich dem Verantwortlichen vorbehalten. (siehe Working Paper Nr.: 169 der Art. 29 Datenschutzgruppe: „Stellungnahme zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, S. 17/18). Sofern zwar klare Definitionen zu den Zwecken, aber nur wenige oder überhaupt keine Weisungen zu technischen und organisatorischen Mitteln vorliegen, sollten die Mittel eine angemessene Methode zur Erreichung des Zwecks darstellen. Sobald jedoch der Auftragsverarbeiter einen Einfluss auf den Zweck hat und die Verarbeitung auch zu seinem eigenen Nutzen durchführt (z. B. Verwendung der erhaltenen personenbezogenen Daten zur Erbringung von Mehrwertdiensten) ist er als ein für die Verarbeitung Verantwortlicher zu betrachten (siehe Working Paper Nr. 169 der Art. 29 Datenschutzgruppe, S. 18). Hierbei besteht möglicherweise auch eine gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO mit dem ursprünglichen für die Verarbeitung Verantwortlichen.
Insgesamt gilt die Sonderregelung für Verarbeitungen von personenbezogenen Daten im Auftrag in der DS-GVO fort. Allerdings werden dem Auftragsverarbeiter künftig mehr Verantwortung und mehr Pflichten auferlegt.
Der Auftragsverarbeiter ist nach Art. 29 DS-GVO weisungsgebunden. Zwischen dem Verantwortlichen, der den Auftrag erteilt und dem Auftragsverarbeiter, der den Auftrag annimmt, besteht ein „Innenverhältnis“, daher wird die Verarbeitung durch den Auftragsverarbeiter grundsätzlich dem Verantwortlichen zugerechnet. Für die Weitergabe von personenbezogenen Daten an den Auftragsverarbeiter und die Verarbeitung durch den Auftragsverarbeiter bedarf es insofern keiner weiteren gesetzlichen Rechtsgrundlage im Sinne des Art. 6 bis 10 der DS-GVO als derjenigen, auf die der Verantwortliche seine Verarbeitung stützt.
Zudem sind Auftragsverarbeiter Empfänger im Sinne des Art. 4 Nr. 9 der DS-GVO von personenbezogenen Daten. Das führt dazu, dass der Verantwortliche im Rahmen seiner Informationspflichten nach Art. 13 und 14 der DS-GVO den Auftragsverarbeiter als Empfänger zu benennen hat. Ferner bestehen nach Art. 19 der DS-GVO Mitteilungspflichten des Verantwortlichen gegenüber den Empfängern der

personenbezogenen Daten hinsichtlich Berichtigung, Löschung und Einschränkung der übermittelten Daten. Im Rahmen des Auskunftsrechts nach Art. 15 der DS-GVO sind Betroffenen die Empfänger der Daten, also die Auftragsverarbeiter, ebenfalls mitzuteilen. Weiterhin sind Empfänger im Verzeichnis von Verarbeitungstätigkeiten (Art. 30 Abs. 1 DS-GVO) vom Verantwortlichen mit anzugeben.

I. Regelungen für die Auftragsverarbeitung

Die Auftragsverarbeitung wird zentral in Art. 28 der DS-GVO geregelt. Dem Verantwortlichen wird dort eine Prüfpflicht auferlegt, wonach er vor der Auftragsvergabe die Eignung des Auftragsverarbeiters zu prüfen hat. Dabei darf der Verantwortliche nur Auftragsverarbeiter wählen, die hinreichende Garantien dafür bieten, geeignete technische und organisatorische Maßnahmen für einen ausreichenden Datenschutz anzuwenden, sodass die Auftragsdatenverarbeitung im Einklang mit der DS-GVO erfolgt und der Schutz der Rechte betroffener Personen gewährleistet ist. Hierfür können auch genehmigte Verhaltensregeln nach Art. 40 der DS-GVO oder Zertifizierungen nach Art. 42 der DS-GVO als Faktoren herangezogen werden.

II. Verträge mit Auftragsverarbeitern

Wie nach bisher geltendem Recht muss ein Vertrag über weisungsgebundene Tätigkeiten zwischen Verantwortlichem und Auftragsverarbeiter geschlossen werden. Der Vertrag kann schriftlich oder in einem elektronischen Format verfasst sein. Es können hierbei individuelle Regelungen getroffen werden, verabschiedete Standardvertragsklauseln der EU-Kommission oder der zuständigen Aufsichtsbehörde verwendet werden. Hiervon haben die deutschen Aufsichtsbehörden allerdings keinen Gebrauch gemacht. Es wird auf der Webseite des TLfDI eine Formulierungshilfe für einen solchen Auftragsverarbeitungsvertrag zur Verfügung gestellt, die beispielhaft genutzt werden kann und die wichtigsten inhaltlichen Punkte berücksichtigt. Die notwendigen Inhalte für einen abzuschließenden Auftragsverarbeitungsvertrag ergeben sich aus Art. 28 Abs. 3 der DS-GVO. Die Anpassung bestehender Verträge muss daher an diesen Anforderungen gemessen werden. Der Vertrag muss beispielsweise eine Regelung zur Bereitstellung der zu verarbeitenden Daten beinhalten und die Einhaltung der besonderen Bedingungen für den Einsatz von Subunternehmen regeln. Zudem muss der Vertrag vorsehen, dass der Auftragsverarbeiter

die nach Art. 32 der DS-GVO erforderlichen technischen und organisatorischen Maßnahmen ergreift. Der Verantwortliche bleibt weiterhin für die Rechtmäßigkeit der Verarbeitung verantwortlich, so dass zumindest die erforderlichen technischen und organisatorischen Maßnahmen dargestellt werden sollten.
Sofern sich der Auftragsverarbeiter zur Erbringung der vereinbarten Dienstleistung eines Subunternehmers bedienen möchte, muss dies zuvor vom jeweiligen Verantwortlichen auf schriftlichen oder elektronischen Weg genehmigt werden. Ein Vertrag zwischen Auftragsverarbeiter und Subunternehmer muss die gleichen vertraglichen Verpflichtungen enthalten, die der Auftragsverarbeiter zugunsten des Verantwortlichen in dessen Auftragsverarbeitungsvertrag übernommen hat. Spätere Änderungen von Subunternehmern sind dem Verantwortlichen vorher mitzuteilen. Dieser kann daraufhin Einspruch erheben und, sofern keine Einigung erzielt werden kann, die Unterbeauftragung an Subunternehmer per Weisung unterbinden bzw. die Auftragsverarbeitung ganz beenden.

III. Neue Verantwortlichkeiten und Pflichten für Auftragsverarbeiter

Verstößt ein Auftragsverarbeiter gegen die Pflicht zur weisungsgebundenen und damit vertraglich festgelegten Verarbeitung, indem er die Daten seines Auftraggebers unrechtmäßig für eigene Zwecke oder Zwecke Dritter verarbeitet, so ist er nach Art. 28 Abs. 10 der DS-GVO selbst als Verantwortlicher mit allen rechtlichen Folgen zu behandeln.
In Art. 82 der DS-GVO sind spezielle Haftungsregelungen für Auftragsverarbeiter bei Datenschutzverletzungen hinzugekommen. Danach drohen dem Auftragsverarbeiter nun bei Verstößen gegen die ihm speziell auferlegte Pflichten der DS-GVO Schadenersatzforderungen betroffener Personen.
Darüber hinaus ist vom Auftragsverarbeiter ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 der DS-GVO zu führen, das alle Kategorien der Verarbeitungstätigkeiten erläutert, die der Auftragsverarbeiter im Auftrag des Verantwortlichen durchführt. Dieses Verzeichnis muss nach Art. 30 Abs. 4 der DS-GVO der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung gestellt werden. Zudem muss ein Auftragsverarbeiter nach Art. 33 Abs. 2 der DS-GVO eine Verletzung des Schutzes personenbezogener Daten nach Bekanntwerden unverzüglich dem Verantwortlichem melden.

IV. Folgen bei Verstößen und typische Dienstleistungen der Auftragsverarbeitung

Hier sind die umfassenden Vorschriften über Geldbußen des Art. 83 Abs. 4, 5 und 6 der DS-GVO zu berücksichtigen. Diese Sanktionen können bei Verstößen nicht nur den Verantwortlichen selbst, sondern auch den Auftragsverarbeiter treffen, z. B. bei Verstößen gegen seine Verpflichtungen nach Art. 28 Abs. 2 bis 4 der DS-GVO.

Derzeit wird von den Aufsichtsbehörden des Bundes und der Länder eine Liste erarbeitet, die Tätigkeiten einer typischen Auftragsverarbeit-ung veranschaulicht. Diese Liste wird auch auf der Webseite des TLfDI veröffentlicht werden. Als Dienstleistungen für eine Auftragsverarbeitung kommen beispielsweise in Betracht:

- DV-technische Arbeiten für Lohn- und Gehaltsabrechnung oder Finanzbuchhaltung durch Rechenzentren
- Werbeadressen-Verarbeitung in einem Lettershop
- Verarbeitung von Kundendaten durch ein Call-Center ohne wesentliche eigene Spielräume
- Datenträgerentsorgung durch Dienstleister
- Auslagerung der Backup-Sicherheitsspeicherung und anderer Archivierungen
- Prüfung oder Wartung (z. B. Fernwartung, externer Support) automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn hier ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann

V. Sonderfall der Auftragsverarbeitung: Lohn- und Gehaltsabrechnung durch Steuerberater

Derzeit ist unter den Aufsichtsbehörden umstritten, ob der Steuerberater als Auftragsverarbeiter im Rahmen der Lohn- und Gehaltsabrechnung gilt. Der TLfDI vertritt die Rechtsauffassung, dass die datenschutzrechtliche Einstufung der Steuerberater als Verantwortlicher im Sinne des Art. 4 Abs. 7 der DS-GVO oder als Auftragsverarbeiter nach Art. 28 der DS-GVO für die Verarbeitung von personenbezogenen Daten je nach dem Kontext seiner Tätigkeit unterschiedlich zu behandeln ist. Nach dem erstellten Arbeitspapier (Working Paper WP) Nr. 169 (S. 34-35) der Art. 29 Datenschutzgruppe handeln Steuerberater als Verantwortliche, wenn Sie Dienstleistungen auf der Grundlage nur sehr allgemeiner Weisungen erbringen, z. B. bei Erstellung einer Steuererklärung. Wenn Sie jedoch für ein Unternehmen tätig

sind, um z. B. eine Buchprüfung oder Lohnbuchhaltung durchzuführen, und dabei ausführlichen Weisungen des Unternehmens unterliegen, dann ist der Steuerberater aufgrund der klaren Weisungen und des eingeschränkten Handlungsspielraums generell als Auftragsverarbeiter einzustufen. Dieses erarbeitete Working Paper dient als Auslegungshilfe zu der EU-Datenschutz-Grundverordnung. Zwar wurde das Working Paper im Rahmen der nicht mehr geltenden EG-Datenschutzrichtlinie (95/46/EG) des Europäischen Parlaments und des Rates vom 24. Oktober 1995 erstellt, jedoch sind die Begrifflichkeiten in der Richtlinie „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ identisch zu den jetzt in der Datenschutz-Grundverordnung verwendeten Begriffen. Um eine einheitliche Anwendung der DS-GVO zu gewährleisten orientieren sich die Aufsichtsbehörden daher an diesen Leitlinien.
Auch hier wird derzeit eine gemeinsame Entschließung aller Aufsichtsbehörden des Bundes und der Länder angestrebt, um eine einheitliche Anwendungspraxis zu gewährleisten. Sobald eine solche Entschließung getroffen wurde, wird auch diese auf der Webseite des TLfDI zu finden sein.

VI. Keine Auftragsverarbeitung im Fall von Datenübermittlungen des Arztes an das Labor

Eine Auftragsverarbeitung liegt nicht vor, wenn ein Arzt Patientendaten an ein Labor übermittelt, das durch einen Laborarzt geleitet wird. Wird ein anderer Facharzt in Anspruch genommen, wird der behandelnde Arzt als Vertreter für den Patienten tätig, wodurch ein selbständiger Vertrag zwischen dem zusätzlichen Arzt und dem Patienten zustande kommt (Palandt, BGB, § 630a, Rdnr. 3.). Die hier erfolgte Datenübermittlung und weitere Verarbeitung der Patientendaten kann daher auf die gesetzliche Rechtsgrundlage des Art. 6 Abs. 1 Buchstabe b) DS-GVO in Verbindung mit Art. 9 Abs. 2 Buchstabe h) DS-GVO gestützt werden, da die Verarbeitung zur Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person (Patient) ist, erforderlich ist.

5.21 Veröffentlichung von Foto- und Filmaufnahmen

Mit der Einführung der Datenschutz-Grundverordnung (DS-GVO) bestand bei allen Verantwortlichen, vom Hochzeitsfotografen bis zum

Fußballverein, eine große Verunsicherung hinsichtlich der rechtlichen Grundlagen für die Erstellung und auch die anschließende Veröffentlichung von Film- und Fotoaufnahmen. In diesem Zusammenhang wurde auch die Umsetzung der Informationspflichten zunächst als schwierig angesehen. Die Aufsichtsbehörden haben hier jedoch praktische Umsetzungsformen gefunden, die im rechtlichen Rahmen der DS-GVO die Handhabe privater Fotoalben, oder die Veröffentlichung von Foto- und Filmaufnahmen von Fotografen oder Vereinen ermöglichen.

Auch bei Fotos handelt es sich um personenbezogene Daten. Personenbezogene Daten liegen gemäß Art. 4 Ziff. 1 DS-GVO vor, wenn sie sich auf „eine identifizierbare natürliche Person beziehen“. Identifizierbar ist eine Person, wenn diese „direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind“. Eine solche Identifizierbarkeit ist hier gegeben. An dieser prinzipiellen Identifizierbarkeit ändert auch der Umstand nichts, dass der einzelne Fotograf in den meisten Fällen keine Zuordnung einzelner Gesichter zu anderen Daten dieser Personen herstellt oder überhaupt selbst herstellen kann. Auf die individuellen Möglichkeiten des einzelnen Fotografen ist bei abstrakter Betrachtung, ob es sich um personenbezogene Daten handelt, nicht abzustellen. Es reicht aus, dass eine Personenbeziehbarkeit der Daten prinzipiell möglich ist, was angesichts der hohen Auflösung von Digitalbildern in Bezug auf Bildaufnahmen und der Verfügbarkeit von Gesichtserkennungssoftware angenommen werden muss. Auch wenn man auf die individuellen Fähigkeiten des einzelnen Fotografen abstellen würde, also einen relativen Begriff der personenbezogenen Daten vertritt, ist es schwierig zu argumentieren, dass körperliche Merkmale einer Person, insbesondere die individuellen Gesichtszüge, wenn sie ausreichend erkennbar sind, nicht geeignet sind, um eine Person eindeutig zu identifizieren. Es handelt sich daher bei ausreichend aufgelösten oder auflösbaren Bildaufnahmen, die eine oder mehrere Personen gut erkennbar zeigen, immer um personenbezogene Daten.

Bei der Bewertung der rechtlichen Anforderungen ist dabei zunächst zwischen der Erstellung und der Veröffentlichung von Fotoaufnahmen zu unterscheiden. Weiterhin sind verschiedene Ausgangssituationen zu berücksichtigen.

I. Das Haushaltsprivileg

Der Anwendungsbereich der DS-GVO greift nur dann, wenn die Erstellung und Verarbeitung von Film- und Fotoaufnahmen nicht ausschließlich persönlichen oder familiären Zwecken dient. Das sogenannte „Haushaltsprivileg“ in Art. 2 Abs. 2 Buchstabe c) DS-GVO ermöglicht die Erstellung und Verwendung von Fotos für den privaten und familiären Gebrauch. Urlaubsfotos, Fotoalben und Erinnerungsfotos sind daher weiterhin möglich ohne die Voraussetzungen, die die DS-GVO für die Datenverarbeitung aufstellt, erfüllen zu müssen. Zu beachten ist hierbei nur, dass diese Ausnahme einen sehr beschränkten Anwendungsbereich hat. Die Verarbeitung darf keinen Zusammenhang oder Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit haben.
Auch bei der Veröffentlichung solcher Aufnahmen ist Vorsicht geboten. Sollen die Fotos in einem sozialen Netzwerk eingestellt werden, ist bei einer durch Nutzernamen und Passwort geschützten Gruppe oder Forum auf einer Webseite davon auszugehen, dass es gerade noch unter das Haushaltsprivileg fällt, da dieses restriktiv, also sehr eng ausgelegt wird.
Wenn die Aufnahmen jedoch einem unbeschränkten Personenkreis zugänglich gemacht werden, beispielsweise durch die Bereitstellung der Aufnahmen auf einer frei zugänglichen Webseite, fällt dies nicht mehr unter das Haushaltsprivileg, da es sich dann nicht mehr um eine rein familiäre oder persönliche Tätigkeit handelt. Hier findet die DS-GVO mit allen Voraussetzungen Anwendung.

II. Das Medienprivileg

Erfolgt die Erstellung und Veröffentlichung zu journalistisch-redaktionellen Zwecken, steht dem Verantwortlichen das sogenannte „Medienprivileg“ zur Seite. Für diesen Fall ist in Art. 85 Abs. 1 der DS-GVO den Mitgliedsstaaten die Möglichkeit eingeräumt worden, nationale Regelungen zu treffen, um den Datenschutz und das Recht auf

freie Meinungsäußerung und Informationsfreiheit sowie der Verarbeitung von Daten für journalistische Zwecke in Einklang zu bringen. Eine derartige Regelung findet sich für öffentliche und nicht-öffentliche Stellen in Thüringen in § 25 Thüringer Datenschutzgesetz (ThürDSG). Danach sind Unternehmen sowie Hilfsunternehmen der Presse weitgehend frei von datenschutzrechtlichen Vorgaben für die Zulässigkeit der Erhebung und Verarbeitung der Daten. In diesem Fall werden nur die Art. 5 Abs. 1 Buchstabe f), sowie die Art. 24, 32 und 33 DS-GVO für anwendbar erklärt. Damit wird dem Recht auf freie Meinungsäußerung und Informationszugang Genüge getan. Zu beachten bleiben allerdings weiterhin das Thüringer Pressegesetz, das allgemeine Persönlichkeitsrecht des Einzelnen und das Urheberrecht. Eine Entbindung von den Vorgaben der DS-GVO, geeignete technische und organisatorische Maßnahmen zur Datensicherheit zu treffen, gibt es aber auch für die journalistische Tätigkeit nicht!

III. Erstellung von Fotoaufnahmen konkreter Personen oder überschaubarer Gruppen

Die Erstellung von Fotos, auf denen die abgebildete Person im Vordergrund steht, ist ausschließlich nach Art. 6 Abs. 1 DS-GVO zu bewerten. Für die Erstellung der Fotos kann auch nicht das Kunsturhebergesetz (KUG) herangezogen werden, da sich dessen Anwendungsbereich allein auf die Veröffentlichung, also die Verbreitung und öffentliche Zurschaustellung von Fotos bezieht.
Die Erstellung von Fotoaufnahmen dieser Art ist daher zulässig, wenn sie zur Erfüllung eines Vertrages notwendig ist. Das ist beispielsweise bei einem beauftragten Fotografen für eine Hochzeit der Fall, wenn er das Brautpaar ablichtet, von dem er beauftragt wurde. Die Fotos des Vertragspartners, hier des Brautpaares, sind aufgrund des bestehenden Werkvertrages mit dem Fotografen gemäß Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO zulässig erstellt. Wenn der Fotograf während der Feier auch Gäste ablichtet oder Gäste zusammen mit dem Brautpaar fotografiert, kann er sich nicht mehr allein auf seine Vertragserfüllung berufen. Als rechtliche Grundlagen kommen hier aber die Einwilligung oder ein berechtigtes Interesse des Verantwortlichen oder eines Dritten gemäß Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO in Frage. Hier haben das Brautpaar (Dokumentation der Veranstaltung) und auch der Fotograf (Berufs- und Kunstfreiheit) ein berechtigtes Interesse an der Erstellung der Fotos, sofern nicht die Interessen oder

Grundrechte und Grundfreiheiten Betroffener überwiegen. Bei Prüfung der Interessenlage sind auch die vernünftigen Erwartungen der betroffenen Personen zu berücksichtigen, die im Falle einer Einladung zu einer Hochzeitsfeier davon ausgehen können, dass zu diesem Anlass auch Fotos erstellt werden. Dies ist ein gebräuchlicher und allseits akzeptierter Umstand. Auch bei Teilnahme an einer anderen Veranstaltung auf Einladung eines Veranstalters, geht die Erwartungshaltung der Gäste und auch des Veranstalters zumeist dahin, dass eine Dokumentation der Veranstaltung auch anhand von Fotografien stattfindet.
Anders wäre die Interessenlage zu bewerten, wenn die Aufnahmen verdeckt oder heimlich erstellt werden würden, die Fotos die Intimsphäre des Abgebildeten erfasst oder die Aufnahmen diskreditierend sind oder die Gefahr einer Diskriminierung bergen.
Von einer überwiegenden Schutzbedürftigkeit der Betroffenen ist auch bei Aufnahmen von Kindern auszugehen, weshalb hier ein Rückgriff auf ein berechtigtes Interesse wohl sehr genau zu prüfen ist und in solchen Fällen grundsätzlich eine Einwilligung für die Erstellung von Bildern bei den Sorgeberechtigten einzuholen ist. Die Interessenabwägung wird auch im Fall von Fotos, die Rückschlüsse auf besondere Kategorien personenbezogener Daten zulassen, also u. a. Religion, Gesundheit, Sexualleben und sexuelle Orientierung, immer zu Gunsten der betroffenen Person ausgehen. Für diese Fälle ist dann auch eine Einwilligung in die Erstellung der Aufnahme gemäß Art. 7 der DS-GVO notwendig.

IV. Verwendung von Fotos konkreter Person oder überschaubarer Gruppe

Das größte Interesse der Verantwortlichen liegt jedoch nicht in der Erstellung der Fotos, sondern in der anschließenden Verarbeitung oder Veröffentlichung der Bilder. Dies findet zumeist auf Webseiten statt oder in Informationsmaterialien wie Vereinszeitschriften. Für die Verbreitung und öffentliche Zurschaustellung von Fotos war bisher auf §§ 22 f. des Kunsturhebergesetzes (KUG) abzustellen. Ob das Kunsturhebergesetz neben der Datenschutz-Grundverordnung anwendbar ist oder bleibt, ist derzeit noch mangels entsprechender Öffnungsklausel in der DS-GVO umstritten (vgl. aber Urteil LG Frankfurt, 13. September 2018, 2-03 O 283/18 u. a.). Eine Anwendung

kann sich nur aus Art. 85 Abs. 1 DS-GVO im Hinblick auf die Verarbeitung zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken ergeben.
Ungeachtet dieser Diskussion ist das Ergebnis in der praktischen Auswirkung mit und ohne direkter Anwendung des KUG aber ähnlich, da die Wertungen des KUG im Rahmen der Interessensabwägung nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO einfließen.
Das KUG regelt insbesondere drei Fälle, bei denen es keiner Einwilligung der abgebildeten Person für die Verbreitung der Aufnahmen bedarf. Dies gilt für Bildnisse der Zeitgeschichte, Bilder bei denen Personen nur als Beiwerk neben einer Landschaft oder einer Örtlichkeit erscheinen und für Bilder von Versammlungen, Aufzügen u. Ä., an denen die abgebildete Person teilgenommen hat. Wenn das KUG nicht unmittelbar anwendbar wäre, würde die Verbreitung derartiger Aufnahmen nach Art. 6 Abs. 1 Satz 1 Buchstabe f) zu prüfen sein, denn auch hinsichtlich der Veröffentlichung von Fotos ist die weitere Verwendung an eine Rechtsgrundlage gebunden. Hier stehen sowohl die Einwilligung sowie Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO, also berechtigte Interessen, zur Verfügung. Während aus Sicht des Verantwortlichen eine Einwilligung immer die „schlechtere“ Verarbeitungsgrundlage ist, weil sie jederzeit widerrufen werden kann, ist im Rahmen von Veröffentlichungen oftmals zwingend auf diese zurückzugreifen. Hinsichtlich ihrer Voraussetzungen wird auf das WP 259 (Guidelines on Consent) der Art. 29 Gruppe verwiesen (http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051),

das nun auch in deutscher Sprache vorliegt (https://www.tlfdi.de/tlfdi/europa/artikel29gruppe/). Sofern eine Einwilligung einzuholen ist, muss dies vor der Fotoaufnahme geschehen. Dies kann auch mündlich erfolgen, allerdings muss der Verantwortliche gemäß Art. 7 Abs. 1 DS-GVO im Zweifel das Vorliegen einer

Einwilligung nachweisen können. Es wird daher empfohlen, die Einwilligungen wenigstens in Textform einzuholen. Es muss vor der Einwilligung immer über wesentliche Umstände informiert werden, auf die sich die Einwilligung bezieht, vor allem:

- die Identität des für die Verarbeitung Verantwortlichen
- für welchen Zweck die Fotos angefertigt werden
- ob und wenn ja, wo eine Veröffentlichung geplant ist
- an wen sich der Betroffene bei Datenschutzfragen (z. B. Widerspruch, Löschung) wenden kann,
- gemäß Art. 7 Abs. 3 DS-GVO, dass die betroffene Person das Recht hat, ihre Einwilligung jederzeit zu widerrufen und durch den Widerruf der Einwilligung die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt wird

Der Grund für den Rückgriff auf die Einwilligung im Rahmen von Veröffentlichungen ist in der oftmals zu Lasten der Verantwortlichen ausgehenden Interessensabwägung im Rahmen des Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO zu suchen. Es stehen sich hier die Interessen des Verantwortlichen z. B. an der Information und Werbung für Vereinsaktivitäten und die der betroffenen Personen gegenüber. Die Veröffentlichung hat grundsätzlich das Potential einen schweren Eingriff in die Rechte des Betroffenen darzustellen, weil die Bilder des Betroffenen einer unüberschaubaren Anzahl an Personen zum Zugriff bereitstehen und einer relativ schwer bis nicht kontrollierbaren Vervielfältigung ausgesetzt werden.

V. Aufnahmen von unüberschaubarer Menge an Personen

Davon zu unterscheiden ist die Verwertung von Aufnahmen, auf denen sich eine Vielzahl von Personen zumeist zusätzlich als sogenanntes Beiwerk oder im Rahmen von Übersichtsaufnahmen befinden, z. B. Zuschauerränge bei Sportveranstaltungen, Publikumsaufnahmen im Hintergrund künstlerischer Darbietungen. Grundsätzlich ist die Aufnahme von Bildern, auf denen sich eine Vielzahl von Personen befinden, die nicht im journalistischen Umfeld oder zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeit vorgenommen wird, nach den allgemeinen Regeln der Datenschutz-Grundverordnung (DS-GVO) zu bewerten. Auf der einen Seite liegen auch bei übersichtsartigen Bildaufnahmen nahezu immer personenbeziehbare

Daten vor, die dem Verbot mit Erlaubnisvorbehalt der DS-GVO unterfallen. Auf der anderen Seite ist es nicht möglich, bei Aufnahmen, auf denen viele Personen zu sehen sind, diese tatsächlich zu identifizieren oder zu kontaktieren. Daher ist die Einholung einer Einwilligung oder die Information der Abgelichteten über Ihre Rechte für die Fotografen nahezu unmöglich.
Die Verarbeitung solcher Bilder muss also den Grundsätzen des Art. 5 Abs. 1 DS-GVO entsprechen. Hierfür muss die Verarbeitung vor allem rechtmäßig erfolgen, Art. 5 Abs. 1 Nr. 1 Buchstabe a) DS-GVO. In Betracht kommen neben der datenschutzrechtlichen Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO nur eine Verarbeitung in Form der Erhebung nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO zur Wahrnehmung berechtigter Interessen. Da eine Einwilligung regelmäßig nicht einholbar sein wird, stellt die zweite Variante letztlich die Rechtsgrundlage dar, auf Grund derer Fotografien gefertigt werden können, sofern die dort genannten Voraussetzungen vorliegen. Dem stehen im Regelfall so lange keine schutzwürdigen Interessen entgegen, wie eine Ansammlung von Personen dargestellt wird, ohne dass eine Person oder wenige Personen im Fokus des Motivs stehen, weil dann nur ihre Sozialsphäre, nicht aber ihre Persönlichkeitssphäre betroffen ist.
Deutlich gründlicher muss die Abwägung bei Kindern und Jugendlichen erfolgen. Diese stellt die DS-GVO hinsichtlich der Abwägung im Rahmen des Art. 6 Abs. 1 Satz 1 Buchstabe f) unter besonderen Schutz. Im Zweifel fällt diese Abwägung zu Gunsten der Kinder aus, weswegen schon die Erstellung solcher Fotografien nur auf eine Einwilligung der sorgeberechtigten Person/en gestützt werden kann.

VI. Informationspflichten

Da die Anfertigung von Fotografien und gegebenenfalls auch ihre Verwendung den Regelungen der DS-GVO unterliegen, fordert diese neben der Rechtmäßigkeit der Datenverarbeitung in Art. 5 Abs. 1 Buchstabe a) auch die Transparenz der Datenverarbeitung. Was sich der Gesetzgeber unter Transparenz vorstellt, wird in den Art. 12 ff. DS-GVO geregelt. Die Informationspflichten nach der DS-GVO sind dabei umfassend und grundsätzlich gegenüber jedem Betroffenen zu erfüllen. Hierzu sind u. a. Angaben hinsichtlich des Zweckes, für den die Fotos erstellt werden, notwendig und die Angabe eines berechtigten Interesses, Angaben dazu, ob und wo eine Veröffentlichung der

Fotos geplant ist, eine genaue Bezeichnung der Medien für die Veröffentlichung und an wen sich die Betroffenen hinsichtlich datenschutzrechtlicher Fragestellungen wenden können.
Eine Ausnahme von den Informationspflichten insgesamt enthält Art. 11 Abs. 1 DS-GVO. Demnach ist ein Verantwortlicher nicht verpflichtet, zur bloßen Einhaltung der DS-GVO, zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren, falls für die Zwecke, für die die personenbezogenen Daten verarbeitet werden, die Identifizierung der betroffenen Person durch den Verantwortlichen nicht oder nicht mehr erforderlich ist. Mit anderen Worten: Die DS-GVO möchte verhindern, dass allein aus Gründen der Informationspflicht umfangreich personenbezogene Daten der betroffenen Personen verarbeitet werden und so ein kleiner oder moderater Eingriff in das informationelle Selbstbestimmungsrecht dieser Personen ein viel größeres Ausmaß erhält. Handelt es sich um ein Foto, auf dem eine größere Menschenmenge ohne erkennbaren Fokus abgebildet ist, hält der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit Art. 11 Abs. 1 DS-GVO insoweit für anwendbar. Damit entfällt in solchen Fällen insoweit die Informationspflicht. Keine Anwendung findet Art. 11 Abs. 1 DS-GVO allerdings bei kleineren überschaubaren Personengruppen oder gar einzelnen Personen, die im Fokus der Aufnahme stehen. Hier ist wenigstens eine Information nach Art. 13 Abs. 1 DS-GVO notwendig; auch im Falle einer Einwilligung.
Grundsätzlich empfiehlt es sich, diesen Informationspflichten beispielsweise durch gut sichtbare Aushänge am jeweiligen Veranstaltungsort und/oder beim Karten(ver)kauf bereits nachzukommen. Auf Nachfrage muss der Fotograf auch in der Lage sein, die vollständige Information nach Art. 13 DS-GVO bereitzustellen.

VII. Besondere Verarbeitungssituationen

Um der Vielfalt der Nutzungsmöglichkeiten von Fotoaufnahmen gerecht zu werden, wird im Folgenden auf eine Reihe von besonderen Verarbeitungssituationen eingegangen, um hier vor allem praxisrelevante Sachverhalte abzubilden.

Das Beschäftigungsverhältnis

Die Datenverarbeitung innerhalb des Beschäftigungsverhältnisses ist an strengen Maßstäben orientiert. Personenbezogene Daten von Beschäftigten durften und dürfen im Beschäftigungskontext nur dann verarbeitet werden, wenn dies zur Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses erforderlich ist. Dies ergibt sich aus § 26 Abs. 1 Bundesdatenschutzgesetz und aus § 27 Abs. 1 ThürDSG in Verbindung mit den §§ 79 bis 87 des Thüringer Beamtengesetzes, soweit der öffentliche Dienst betroffen ist. Die Veröffentlichung von Fotos von Mitarbeitern ist aber nach diesen Vorschriften regelmäßig nicht erforderlich. Die Interessenabwägung gilt im Beschäftigtenverhältnis nicht in gleicher Weise. Eine dahingehende eingeholte Einwilligung für die Nutzung von Mitarbeiterfotos ist daher schriftlich einzuholen und insbesondere im Hinblick auf ihre Freiwilligkeit zu prüfen.

Öffentlichkeitsarbeit von öffentlichen und nicht-öffentlichen Stellen

Bei der Verarbeitung von Fotos im Rahmen der Öffentlichkeitsarbeit von verantwortlichen Stellen ist zunächst erst einmal zu prüfen, ob das Medienprivileg anzuwenden ist. Die Nutzung für journalistische Zwecke kann daher für Pressemappen oder für die Erstellung eigener Zeitschriften oder Zeitungen einer Stelle zulässig sein. Wenn die Verarbeitung allerdings der reinen Werbung und Darstellung für die Stelle dient, sind bei nicht-öffentlichen Stellen die oben dargestellten Ausführungen zu beachten. Möglicherweise kann sich die Stelle auch auf das berechtigte Interesse hinsichtlich der Öffentlichkeitsarbeit und einer damit einhergehenden Veröffentlichung von Bildmaterial stützen. Bezüglich der öffentlichen Stellen, steht dem allerdings der Art. 6 Abs. 1 Satz 2 DS-GVO entgegen, wonach der Rückgriff auf Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO für Behörden in Erfüllung ihrer Aufgaben nicht gilt. Hier muss als Rechtsgrundlage der Art. 6 Abs. 1 Satz 1 Buchstabe e) DS-GVO in Verbindung mit den Landes- und Spezialgesetzen herangezogen werden. Hierbei ist ausschlaggebend, was für die Organisationskommunikation jeweils erforderlich ist.
Sowohl für öffentliche als auch für nicht-öffentliche Stellen bleibt aber festzuhalten, dass kein relevanter Unterschied zur früheren Rechtslage zu erkennen ist, wonach auch hier nur selten die Ausnahmen des § 23 KUG einschlägig gewesen sind.

Denn nicht jede Veranstaltung ist ein Ereignis der Zeitgeschichte und auch nicht jedes Fest eine Versammlung!

Vereine

Besonders die Arbeit der Vereine lebt oftmals von der Veröffentlichung von Fotoaufnahmen. Hier sind insbesondere Wettkämpfe, Mannschaftsfotos, Jubiläen, Jahrestage oder andere Vereinsfeierlichkeiten eingeschlossen. Doch auch diese Dokumentationen unterliegen der DS-GVO und bedürfen zu ihrer Verarbeitung einer rechtlichen Grundlage. Zwar kann sich diese zunächst aus dem Vereinszweck ergeben, also auf vertraglicher Grundlage im Rahmen einer Satzung beruhen, jedoch ist zur Durchführung der Mitgliedschaft, eine Verarbeitung von Fotos wohl regelmäßig nicht erforderlich. Die Veröffentlichung kann aber auf Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO gestützt werden, da der Verein ein berechtigtes Interesse daran hat, über das Vereinsgeschehen zu informieren. Hierfür können beispielsweise Mannschaftsfotos zur Dokumentation der Mannschaftsaufstellung eines Sportvereins auf der vereinseigenen Webseite eingestellt werden. Die gleichzeitige Veröffentlichung bei sozialen Netzwerken schließt dieses berechtigte Interesse jedoch nicht zwangsläufig mit ein. Weiterhin ist es über die Anwendung des Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO auch möglich, Fotos von offiziellen Vereinsveranstaltungen, Sportveranstaltungen oder Wettkämpfen zu veröffentlichen, da auch hier ein berechtigtes Interesse der Vereine daran besteht, über das Vereinsgeschehen zu berichten. Es muss sich allerdings um Fotos handeln, auf denen das Spielgeschehen als solches oder die Veranstaltung als solche erkennbar ist und nicht einzelne im Vordergrund stehende Personen. Sobald eine Person im Fokus steht, gelten die Vorschriften zu Einzelaufnahmen und deren Veröffentlichung unter Punkt IV oben.

Bezüglich der vereinsinternen Aktivitäten, wie interne Vereinsfeiern, Ausflüge, Geburtstage von Mitgliedern u. Ä. ist eine Veröffentlichung von Fotos nicht mehr von einem berechtigten Interesse des Vereins gedeckt. Hier gehen die Erwartungen der Mitglieder keinesfalls dahin, dass mit einer Veröffentlichung auf der Vereinsseite zu rechnen ist.

Da die Veröffentlichung eine fortwährende Form der Verarbeitung darstellt, ist eine Interessensabwägung über die Fortführung der Veröffentlichung erneut durchzuführen, wenn für widerstreitende Interessen Anhaltspunkte vorliegen. Dies kann beispielsweise dann der Fall sein, wenn eine Person sich mit der Bitte meldet, das veröffentlichte

Foto zu entfernen, auch wenn er hierfür keine Gründe aufführt. Gerade bei älteren Bildern wird sich ein solcher Anspruch unmittelbar aus Art. 17 Abs. 1 DS-GVO ableiten lassen. Bei Bildern jüngeren Datums ist vom Verantwortlichen zu prüfen, inwieweit die Veröffentlichung auch ohne Einwilligung zulässig wäre. Das kann nur dann der Fall sein, wenn ein berechtigtes Interesse des Vereins nach dem o. a. Grundsätzen besteht und die Interessenabwägung nicht aufgrund besonderer Umstände zugunsten des Abgebildeten zu treffen ist. Wenn das Interesse der betroffenen Person überwiegt, ist eine weitere Veröffentlichung nicht zulässig und das Foto muss entfernt oder die Person unkenntlich gemacht werden.

Kinder insbesondere in Kitas / Schulen

Die DS-GVO stellt den Schutz von Kindern bei der Verarbeitung ihrer Daten unter einen besonderen Vorbehalt. Dieser wird in Art. 6 Abs. 1 Satz 1 Buchstabe f) der DS-GVO formuliert.
Danach überwiegt stets das schutzwürdige Interesse der Kinder. Aus diesem Grund ist die Verarbeitung von Daten, wenn Kinder betroffen sind, nur aufgrund einer Einwilligung möglich, aufgrund einer vertraglichen Grundlage oder aufgrund gesetzlicher Regelungen. Für das Mannschaftsfoto im Verein, Aushänge in der Schule oder Kita, gilt daher, wenn Minderjährige erkennbar abgebildet werden, ist das Erstellen und auch das Veröffentlichen nur mit der Einwilligung der Sorgeberechtigten möglich.
Dies ist jedoch für Bildnisse eines Spielablaufs/Veranstaltungsablaufs dann nicht der Fall, wenn nur das Spielgeschehen oder der Veranstaltungsablauf dargestellt werden sollen, ohne dass erkennbar Kinder im Vordergrund abgebildet sind oder diese nur als sogenanntes „Beiwerk“ zu einer Übersichtsaufnahme erscheinen. Solche Aufnahmen werden zumeist zur Dokumentation von schulischen Veranstaltungen im Rahmen der Öffentlichkeitsarbeit erstellt. Sobald die Kinder jedoch erkennbar, einzeln oder in kleiner Gruppe und im Vordergrund abgebildet sind, das Bild also prägen, kann nicht mehr von Beiwerk ausgegangen werden und eine Einwilligung ist notwendig.

„Altbestände“ an Fotos

Hinsichtlich eines bereits vorliegenden Bildbestandes ist vom Verantwortlichen zu prüfen, ob diese bereits vorliegenden Aufnahmen auch datenschutzkonform weiterverwendet werden dürfen. Bei bestehen-

den Einwilligungen ist insbesondere für die mögliche Weiterverarbeitung von „Bestandsbildern“ darauf zu achten, dass diese Einwilligung auch den Anforderungen des Art. 7 DS-GVO genügt, d. h., wenn sie im Rahmen einer schriftlichen Erklärung, die noch andere Sachverhalte betrifft, abgegeben wurde, muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form, in einer klaren und einfachen Sprache erfolgen und von anderen Sachverhalten klar zu unterscheiden sein. Außerdem muss auf das Widerrufsrecht in der Einwilligung ausdrücklich hingewiesen werden. Die Einwilligung ist zudem nur dann freiwillig erteilt, wenn weder die Erfüllung des Vertrages noch die Erbringung der Dienstleistung von ihr abhängig gemacht werden. Im Rahmen der Einwilligung ist der Verantwortliche bezüglich der Erteilung der Einwilligung durch die betroffene Person zudem in der Nachweispflicht, gemäß Art. 7 Abs. 1 DS-GVO.

5.22 No risk no fun? Was bei der Meldung und im Umgang mit Datenpannen zu beachten ist

Mit Einführung der Datenschutz-Grundverordnung (DS-GVO) hat sich hinsichtlich des Verhaltens bei Datenpannen einiges geändert. Es besteht nun eine Pflicht zur Meldung einer solchen Verletzung des Schutzes personenbezogener Daten. Zudem müssen bei einer Meldung auch genaue Angaben zur Art der Datenverletzung, den betroffenen Datenkategorien sowie zu den betroffenen Personen gemacht werden. Nur beim Begriff „Risiko“ bleibt die Datenschutz-Grundverordnung noch ein wenig schwammig; deutsche Aufsichtsbehörden haben dort nachgebessert.

Bei der Meldung von Datenpannen hat sich mit der DS-GVO, im Gegensatz zu vielen anderen Bereichen, tatsächlich Wesentliches im Vergleich zur alten Rechtslage geändert. Bis zum 25. Mai 2018 waren nach § 42a des Bundesdatenschutzgesetzes (BDSG) der Aufsichtsbehörde nur Datenpannen bei bestimmten Datenkategorien zu melden.
Das hat sich geändert; mittlerweile ist der Aufsichtsbehörde jede Verletzung des Schutzes personenbezogener Daten zu melden, wenn eine solche Verletzung ein Risiko für die Rechte und Freiheiten natürlicher Personen darstellt.
Zum Begriff des Risikos haben die deutschen Aufsichtsbehörden ein gemeinsames Kurzpapier erstellt, da die DS-GVO selber den Begriff

des Risikos nicht klar definiert. Danach ist ein Risiko im Sinne der DS-GVO die Möglichkeit, dass ein Ereignis eintritt, das selbst einen Schaden darstellt, einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen, oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann. Das Risiko ergibt sich dabei aus einer zweiteiligen Gewichtung: Erstens die Schwere des Schadens und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten. Als mögliche Schäden nennt der Erwägungsgrund 75 physische, materielle und immaterielle Schäden.

Folglich hat die DS-GVO die Meldeschwelle gegenüber der Aufsichtsbehörde erheblich abgesenkt. Zwar ist die Prognoseentscheidung, ob ein solches Risiko durch eine Verletzung des Schutzes personenbezogener Daten besteht, die Aufgabe des jeweils Verantwortlichen, jedoch kann eine Meldepflicht nur dann sicher ausgeschlossen werden, wenn auch ein Risiko sicher ausgeschlossen werden kann.

Erleichterung bringt die DS-GVO allerdings hinsichtlich der Information betroffener Personen über eine solche Datenpanne. Diese Informationspflicht ist nur dann zwingend erforderlich, wenn ein *hohes* Risiko besteht, dass es zu einem Schadenseintritt kommt. Näheres können Sie dem Kurzpapier 18 der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder über das Risiko für die Rechte und Freiheiten natürlicher Personen entnehmen (https://www.tlfdi.de/mam/tlfdi/datenschutz/dsk_kpnr_18_risiko.pdf).

Hinsichtlich der Meldung ist Art. 33 der Datenschutz-Grundverordnung (DS-GVO) zu berücksichtigen. Danach hat der Verantwortliche die Pflicht, innerhalb von 72 Stunden nachdem die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde zu melden. Die Meldung muss inhaltlich den Anforderungen des Art. 33 Abs. 3 der DS-GVO gerecht werden. Sie muss unter anderem die Art der Verletzung, die Kategorien der Daten und die ungefähre Anzahl der betroffenen Personen sowie die Anzahl der betroffenen personenbezogenen Datensätze enthalten. Weiterhin sind der Name und die Kontaktdaten des Datenschutzbeauftragten anzugeben. Eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten

und eine Beschreibung der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung und Abmilderung möglicher, nachteiliger Auswirkungen sind ebenfalls beizufügen.
Im Fall einer Verletzung des Schutzes personenbezogener Daten mit einem voraussichtlich hohen Risiko für natürliche Personen ist bei der Benachrichtigung der betroffenen Personen vom Verantwortlichen zusätzlich Art. 34 der DS-GVO zu berücksichtigen. Hier werden die inhaltlichen Anforderungen an die Benachrichtigung erläutert. Der Verantwortliche hat hierbei in klarer und einfacher Sprache die Art der Datenverletzung anzugeben. Weiterhin sind der Name und die Kontaktdaten des Datenschutzbeauftragten zu nennen. Der Verantwortliche muss die wahrscheinlichen Folgen der Datenschutzverletzung für die betroffene Person beschreiben sowie die von ihm ergriffenen Maßnahmen zur Abmilderung der nachteiligen Auswirkungen oder zur Behebung der Verletzung erläutern.

Um jedem Verantwortlichen diese Meldeverpflichtung ein wenig zu erleichtern, hat der TLfDI ein Meldeformular erarbeitet, das unter folgender Internetadresse (https://www.tlfdi.de/tlfdi/europa/europaeischedsgvo/) zum Download bereitsteht.

5.23 Datenpannen und die Meldepflicht nach alter und neuer Gesetzgebung

In vergangenen Tätigkeitsberichten hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bemängelt, dass in Thüringen mit hoher Wahrscheinlichkeit nicht alle Meldungen nach § 42a BDSG-alt (Meldepflicht bei Datenpannen nach altem Recht) vorgenommen wurden (siehe S. 50f. 2. Tätigkeitsbericht für den nicht-öffentlichen Bereich). Die ersten Erfahrungen unter der neuen Rechtslage scheinen diesen Verdacht zu bestätigen.

In den ersten Monaten nach Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) erreichten 78 Meldungen nach Art. 33 DS-GVO den TLfDI. Eine Vielzahl dieser Meldungen hätte auch unter der alten Regelung gemeldet werden müssen. Dies legt nahe, dass der vom TLfDI gehegte Verdacht von zu wenigen Meldungen in den vergangenen Jahren nicht ganz zu Unrecht bestand.

In einigen dieser Fälle wurde vom TLfDI ein hohes Risiko durch die Verletzung des Schutzes personenbezogener Daten festgestellt. In solchen Fällen wird der Verantwortliche aufgefordert, die betroffenen Personen über den Vorfall zu informieren, soweit er dies noch nicht von sich aus vorgenommen hat. Wann ein solch hohes Risiko vorliegt ergibt sich immer aus der Art der Verletzung und der Kategorien der betroffenen Daten und muss für jeden Fall bewertet werden. Dies erfolgt zunächst durch eine eigene Bewertung des Vorfalls durch den Verantwortlichen im Rahmen der Meldung und anschließend durch den TLfDI. Wenn der TLfDI zu der Einschätzung gelangt, dass ein hohes Risiko für die Betroffenen vorliegt, kann er vom Verantwortlichen verlangen, diese Benachrichtigung der Betroffenen nachzuholen.

Die Meldungen selbst lassen sich grob in drei Kategorien einteilen.

1. Falschversendungen/Kuvertierfehler
2. unbefugte Zugriffe bzw. systemkompromittierende Hackerangriffe
3. Verlust und Diebstahl (PCs, Telefone, Laptops, Pads)

Einen Großteil der Meldungen, vor allem im öffentlichen Bereich, betreffen Falschversendungen oder Kuvertierfehler (1). Auch im nichtöffentlichen Bereich liegt hier die Meldungsquote bisher bei gut einem Drittel.

Weiterhin gibt es Meldungen zu unbefugten Zugriffen bzw. systemkompromittierenden Hackerangriffen (2) welche vor allem im nichtöffentlichen Bereich mehr als ein weiteres Drittel der Meldungen ausmachen. Mit etwas weniger Meldungen wurde der TLfDI auf Diebstahl bzw. Verlust von personenbezogenen Daten (3) hingewiesen.

Den Anstieg der Meldungen im Vergleich zu den Vorjahren führt der TLfDI auf zwei Faktoren zurück:
Zum einen ist das Problemfeld Datenschutz durch die erhöhte mediale Aufmerksamkeit und nicht zuletzt durch höhere Bußgelder mehr in den Mittelpunkt gerückt worden. Zum anderen sind die Meldevoraussetzungen für Datenverletzungen in der DS-GVO erheblich abgesenkt worden, wodurch ohnehin mit mehr Meldungen als vorher gerechnet werden musste. (siehe Beitrag 5.23 zu Meldevoraussetzungen)

5.24 Ja, ich will? Eine Übersicht zur schriftlichen, elektronischen und ausdrücklichen Einwilligung nach der Datenschutz-Grundverordnung

Eine Vielzahl der beim TLfDI eingegangenen Anfragen beschäftigten sich mit dem Thema Einwilligungen. Unsicherheiten bestanden hierbei insbesondere bei den Fragen, ob unter anderem Alteinwilligungen fortgelten und wann eine Einwilligung nach neuem Recht benötigt wird. Zudem gab es im Bereich der elektronischen Datenverarbeitung hohes Interesse daran, was im Rahmen von Newslettern und elektronischen Einwilligungserklärungen zu beachten ist.

Grundsätzlich muss gemäß Art. 5 Abs. 1 Buchstabe a) Datenschutz-Grundverordnung (DS-GVO) die Verarbeitung personenbezogener Daten rechtmäßig erfolgen. Wann eine Rechtmäßigkeit der Datenverarbeitung vorliegt, ergibt sich aus Art. 6 der DS-GVO, wo abschließend alle wichtigen Merkmale einer rechtmäßigen Datenverarbeitung aufgeführt sind. Die Einwilligungserklärung der betroffenen Personen stellt nach Art. 6 Abs. 1 Buchstabe a) der DS-GVO eine solche Rechtsgrundlage für eine erfolgende Datenverarbeitung dar. Im Rahmen der Einwilligungserklärung darf der betroffenen Person jedoch keine Entscheidungsmacht suggeriert werden, die so tatsächlich nicht besteht, z. B. wenn die Verarbeitung auch auf eine andere Rechtsgrundlage nach Art. 6 Abs. 1 DS-GVO gestützt werden kann. Sofern die datenverarbeitende Stelle bei der betroffenen Person eine Einwilligungserklärung einholt, signalisiert sie ihr, dass es für die Zulässigkeit einer Datenverarbeitung allein auf ihr Einverständnis ankommen soll. Dann aber wäre es in sich widersprüchlich und damit unzulässig, wenn die datenverarbeitende Stelle im Falle der Verweigerung oder Unwirksamkeit der Einwilligung alternativ doch wieder auf einen gesetzlichen Erlaubnistatbestand zurückgreifen könnte (Working Paper Nr. 259: „Leitlinien in Bezug auf die Einwilligung“ der Art. 29-Datenschutzgruppe, S. 27; Buchner/Petri in Kühling/Buchner, Kommentar zur DS-GVO und BDSG, Art. 6, Rdnr. 23.). Daher sollte die Einwilligung als Rechtsgrundlage für die Verarbeitung nur dann herangezogenen werden, wenn die Verarbeitung auf keinen der anderen Sachverhalte in Art. 6 Abs. 1 Buchstabe b) bis f) DS-GVO gestützt werden kann. Zwar steht die Einwilligung als Rechtsgrundlage gleichwertig neben den anderen Erlaubnistatbeständen, ist aber als Rechtsgrundlage für eine Datenverarbeitung deutlich unzuverlässiger, da der jederzeit mögliche Widerruf der Einwilligungserklärung dazu führt, dass die betroffene Person die Löschung der sie betreffenden Daten verlangen kann und der Verantwortliche verpflichtet ist, diese Daten ohne unangemessene Verzögerung zu löschen.

I. Einwilligungserklärungen nach der Datenschutz-Grundverordnung

Die DS-GVO definiert die Einwilligung in Art. 4 Nr. 11 als eine von „der betroffenen Person freiwillig für den bestimmen Fall, in infor-

mierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“. Sogenannte „Opt-out“-Verfahren gehören damit der Vergangenheit an, da solche Verfahren keine eindeutig bestätigende Handlung darstellen.
Eine Besonderheit der DS-GVO hinsichtlich Einwilligungen ist, dass die Bedingung einer in schriftlicher Form verfassten Einwilligung aus dem alten § 4a Bundesdatenschutzgesetz-alt (BDSG-alt) weggefallen ist. Der Verantwortliche muss jedoch nach Art. 7 Abs. 1 der DS-GVO, der die Bedingungen für eine Einwilligungserklärung regelt, nachweisen können, dass die betroffene Person wirksam in die Verarbeitung ihrer Daten eingewilligt hat, sodass die Schriftlichkeit eine gewisse Nachweis-Bedeutung behalten hat. Die Einwilligung muss wie bereits zuvor freiwillig erfolgen.
In Art. 7 Abs. 4 der DS-GVO wird das sogenannte Kopplungsverbot geregelt, wonach entscheidend ist, inwieweit die Erfüllung eines Vertrages von der Einwilligung in die Verarbeitung der personenbezogenen Daten, die für eine Erfüllung des Vertrages nicht automatisch erforderlich sind, abhängig gemacht werden kann. Ein weiteres Kriterium für das Vorliegen einer unfreiwilligen Einwilligungserklärung ist das Bestehen eines Ungleichgewichts zwischen dem Verantwortlichen und der betroffenen Person. Es liegt dann keine Freiwilligkeit vor, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eingewilligt werden kann, obwohl dies im Einzelfall angebracht ist, z. B. wenn personenbezogene Daten neben der Erhebung und Speicherung auch veröffentlicht werden sollen.
Eine Einwilligungserklärung muss zudem in „informierter Weise“ abgegeben werden. Hierbei ist zu beachten, dass die betroffene Person abschätzen kann, welche Auswirkungen die Erteilung einer Einwilligung für sie hat. Die betroffene Person muss die Umstände der Datenverarbeitung, sowie die Tragweite ihrer Einwilligung eindeutig und klar erkennen können. Erforderlich ist daher die Angabe der verwendeten Daten (z. B. Name, Adresse, Telefonnummer, E-Mail, Fotoaufnahmen), zu welchem Zweck diese verarbeitet werden (z. B. Zusenden von Angeboten, Produktvorschläge, Newsletter-Abo, Veröffentlichung von Fotos zur Außendarstellung eines Unternehmens oder Vereins, etc.), wer der Verantwortliche ist, wie dieser zu erreichen ist

und an welche Dritte die Daten im Falle der Übermittlung weitergegeben werden. Bei den zu nennenden Zwecken ist darauf zu achten, dass zwischen den einzelnen Zwecken differenziert wird und für jeden Zweck einzeln die Einwilligung einzuholen ist (z. B. durch Ankreuzoptionen für die einzelnen Zwecke). Als Orientierungsrahmen für Art und Umfang der Informationspflichten gelten die Angaben in Art. 13 und 14 der DS-GVO. Diese Informationspflichten sind jedoch zusätzlich zu erfüllen z. B. mit dem Verweis auf Informationsbroschüren, Aushänge oder FAQs auf einer Homepage. Damit soll sichergestellt werden, dass die betroffene Person in „informierter Weise“ alle relevanten Informationen zur Verarbeitung ihrer personenbezogenen Daten erhält.

Eine weitere Voraussetzung für Einwilligungserklärungen in schriftlicher Form in Bezug auf Datenverarbeitung und weiterer datenschutzrechtlicher Sachverhalte ist, dass die Bitte um die Einwilligung in verständlicher, leicht zugänglicher Form sowie in einer klaren und einfachen Sprache verfasst wurde. Darüber hinaus muss die Bitte um Einwilligung von anderen Sachverhalten klar unterscheidbar sein im Sinne von Art. 7 Abs. 2 der DS-GVO. Informationen sind demnach so aufzubereiten, dass sie für den durchschnittlichen Verbraucher ohne juristische Vorbildung zugänglich und verständlich sind.

Weiterhin ist gemäß Art. 7 Abs. 3 der Datenschutz-Grundverordnung auf das Widerrufsrecht der betroffenen Person vor Abgabe der Einwilligung hinzuweisen. Sofern eine Einwilligung widerrufen wird, ist die bis dahin rechtmäßig erfolgte Verarbeitung von diesem Widerruf nicht berührt. Mit dem Zeitpunkt des Widerrufs hat die betroffene Person nach Art. 17 Abs. 1 Buchstabe b) der DS-GVO das Recht, von dem Verantwortlichen zu verlangen, dass die sie betreffenden personenbezogenen Daten unverzüglich gelöscht werden. Wurden die Daten veröffentlicht, kann die betroffene Person zudem ihr Recht auf Vergessenwerden nach Art. 17 Abs. 2 DS-GVO gegenüber dem Verantwortlichen geltend machen. Es ist darauf zu achten, dass der Widerruf der Einwilligungserklärung so einfach wie die Erteilung der Einwilligung sein muss, was insbesondere bei elektronischen Einwilligungen zu beachten ist. Für weiterführende Informationen sind die vom Europäischen Datenschutzausschuss erarbeiteten „Guidelines on Consent“ („Leitlinien zur Einwilligung“) zu empfehlen, die mittlerweile auch in deutscher Übersetzung vorliegen. Diese Leitlinien bieten eine gründliche Analyse und helfen bei der Vertiefung der rechtlichen Bedeutung des Begriffes „Einwilligung“. Eine Arbeitshilfe zum

Thema Einwilligungserklärung wird auf der Webseite des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zur Verfügung gestellt.
Sofern der Verantwortliche Einwilligungen vor dem Inkrafttreten der Datenschutz-Grundverordnung am 25. Mai 2018 eingeholt hat, gelten diese fort, sofern sie den Bedingungen der Datenschutz-Grundverordnung entsprechen (siehe Erwägungsgrund 171, Satz 3 DS-GVO). Die bisher rechtswirksam erteilten Einwilligungen erfüllen grundsätzlich diese Bedingungen. Jedoch gelten Einwilligungen nicht fort, wenn ein Verstoß gegen die Freiwilligkeit, insbesondere gegen das Kopplungsverbot vorliegt. Ob diese Voraussetzungen gegeben sind, ist vom Verantwortlichen anhand der bereits erwähnten Voraussetzungen und Leitlinien des Europäischen Datenschutzausschusses sorgfältig zu prüfen.

II. Einwilligungserklärung von Kindern

In Art. 8 der DS-GVO wurde eine eigene rechtliche Regelung getroffen, die die Bedingungen für Einwilligungserklärungen von Kindern in Bezug auf Informations- und Kommunikationsdienstleistungen festschreibt (z. B. Internet Videotelefonie-Dienste, soziale Netzwerke). Demnach ist eine Einwilligung in die Verarbeitung von personenbezogenen Daten, die einem Kind bei einem Angebot von Anbietern für Informations- und Kommunikationsdienstleistungen direkt gemacht wird, rechtmäßig, wenn das Kind das sechzehnte Lebensjahr vollendet hat. Sofern das Kind noch nicht 16 Jahre alt ist, ist die Verarbeitung rechtmäßig, sofern die Einwilligung durch den Erziehungsberechtigten erteilt wird oder mit dessen Zustimmung erfolgt. Zusätzlich wurde geregelt, dass die EU-Mitgliedstaaten eigene Rechtsvorschriften zur Altersgrenze im Rahmen einer solchen Einwilligung treffen können, jedoch dürfte diese dann nicht unter dem vollendeten dreizehnten Lebensjahr liegen. Hiervon hat der deutsche Gesetzgeber keinen Gebrauch gemacht.
Daneben müssen die übrigen Wirksamkeitsvoraussetzungen des Art. 6 Abs. 1 Buchstabe a) und Art. 7 DS-GVO vorliegen. In Fällen von erteilten Einwilligungserklärungen Minderjähriger außerhalb von Art. 8 der DS-GVO kommt es zudem auf die Einsichtsfähigkeit der Minderjährigen in Bezug auf die Verwendung ihrer personenbezogenen Daten an. Dies wird am jeweiligen Einzelfall beurteilt und hängt zum einen von der Fähigkeit des Minderjährigen zu selbständigen und

verantwortungsbewusstem Handeln ab und zum anderen von Art und Zweck der konkreten Datenpreisgabe. Art. 8 DS-GVO geht daher von einer Einsichtsfähigkeit des Minderjährigen ab der Vollendung des 16. Lebensjahres aus. Jedoch nur im Rahmen dieses Anwendungsbereichs.

III. Einwilligung im Beschäftigungsverhältnis

Aufgrund des bestehenden Über-/Unterordnungsverhältnisses zwischen Arbeitgeber und Beschäftigten kommt eine freiwillige und damit wirksame Einwilligung regelmäßig nicht in Betracht. Jedoch fehlt im BDSG bzw. der DS-GVO ein grundsätzlicher Ausschluss der Einwilligung im Beschäftigungskontext. § 26 Abs. 2 BDSG enthält nunmehr restriktive Regelungen hinsichtlich der Freiwilligkeit einer Einwilligung. Es ist möglich, dass Beschäftigte in Datenverarbeitungen dann freiwillig einwilligen können, wenn für sie dadurch ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird. Das gleiche gilt, wenn Arbeitgeber und Beschäftigte gleichgelagerte Interessen verfolgen. Es sind jedoch aufgrund des Über-/Unterordnungsverhältnisses hohe Anforderungen an den Zweck der Einwilligung zu stellen, sofern eine Verarbeitung von Beschäftigtendaten im Einzelfall auf eine Einwilligung gestützt werden soll.
In der Praxis werden daher Einwilligungen überwiegend in Konstellationen möglich sein, die nicht das Arbeitsverhältnis als solches, sondern Zusatzleistungen des Arbeitgebers betreffen (wie z. B. bei der Gestattung privater Nutzung dienstlicher Fahrzeuge, Telefone und EDV-Geräte, Einführung eines Gesundheitsmanagements zur Gesundheitsförderung, Aufnahme in Geburtstagslisten).
Für die Einwilligung im Beschäftigungsverhältnis ist die Schriftform angeordnet, um die informationelle Selbstbestimmung der betroffenen Beschäftigten zu sichern. Gleichzeitig wird hiermit die Nachweispflicht des Art. 7 Abs. 1 DS-GVO des Arbeitsgebers konkretisiert. Der Arbeitgeber hat ferner die Pflicht den Beschäftigten in Textform über den Zweck der Datenverarbeitung, das bestehende jederzeitige Widerrufsrecht sowie die damit verbundenen Folgen nach Art. 7 Abs. 3 DS-GVO aufzuklären.
Den TLfDI erreichte im Berichtszeitraum eine Anfrage zur Veröffentlichung von Namen einzelner Musiker eines Orchesters auf der Webseite des dafür verantwortlichen Vereins. Hierbei mussten auch die

entsprechenden Grundsätze für die Einwilligung im Beschäftigungsverhältnis angewendet werden. Hinsichtlich der Veröffentlichung der Namen der Musiker im Orchester war eine Einwilligung seitens des Vereinsvorstand bei den Musikern einzuholen, da sämtliche anderen Rechtsgrundlagen des Art. 6 Abs. 1 Buchstabe b) bis f) DS-GVO nicht einschlägig waren. Insbesondere konnte die Veröffentlichung nicht auf Art. 6 Abs. 1 Buchstabe f) DS-GVO gestützt werden, da die Veröffentlichung ohne jegliche Einbeziehung des Betroffenen erfolgte. Die Freiwilligkeit einer solchen Einwilligungserklärung ergab sich hier daraus, dass eine Veröffentlichung im Interesse des betroffenen Musikers erfolgte, da die Veröffentlichung auch der Eigenwerbung des Musikers diente.

IV. Elektronische Einwilligung nach der Datenschutz-Grundverordnung

Bei elektronischen Einwilligungserklärungen ist sicherzustellen, dass der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat – bisheriger § 15 Telemediengesetz (TMG) und § 94 Telekommunikationsgesetz (TKG). Die Vorgaben hierzu werden im Rahmen der E-Privacy-Verordnung angepasst. Erwägungsgrund 32 führt hierzu aus, dass eine unmissverständliche und eindeutige Erklärung z. B. durch Anklicken eines Kästchens beim Besuch einer Webseite vorliegen muss. Das bedeutet, dass es sich dabei um die Einholung einer Einwilligung im Wege des sogenannten „Opt-In"-Verfahrens handelt, indem der Betroffene seine Einwilligung in die Datenverarbeitung aktiv erklärt. Am wirksamsten ist hier das sogenannte „Double-Opt-in"-Verfahren, um eine eindeutige Bestätigung der betroffenen Person zu gewährleisten. Insbesondere bei der Einwilligung in die Verarbeitung von besonderen Kategorien personenbezogener Daten nach Art. 9 DS-GVO ist dieses Verfahren anzuwenden (Working Paper Nr. 259 „Leitlinien in Bezug auf die Einwilligung" der Art. 29-Datenschutzgruppe, S. 23). Beim „Double-Opt-In"-Verfahren muss der Eintrag in die Abonnentenliste in einem zweiten Schritt bestätigt werden, wobei hierzu eine E-Mail-Nachricht mit der Bitte um Bestätigung an die eingetragene Kontaktadresse versandt wird. Sofern es sich um ein erwünschtes „Opt-in" handelt, kann der Abonnent den Bestätigungslink anklicken, um seine Zustimmung zu erteilen. Sofern es sich um einen missbräuchlichen Eintrag handelt, kann die E-Mail zur Bestätigungs-Aufforderung ignoriert werden. Eine Registrierung als z. B. E-Mail

Newsletter-Abonnent wird erst dann rechtlich wirksam, wenn diese auf dem zuvor beschriebenen „Opt-in"-Weg bestätigt wird. Zudem sind die bereits aufgeführten Bedingungen für eine wirksame Einwilligungserklärung ebenfalls zu erfüllen.

V. Einwilligungen für besonders sensible Kategorien personenbezogener Daten

Besonderheiten ergeben sich bei Einwilligungserklärungen, die nach Art. 9 Abs. 1 der Datenschutz-Grundverordnung besondere Kategorien personenbezogener Daten betreffen. Grundsätzlich ist es untersagt personenbezogene Daten zu verarbeiten „aus denen die rassische und ethnische Herkunft, politische Haltung, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen". Zu dieser Kategorie der besonderen personenbezogenen Daten gehören auch genetische Daten, biometrische Daten zur eindeutigen Identifizierung, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Eine Verarbeitung dieser Daten ist nach Art. 9 Abs. 2 der DS-GVO nur dann zulässig, wenn entweder eine ausdrückliche Einwilligung der betroffenen Person in die Verarbeitung dieser besonderen Kategorie von personenbezogenen Daten für die von dem Verantwortlichen festgelegten Zwecke vorliegt oder sofern kein anderer Ausnahmetatbestand nach Art. 9 Abs. 2 Buchstabe b) bis j) der DS-GVO besteht. Insbesondere bei handwerklichen Gesundheitsberufen (z. B. Optiker, technischer Orthopäde) ist vom Verantwortlichen eine Einwilligungserklärung hinsichtlich der Verarbeitung besonderer Kategorien personenbezogener Daten einzuholen, da hier der Ausnahmetatbestand des Art. 9 Abs. 2 Buchstabe h) der DS-GVO nicht eingreift. Im Rahmen dieses Ausnahmetatbestands sind die in Art. 9 Abs. 3 der Datenschutz-Grundverordnung genannten Garantien zu erfüllen, wonach jene besonderen Daten-Kategorien nur dann zum Zweck der Gesundheitsvorsorge verarbeitet werden dürfen, wenn die Daten von Personen verarbeitet werden, die einer Berufsgeheimnispflicht oder einer Geheimhaltungspflicht national zuständiger Stellen unterliegen. Eine solche Geheimhaltungspflicht ergibt sich zum einen aus dem Gesetz (insbesondere § 203 Abs. 1 Strafgesetzbuch), zum anderen aus von Kammern erlassenen Berufsordnungen und aus berufsständischen Satzun-

gen. Für Optiker und technische Orthopäden existieren solche Vorschriften nicht, die eine Geheimhaltungspflicht gegenüber den betroffenen Personen begründet.
Die Einwilligungserklärung für besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 2 Buchstabe a) der Datenschutz-Grundverordnung muss neben den Bedingungen nach Art. 6 Abs. 1 Buchstabe a) und Art. 7 der DS-GVO weitere Voraussetzungen erfüllen. Eine solche Einwilligungserklärung muss sich explizit auf die Verarbeitung sensibler Daten beziehen. Es muss auf die Sensibilität bzw. den besonderen Charakter der zu verarbeitenden Daten hingewiesen werden, so dass der betroffenen Person bewusst wird, dass sie sich mit ihrer ausdrücklichen Erklärung möglicherweise außerhalb des besonderen rechtlichen Schutzes begibt. Zudem ist der Inhalt der Einwilligung so zu formulieren, dass ein erhöhtes Maß an Bestimmtheit und Genauigkeit gegeben ist.

VI. Einwilligung gegenüber Behörden

Aus seiner Prüfpraxis weiß der TLfDI, dass die öffentlichen Stellen in Thüringen in bestimmten Fällen auch gerne zu Instrument der Einwilligung gegriffen haben. War doch entweder die Rechtsgrundlage der Verarbeitung etwas sperrig oder zu eng und steigerte die Einwilligung doch oftmals die Akzeptanz bei den betroffenen Personen. Damit ist es nun in den allermeisten Fällen vorbei! Die DS-GVO stellt in Erwägungsgrund 43 klar, dass die Einwilligung eines Bürgers gegenüber einer Behörde nicht freiwillig abgegeben werden kann, weil zwischen der betroffenen Person und dem Verantwortlichen in Anbetracht der Umstände ein klares Ungleichgewicht besteht. Eine wirksame Einwilligung gegenüber öffentlichen Stellen kommt daher nur in Betracht, wenn ein solches Ungleichgewicht nicht besteht. Hinzu kommt, dass bei einem Widerruf der Einwilligung jegliche Datenverarbeitung für die Zukunft rechtswidrig wird. Das bedeutet, dass alle personenbezogenen Daten gelöscht werden müssen. Damit kommt die Einwilligung im Bereich des staatlichen Handelns nur in einigen Nischen in Betracht (s. beispielsweise Nummer 5.21 zu Fotografien in Kindertageseinrichtungen). Als Beispiel sei hier die Einwilligung in die Speicherung der E-Mail-Adresse für das Abonnement eines Newsletters genannt. In allen anderen Fällen muss die Datenverarbeitung auf der Rechtsgrundlage einer gesetzlichen Ermächtigung basieren.

Ob eine Einwilligungserklärung für bestimmte Verarbeitungssituationen erforderlich ist, sollte durch den Verantwortlichen sorgfältig geprüft werden. Ein Widerruf der Einwilligungserklärung führt dazu, dass die betroffene Person die Löschung der sie betreffenden Daten verlangen kann und der Verantwortliche verpflichtet ist, diese Daten ohne unangemessene Verzögerung zu löschen.

5.25 Risikobeurteilung: Wann und wie muss ein Verantwortlicher eine Datenschutz-Folgenabschätzung durchführen?

Die Datenschutz-Folgenabschätzung (DSFA) ist eine Neuerung der Datenschutz-Grundverordnung (DS-GVO) und ersetzt die bisher nach Richtlinie 95/46/EG geregelte Vorabkontrolle. Verantwortlichen ist oft nicht ganz klar, wann eine solche DSFA durchzuführen ist.

Eine Datenschutz-Folgenabschätzung (DSFA) ist die Pflicht des Verantwortlichen zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten. Sie ist in Art. 35 der DS-GVO geregelt und stellt eine der wichtigsten Neuerungen der DS-GVO gegenüber dem Bundesdatenschutzgesetz dar.
Es stellt sich dabei immer wieder die Frage, wann eine solche DSFA eigentlich zwingend durchzuführen ist. Eine DSFA ist immer dann durchzuführen, wenn die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko zur Folge hat. Sie befasst sich insbesondere mit Abhilfemaßnahmen, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Verordnung nachgewiesen werden kann (Art. 35 Abs. 1, 7 DS-GVO sowie Erwägungsgrund 84, 90). Die Entscheidung über die Durchführung oder Nichtdurchführung der DSFA ist vom Verantwortlichen mit Angabe der maßgeblichen Gründe für den konkreten Verarbeitungsvorgang schriftlich zu dokumentieren.
Ob eine DSFA durchzuführen ist, ergibt sich aus einer Abschätzung der Risiken der Verarbeitungsvorgänge. Dieses Vorgehen wird auch als Schwellwertanalyse bezeichnet. Die Bestimmung, wann es sich um ein hohes Risiko handelt, wird nach der Risikobeurteilung vorgenommen, die sich in drei Stufen gliedert. Zunächst erfolgt die Risiko-

Identifikation, danach die Abschätzung der Eintrittswahrscheinlichkeit und Schwere möglicher Schäden und abschließend die Zuordnung zu den Risikoabstufungen. Wenn diese Risikobeurteilung anhand der drei zu absolvierenden Stufen ein hohes Risiko ergibt, ist eine DSFA zwingend durchzuführen.

Art. 35 Abs. 3 der DS-GVO benennt einige Faktoren, die wahrscheinlich zu einem hohen Risiko führen im Sinne des Art. 35 Abs. 1 der DS-GVO. Als Hilfestellung bei der Risikobeurteilung haben die Datenschutzaufsichtsbehörden dazu eine nicht-abschließende Liste mit Verarbeitungstätigkeiten, bei denen eine DSFA durchzuführen ist, erstellt. Diese Liste ist auch auf der Webseite des TLfDI zu finden unter folgendem Link: https://www.tlfdi.de/mam/tlfdi/datenschutz/dsfa_muss-liste_04_07_18.pdf. Sobald ein Verantwortlicher eine auf der Liste genannte Form der Verarbeitung ausführt, muss er vor Beginn der Verarbeitung auch eine DSFA vornehmen. Darüber hinaus ist zu beachten, dass der Verantwortliche dann in jedem Fall auch einen Datenschutzbeauftragten bestellen muss. Diese Verpflichtung ist in § 38 Bundesdatenschutzgesetz festgeschrieben.

Ausdrücklich geregelt ist auch der Fall, dass eine DSFA dann erforderlich ist, wenn eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen erfolgt, die sich auf automatisierte Verarbeitung einschließlich Profiling stützt und zudem als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen.

Weiterhin ist eine DSFA auch dann obligatorisch, wenn eine umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 oder personenbezogene Daten über strafrechtliche Verurteilungen gemäß Art. 10 der DS-GVO erfolgt.

Wann eine Verarbeitung als umfangreich gilt, ist je nach Situation zu bestimmen. Nicht als umfangreich soll dabei die Verarbeitung personenbezogener Daten von Patienten eines einzelnen Arztes oder sonstigen Angehörigen eines Gesundheitsberufes oder Mandanten eines einzelnen Rechtsanwaltes gelten, wie in Erwägungsgrund 91 am Ende

dargestellt. Wenn Verarbeitungsvorgänge dazu dienen personenbezogene Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, eine große Zahl von natürlichen Personen betroffen ist und gegebenenfalls besondere Kategorien von Daten verarbeitet werden, die ein hohes Risiko mit sich bringen oder bei denen eine neue Technologie bei der Verarbeitung eingesetzt wird, ist eine DSFA erforderlich. Letztlich ist auch bei einer systematischen umfangreichen und weiträumigen Überwachung öffentlich zugänglicher Bereiche, insbesondere beim Einsatz von opto-elektronischen Vorrichtungen, eine DSFA zwingend notwendig.
Eine DSFA ist grundsätzlich vor der Aufnahme der zu betrachtenden Verarbeitungsvorgänge durchzuführen. Auch bereits bestehende Verarbeitungsvorgänge können unter die Pflicht einer DSFA fallen, zum Beispiel, wenn Veränderungen in den Verarbeitungsvorgängen vorgenommen werden. Da eine DSFA meist nicht ad hoc in wenigen Tagen erstellt werden kann, muss sie rechtzeitig, beispielsweise auch unterstützt durch ein allgemeines Datenschutz-Managementsystem auf den Weg gebracht werden.
Wie eine solche DSFA durchzuführen ist, wird im Folgenden näher erläutert, denn wenn Verantwortliche eine DSFA im Sinne der Datenschutz-Grundverordnung durchführen müssen, stellt sich ihnen oft die nicht weniger schwierige Frage nach dem Wie der Durchführung. In dieser Angelegenheit stehen die Aufsichtsbehörden den Verantwortlichen helfend zur Seite. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder widmete sich diesem Thema und hat alle relevanten Informationen dazu im Kurzpapier Nr. 5 zusammengetragen.
Die formellen Anforderungen an die Durchführung einer Datenschutz-Folgenabschätzung (DSFA) ergeben sich aus der DS-GVO, speziell aus Art. 35 sowie den Erwägungsgründen 84, 90, 91, 92 und 93. Bei der verwendeten Durchführungsmethode wird dem Verantwortlichen ein gewisser Spielraum gelassen. Werden bestehende Methoden oder Standards eingesetzt, ist allerdings zu beachten, dass die Anforderungen der DS-GVO immer vorrangig zu beachten sind.
Da es sich bei einer DSFA um einen umfangreichen Prozess handelt, ist eine sorgfältige Vorbereitung geboten. Zunächst sollte ein DSFA-Team zusammengestellt werden. Dieses besteht aus einem interdisziplinären Team der Bereiche Datenschutz, Risikoermittlung und Fachprozesse. Der Datenschutzbeauftragte selbst steht während des

Gesamtprozesses beratend zur Seite, da es Aufgabe des Verantwortlichen ist, die DSFA durchzuführen. In einem weiteren Schritt ist der Beurteilungsumfang festzulegen, in dem die zu prüfenden Datenverarbeitungsvorgänge von anderen Geschäftsprozessen abgegrenzt werden. Daraufhin werden dann die ermittelten Datenflüsse unter Berücksichtigung ihrer Verwendungswecke beschrieben. Anschließend erfolgt eine Bewertung, ob der durch die Datenverarbeitung bewirkte Eingriff in die Rechte und Freiheiten betroffener Personen verhältnismäßig zum angestrebten Verwendungsweck ist und dafür auch tatsächlich notwendig ist. Abschließend werden die Rechtsgrundlagen für die jeweilige Verarbeitung bestimmt und dokumentiert.
Wenn diese Vorbereitungsphase abgeschlossen ist, kann die eigentliche Durchführung erfolgen. Dazu ist es als erstes notwendig die Risikoquellen für die Rechte und Freiheiten der betroffenen Personen zu identifizieren. Danach sind die festgestellten Risiken zu bewerten. Dies erfolgt anhand der Eintrittswahrscheinlichkeit und der Schwere des daraus resultierenden potenziellen Schadens. Potenzielle Schäden können physischer, materieller oder immaterieller Art sein.
Anschließend müssen die einzelnen ermittelten Risiken durch geeignete Abhilfemaßnahmen ausgeschlossen oder eingedämmt werden. Dies wird durch die Implementierung technischer und organisatorischer Maßnahmen erreicht. Verbleibende Restrisiken werden ermittelt und dokumentiert. Nach Abschluss dieser Maßnahmen wird der DSFA-Bericht erstellt, der gemäß Art. 35 Abs. 7 der DS-GVO die geplanten Verarbeitungsvorgänge und deren Verarbeitungszwecke systematisch beschreibt. Hinzu kommt eine zweckbezogene Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge und die Beschreibung und Beurteilung von Risiken und geplante Abhilfemaßnahmen zur Risikoeindämmung. Abschließend sind die ermittelten Restrisiken darzustellen und zu entscheiden wie damit umzugehen ist.
Gemäß Art. 5 Abs. 2 der DS-GVO hat der Verantwortliche eine umfassende Dokumentations-und Rechenschaftspflicht mit der die Einhaltung der DS-GVO insgesamt nachgewiesen werden soll. Der DSFA-Bericht ist somit auch als Teilstück zur Umsetzung der Rechenschaftspflicht des Verantwortlichen zu verstehen.
Ergibt eine DSFA, dass trotz technischer und organisatorischer Maßnahmen zur Risikoeindämmung weiterhin ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht (Restrisiko), muss

nach Art. 36 DS-GVO der Verantwortliche die zuständige Aufsichtsbehörde konsultieren. Die Aufsichtsbehörde prüft im Konsultationsverfahren die vorgenommene Datenschutz-Folgenabschätzung und spricht Empfehlungen aus, wie das noch vorhandene hohe Restrisiko verringert werden kann. Die Aufsichtsbehörde kann zudem ihre Befugnisse aus Art. 58 der DS-GVO ausüben, also Warnungen aussprechen oder Anordnungen treffen, um die Verarbeitung in Einklang mit der DS-GVO zu bringen. Der Verantwortliche entscheidet dann im Hinblick auf die Empfehlungen der Aufsichtsbehörde, ob oder wie die Verarbeitungsvorgänge angesichts der verbleibenden Restrisiken durchgeführt werden können und welche zusätzlichen Abhilfemaßnahmen in diesem Fall eventuell zum Einsatz kommen könnten.
Die DSFA ist zudem ein lebendiger Prozess, der nicht statisch zu bewerten ist. Bei Änderungen oder Anpassungen in den Datenverarbeitungsvorgängen oder bei Einführung neuer Datenflüsse ist die DSFA regelmäßig zu wiederholen. Auch laufende Verarbeitungsvorgänge sind zu beobachten und darauf zu prüfen, ob sich möglicherweise die Risiken verändern.

5.26 Datenschutz-Schutzziele und das Standard-Datenschutzmodell

Das Standard-Datenschutzmodell (SDM) wurde von den unabhängigen Datenschutzbeauftragten des Bundes und der Länder erarbeitet. Seit April 2018 liegt die überarbeitete Version 1.1 (Erprobungsfassung) vor. Die ersten SDM-Bausteine wurden mittlerweile veröffentlicht.

Im April 2018 verabschiedete die 95. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) einstimmig das SDM: „Das Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 1.1 Erprobungsfassung“.
Der Arbeitskreis „technische und organisatorische Datenschutzfragen“ der DSK erhielt zeitgleich den Auftrag, das SDM laufend weiter zu entwickeln und insbesondere die Bausteine des Maßnahmenkatalogs gemäß Beschluss der 92. DSK zu veröffentlichen.

Mit dem SDM wird eine Methode bereitgestellt, mit der Verantwortliche und Aufsichtsbehörden bei der Entwicklung, Datenschutzberatung und bei der Prüfung von Datenverarbeitungen beurteilen können, ob personenbezogene Daten datenschutzkonform verarbeitet werden. Ziel des SDM ist es, zudem bei der Umsetzung der DS-GVO gemeinsame Standards zur Beratungs- und Prüfungskonzeption vorzugeben, sodass ein abgestimmtes, transparentes und nachvollziehbares System der datenschutzrechtlichen Bewertung erreicht wird.
Ein Teil der Bausteine für den SDM-Maßnahmenkatalog sind nun veröffentlicht. Dabei handelt es sich um die Bausteine „Aufbewahrung“, „Planung und Spezifikation“, „Dokumentation“, „Protokollierung“, „Trennung“, „Löschen und Vernichten“ und „Datenschutzmanagement“.
Sie dienen als Handlungsempfehlung und Diskussionsgrundlage zur Weiterentwicklung, um die Gewährleistungsziele des SDM (Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz und Intervenierbarkeit) sicherzustellen. Eine Zuordnung der Artikel und der Erwägungsgründe der DS-GVO zu den Gewährleistungszielen wird in Kapitel 6.2 des SDM dargestellt. So ergibt sich beispielsweise die Intervenierbarkeit der Betroffenen explizit aus den Vorschriften zur Berichtigung, Löschung, Einschränkung der Verarbeitung und zum Widerspruch (Art. 16, 17, 18 und 21 DS-GVO) sowie das Recht auf Datenübertragbarkeit (Art. 20 DS-GVO).
Weiterhin ist das SDM auch für die Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO geeignet. Die Datenschutzgruppe nach Art. 29 der Richtlinie 95/46/EG hat deshalb in ihrem Working Paper 248 „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679, wahrscheinlich ein hohes Risiko mit sich bringt“ ausdrücklich das SDM als Mittel zur Durchführung einer Datenschutz-Folgenabschätzung mit benannt (siehe https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236).

Das SDM kann aber auch dazu beitragen, die vom IT-Planungsrat verabschiedete Nationale E-Government Strategie (NESG) datenschutzkonform umzusetzen. So hat der IT-Planungsrat in seiner 26. Sitzung im Juni 2018 die Version 1.1 (Erprobungsfassung) des Standard-Datenschutzmodells zustimmend zur Kenntnis genommen. Weiterhin wurden die Mitglieder des IT-Planungsrates gebeten, ihre Erfahrungen bei der Erprobung des SDM den Datenschutzaufsichtsbehörden des Bundes und der Länder mitzuteilen und somit zur Weiterentwicklung der Methode beizutragen.

Die aktuelle Version des Standarddatenschutzmodells in der Version 1.1 ist unter https://www.tlfdi.de/tlfdi/gesetze/orientierungshilfen/ abrufbar.

5.27 Die Befugnisse der Aufsichtsbehörde: Sanktionsverfahren bei Verstößen gegen den Datenschutz

Zur Einhaltung der Bestimmungen der Datenschutz-Grundverordnung und des Bundesdatenschutzgesetzes sind dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit als Aufsichtsbehörde zahlreiche Befugnisse und Sanktionsmöglichkeiten gegeben. Dabei ist zwischen Untersuchungs-, Abhilfe- und Sanktionsbefugnissen zu unterscheiden. Jede Maßnahme muss geeignet, erforderlich und angemessen sein.

Mit der Novellierung des Datenschutzrechts und der Einführung der EU-weiten Datenschutz-Grundverordnung (DS-GVO) wurden den Aufsichtsbehörden zahlreiche Befugnisse und Sanktionsmöglichkeiten an die Hand gegeben, um die Einhaltung der Datenschutz-Grundverordnung und des Bundesdatenschutzgesetzes (BDSG) zu gewährleisten. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) entscheidet im Einzelfall, ob und welche der Maßnahmen vorgenommen werden. Dabei ist zunächst zwischen den Abhilfebefugnissen der Aufsichtsbehörde und den Sanktionsbefugnissen zu unterscheiden. Unabhängig davon muss jede Maßnahme geeignet, erforderlich und angemessen sein.

I. Untersuchungsbefugnisse

Insgesamt sind in Art. 58 Abs. 1 DS-GVO sechs verschiedene Untersuchungsbefugnisse der Aufsichtsbehörden geregelt. Diese können gegenüber dem Verantwortlichen oder dem Auftragsverarbeiter geltend gemacht werden. Unabhängig davon, ob es sich bei dem Verantwortlichen um eine Behörde oder ein Unternehmen handelt. Die Besonderheiten des Thüringer Datenschutzgesetzes (ThürDSG) im Zusammenhang mit festgestellten Verstößen bei Behörden sind unter II. dargestellt. Nach Art. 4 Nr. 7 DS-GVO ist jede natürlich oder juristische Person, Behörde, Einrichtung oder andere Stelle Verantwortlicher, soweit sie über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden.

Der TLfDI hat das Recht, den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, alle Informationen bereitzustellen (Buchstabe a), die für die Erfüllung der Aufgaben einer Aufsichtsbehörde erforderlich sind. Diese Verpflichtung bezieht sich auf alle (Er-)Kenntnisse, die den jeweiligen Beteiligten zur Verfügung stehen, und soll verhindern, dass nur einzelne Auskünfte gegeben werden. Die Anweisung auf Bereitstellung von Informationen stellt einen Verwaltungsakt dar. Korrespondierend mit Art. 58 Abs. 1 Buchstabe a) DS-GVO verpflichtet Art. 31 DS-GVO den Verantwortlichen, den Auftragsverarbeiter bzw. deren Vertreter bei der Erfüllung ihrer Aufgaben mit der Aufsichtsbehörde auf Anfrage zusammenzuarbeiten. Allerdings kann sich der Verantwortliche oder Auftragsverarbeiter aufgrund der Rechtsstaatlichkeitsklausel in Art. 58 Abs. 4 auf ein Auskunftsverweigerungsrecht berufen, soweit er sich durch die Bereitstellung der Informationen selbst belasten würde (verlgeiche Boehm in Kühling/Buchner, DS-GVO-Kommentar, Art. 58, Rdnr. 14).

Datenschutzüberprüfungen (Buchstabe b) hinsichtlich des Datenschutz- und Datensicherheitsniveaus der Datenverarbeiter gehören zum Standard der Aufsichtsbehörden. Dabei werden die technisch-organisatorischen Maßnahmen und das Sicherheitskonzept überprüft. Ebenfalls möglich ist z. B. auch die Prüfung der datenschutzkonformen Ausgestaltung einer Videoüberwachungsanlage.

Nach Art. 42 DS-GVO kann die Zertifizierungsstelle oder die zuständige Aufsichtsbehörde für eine Höchstdauer von drei Jahren Zertifizierungen erteilen. Eine weitere Aufgabe für die Aufsichtsbehörden ist daher die Überprüfung von Zertifizierungen (Buchstabe c). Diese können unter denselben Bedingungen verlängert werden, sofern die

einschlägigen Voraussetzungen erfüllt werden. Wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden, wird sie von der Zertifizierungsstelle oder dem TLfDI als Aufsichtsbehörde widerrufen (Art. 42 Abs. 7 DS-GVO).
Weiterhin hat der TLfDI die Möglichkeit auf einen vermeintlichen Verstoß gegen die DS-GVO hinzuweisen (Buchstabe d). Diese Befugnis dient der Prävention und soll dem Verarbeiter die Möglichkeit geben, sein Verhalten zu ändern. Geschieht dies nicht, können Verwarnungen oder Anweisungen folgen.
Buchstabe e) regelt den Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung der Aufgaben des TLfDI notwendig sind. Art. 31 DS-GVO korrespondiert mit dieser Vorschrift und verpflichtet den Verantwortlichen, den Auftragsverarbeiter bzw. deren Vertreter, mit der Aufsichtsbehörde zusammenzuarbeiten und die Behörde bei der Erfüllung ihrer Aufgaben zu unterstützen. Das Einholen von Informationen stellt im Rahmen der Untersuchungsbefugnisse eines der wichtigsten Mittel des TLfDI als Aufsichtsbehörde dar (vergleiche Boehm a. a. O., Art. 58, Rdnr. 18).
Zur aufsichtsbehördlichen Tätigkeit gehört auch der Zugang zu den Geschäftsräumen (Buchstabe f), einschließlich der Datenverarbeitungsanlagen und -geräte. Dementsprechend sind anlasslose Überprüfungen grundsätzlich möglich und für eine wirksame Anwendung und Durchsetzung der DS-GVO sogar geboten.
Das Auskunftsersuchen ist eine weitere Untersuchungsbefugnis des TLfDI, die es der Aufsichtsbehörde ermöglicht, an Verantwortliche und das entsprechende Führungspersonal heranzutreten. Nach Art. 40 Abs. 4 BDSG haben diese Stellen und Personen auf Verlangen die erforderlichen Auskünfte zu erteilen, soweit diese Auskünfte für die Aufgabenerfüllung des TLfDI notwendig sind. Dabei kann sich der Auskunftspflichtige auf ein Zeugnisverweigerungsrecht aus § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung berufen. Der Auskunftspflichtige wird bei jedem Auskunftsersuchen darauf hingewiesen. Bei Beschwerden wendet sich der TLfDI regelmäßig an den Verantwortlichen, um den vorgetragenen Sachverhalt aufzuklären.

II. Abhilfebefugnisse

In Art. 58 Abs. 2 DS-GVO sind die insgesamt zehn Abhilfebefugnisse geregelt, die dem TLfDI als Aufsichtsbehörde zustehen. Diese Maßnahmen sollen zur (Wieder-)Herstellung datenschutzkonformer Zustände bei den Verantwortlichen beitragen. Diese Abhilfebefugnisse

können bei Unternehmen und Behörden angewendet werden. Kommt der TLfDI zu dem Ergebnis, dass Verstöße gegen die Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung personenbezogener Daten einer Behörde vorliegen, teilt er dies nach § 7 Abs. 1 Satz 2 ThürDSG der verantwortlichen Behörde vor Ausübung der nachfolgend genannten Befugnisse mit und fordert diese in einer angemessenen Frist zur Stellungnahme auf. Wenn der TLfDI die zur Verfügung stehenden Abhilfebefugnisse ergreift, müssen die rechtsverbindlichen Maßnahmen nach Erwägungsgrund 129 formale Voraussetzungen erfüllen. Jede Person wird vor dem Erlass einer Maßnahme mit nachteiligen Auswirkungen gemäß § 28 Thüringer Verwaltungsverfahrensgesetz grundsätzlich angehört. Überflüssige Kosten und übermäßige Unannehmlichkeiten für die Betroffen werden vermieden. Die Maßnahmen (Verwaltungsakte) des TLfDI werden schriftlich erlassen und darüber hinaus klar und eindeutig formuliert. Darin muss das Datum, an dem die Maßnahme erlassen wurde angegeben werden und das Schreiben muss vom Leiter oder einem von ihm bevollmächtigten Mitglied der Aufsichtsbehörde unterschrieben sein. Die Entscheidung des TLfDI enthält zudem eine Begründung für die getroffenen Maßnahmen sowie einen Hinweis auf das Recht eines wirksamen Rechtsbehelfs, denn ein rechtsverbindlicher Beschluss des TLfDI als zuständige Aufsichtsbehörde, ist gerichtlich überprüfbar.
Die folgenden Abhilfebefugnisse können nebeneinander angewendet werden und sind nach Schweregrad gestaffelt. Sie sollen den Aufsichtsbehörden, je nach Schwere und Dauer des Verstoßes, unterschiedliche Reaktionsmöglichkeiten zur Verfügung stellen.
Mit einer Warnung bei voraussehbaren Verstößen (Buchstabe a) wird der Verantwortliche oder ein Auftragsverarbeiter gewarnt, wenn beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen die DS-GVO verstoßen. Diese Befugnis hat eher beratenden Charakter. Sollte allerdings der Adressat einer solchen Warnung trotz des dringenden Hinweises seine Verarbeitungsvorgänge unverändert durchführen und somit ein Verstoß gegen die DS-GVO festgestellt werden, ist dies möglicherweise erschwerend bei einer Ahndung zu berücksichtigen.
Dagegen wird eine Verwarnung bei Verstößen (Buchstabe b) gegen die DS-GVO ausgesprochen. Sie kann auch als Ermahnung verstanden werden. Denkbar ist, dass eine Verwarnung in den Fällen ausgesprochen wird, in denen es sich um unerhebliche oder inzwischen beseitigte Mängel handelt oder die Beseitigung der Mängel sichergestellt

ist. Diese Maßnahme stellt eine Vorstufe zu den nachfolgenden Abhilfebefugnissen dar.
Mit Anweisungen, Anträgen von Betroffenen zu entsprechen (Buchstabe c), können die Betroffenenrechte direkt durchgesetzt werden. Der TLfDI weist die Verantwortlichen oder Auftragsverarbeiter an, den Anträgen der betroffenen Person auf Ausübung ihrer Rechte zu entsprechen. Das kann zum Beispiel der Auskunftsanspruch über gespeicherte Daten (Art. 15), der Löschanspruch (Art. 17) oder das Widerspruchsrecht (Art. 21) sein.
Der TLfDI kann Anweisungen, wie bestimmte Verarbeitungsvorgänge auszuführen sind (Buchstabe d), treffen. Damit sollen Verarbeitungsvorgänge auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DS-GVO gebracht werden.
Um die Rechte der Betroffenen bei der Verletzung des Schutzes ihrer personenbezogenen Daten gemäß Art. 34 DS-GVO zu gewährleisten, können Anweisungen gegenüber Verantwortlichen getroffen werden, die betroffene Person zu benachrichtigen (Buchstabe e), wenn eine Verletzung ein hohes Risiko für die Rechte und Freiheiten des Betroffenen zur Folge hat. Die Benachrichtigung ist nachzuholen, sofern sie (fälschlicherweise) unterblieben ist.
Ein Verstoß gegen Anweisungen nach Buchstabe c) bis Buchstabe e) kann gemäß Art. 83 Abs. 6 DS-GVO mit der Festsetzung eines Bußgeldes geahndet werden.
Eine noch weitreichendere Maßnahme ist die Verhängung einer vorübergehenden oder endgültigen Beschränkung der Verarbeitung, einschließlich eines Verbots (Buchstabe f), unabhängig davon, ob die Datenverarbeitung bei dem Verantwortlichen oder dem Auftragsverarbeiter vorgenommen wird. Diese Maßnahme kann als unmittelbarer Eingriff in die Datenverarbeitung angesehen werden.
Buchstabe g) ermöglicht eine Anordnung der Berichtigung oder Löschung von personenbezogenen Daten bzw. die Anordnung einer Einschränkung der Verarbeitung einschließlich entsprechenden Benachrichtigungen von Datenempfängern. Da sich alle in den Art. 16 bis 19 DS-GVO genannten Rechte nur gegen den Verantwortlichen richten, ist dieser auch gemäß Art. 58 Abs. 2 Buchstabe g) der Adressat der Maßnahme.
Weiterhin ist der TLfDI befugt, Zertifizierungen zu widerrufen oder die Zertifizierungsstelle anzuweisen, eine gemäß Art. 42 und 43 DS-GVO erteilte Zertifizierung zu widerrufen (Buchstabe h). Kommt die

Zertifizierungsstelle der Anweisung nicht nach, so könnte gegen sie ein Bußgeld ausgesprochen werden, Art. 83 Abs. 6 DS-GVO.
Geldbußen (Buchstabe i) gemäß Art. 83 DS-GVO können zusätzlich oder anstelle der vorgenannten Maßnahmen verhängt werden. Auch hier wird im Einzelfall entschieden.
Der TLfDI kann als Aufsichtsbehörde die Aussetzung der Datenübermittlung in Drittländer (Buchstabe j) oder an internationale Organisationen anordnen. Diese Befugnis wurde vom Europäischen Gerichtshof (EuGH) bestätigt (EuGH Urteil vom 6. Oktober 2015 – C-362/14) und wird nach den Bestimmungen des Thüringer Verwaltungszustellungs- und Vollstreckungsgesetz (ThürVwZVG) durchgesetzt.

Alle Anordnungen gegenüber Unternehmen werden nach den Regelungen des ThürVwZVG durchgesetzt und vollstreckt. Dies kann die Festsetzung eines Zwangsgelds, die Ersatzvornahme oder unmittelbarer Zwang sein.

III. Sanktionsbefugnisse

Das Verhängen von Geldbußen ist in Art. 83 DS-GVO geregelt. Dabei stellt der TLfDI sicher, dass die Geldbuße in jedem Einzelfall wirksam, verhältnismäßig, aber auch abschreckend ist. Wirksam und abschreckend ist eine Sanktion, wenn sie einerseits generalpräventiv geeignet ist, allgemeine Verstöße abzuwenden und andererseits aber auch spezialpräventiv geeignet ist, einen Täter von weiteren Verstößen abzuhalten (Bergt in Kühling/Buchner, a. a. O, Art. 83, Rdnr. 50). Bei der Entscheidung über das Verhängen einer Geldbuße und über den festzusetzenden Betrag ist der in Art. 83 Abs. 2 DS-GVO enthaltene Kriterienkatalog zu berücksichtigen. Die Geldbuße richtet sich unter anderem nach Art, Schwere und Dauer des Verstoßes. Insbesondere wird die Zahl der von der Verarbeitung betroffenen Personen und das Ausmaß des von ihnen erlittenen Schadens bewertet. Ob die Tat vorsätzlich oder fahrlässig begangen wurde, wird ebenfalls berücksichtigt. Lindernd auf den Betrag der Geldbuße wirken sich jegliche vom Verantwortlichen oder Auftragsverarbeiter getroffenen Maßnahmen aus, die zur Milderung des entstandenen Schadens für die betroffenen Personen beitragen. Zudem muss auch der Grad der Verantwortung des Verantwortlichen unter Berücksichtigung der getroffenen technischen und organisatorischen Maßnahmen berücksichtigt werden, wie z. B. der Umfang der Zusammenarbeit mit der Aufsichtsbehörde. Erschwerend auf die Festsetzung einer Geldbuße wirken sich

einschlägige frühere Verstöße des Verantwortlichen oder Auftragsverarbeiters aus. Die Höhe des Bußgeldes bemisst sich dabei auch nach der Art und Weise, wie dem TLfDI der Verstoß bekannt wurde und inwieweit frühere Anordnungen des TLfDI in selber Sache umgesetzt wurden. Zugleich müssen jegliche andere erschwerenden Umstände im Einzelfall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste, in die Erwägungen zur Festsetzung eines Bußgeldes einbezogen werden.
Der Bußgeldrahmen für einzelne Verstöße kann nach Art. 83 Abs. 4 DS-GVO bis zu 10 Millionen Euro oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs betragen, je nachdem, welcher der Beträge höher ist. Diese Regelung greift bei Verstößen gegen Bestimmungen nach:

- Buchstabe a)

Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß der Art. 8, 11, 25 bis 39, 42 und 43 DS-GVO

- Buchstabe b)

die Pflichten der Zertifizierungsstelle gemäß der Art. 42 und 43 DS-GVO

- Buchstabe c)

die Pflichten der Überwachungsstelle gemäß Art. 41 Abs. 4 DS-GVO.

Der Bußgeldrahmen für einzelne Verstöße kann nach Art. 83 Abs. 5 DS-GVO bis zu 20 Millionen Euro oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs betragen, je nachdem, welcher der Beträge höher ist. Das ist der Fall bei Verstößen gegen eine der folgenden Bestimmungen:

- Buchstabe a)

die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung gemäß der Art. 5, 6, 7 und 9 DS-GVO

- Buchstabe b)

die Rechte der betroffenen Personen gemäß der Art. 12 bis 22 DS-GVO

- Buchstabe c)

die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß der Art. 44 bis 49 DS-GVO

- Buchstabe e)

die Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Art. 58 Abs. 2 DS-GVO oder die Nichtgewährung des Zugangs unter Verstoß gegen Art. 58 Abs. 1 DS-GVO

Nach den Sanktionsvorschriften der DS-GVO ist nahezu jede Verletzung der Datenschutzbestimmungen bußgeldbewehrt. Der TLfDI kann Bußgelder zusätzlich oder anstelle der vorgenannten Abhilfemaßnahmen verhängen (Art. 58 Abs. 2 Buchstabe j) DS-GVO). Soweit der Verantwortliche mehrmals gegen dieselbe Regelung verstößt, kann für jeden Verstoß ein Bußgeld festgesetzt werden. Je nach Zeitabfolge der Verstöße werden diese in einem Bußgeldbescheid geahndet. Soweit ein Datenschutzverstoß nach Zahlung eines Bußgeldes nicht abgestellt worden ist, kann wegen desselben Verstoßes erneut ein Bußgeldbescheid erlassen werden.

IV. Bußgeldverfahren nach BDSG

Weitere Bußgelder können nach Art. 83 Abs. 5 Buchstabe d) DS-GVO verhängt werden, sofern die Mitgliedsstaaten Regelungen im Rahmen der Art. 85 bis 91 DS-GVO getroffen haben und diese Pflichten verletzt werden. Hierzu zählt zum Beispiel § 26 BDSG. Er regelt die Datenverarbeitung im Rahmen von Beschäftigungsverhältnissen.

Weitere Tatbestände für Ordnungswidrigkeiten finden sich in § 43 BDSG. Verstöße gegen § 30 BDSG, der die Datenverarbeitung bei Verbraucherkrediten regelt, können mit einem Bußgeldrahmen bis zu 50.000 Euro sanktioniert werden. Nach § 41 Abs. 1 BDSG ist für die Bußgeldregelung des § 43 BDSG das gesamte Ordnungswidrigkeitengesetz (OWiG) anwendbar.

V. Sanktionsbefugnisse gegenüber Behörden

Behörden sind nach Art. 7 Nr. 7 DS-GVO Verantwortliche, da sie über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Daher unterliegen Behörden ebenfalls den unter Punkt I. aufgeführten Untersuchungsbefugnissen des TLfDI als Aufsichtsbehörde.

Darüber hinaus kann der TLfDI gegen Behörden auch die unter Punkt II. genannten Abhilfebefugnisse wahrnehmen. Kommt der TLfDI allerdings zu dem Ergebnis, dass Verstöße gegen die Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung personenbezogener Daten einer Behörde vorliegen, teilt er

dies nach § 7 Abs. 1 Satz 2 Thüringer Datenschutzgesetz (ThürDSG) dem Verantwortlichen vor Ausübung der unter Punkt II. genannten Befugnisse mit und fordert diesen innerhalb einer angemessenen Frist zur Stellungnahme auf.
Nach dem ThürDSG handelt ordnungswidrig, wer entgegen den Bestimmungen der DS-GVO, des ThürDSG oder anderer Rechtsvorschriften zum Schutz personenbezogener Daten solche Daten erhebt, speichert, verändert, übermittelt, nutzt, sie mithilfe von automatisierten Verfahren abrufbereit hält oder sich beziehungsweise Dritten aus Dateien mit personenbezogenen Daten verschafft oder sonst verarbeitet (§ 61 ThürDSG). Dies kann mit einer Geldbuße bis zu 50.000 Euro geahndet werden. Gegen öffentliche Stellen nach § 2 Abs. 1 und 2 ThürDSG werden keine Geldbußen verhängt, es sei denn, es handelt sich um öffentliche Stellen, die am Wettbewerb im Sinne des § 26 ThürDSG teilnehmen. Nach § 61 Abs. 6 ThürDSG ist der TLfDI dabei Verwaltungsbehörde gemäß § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten (OWiG).
Nach § 9 Abs. 1 ThürDSG ist für Streitigkeiten zwischen öffentlichen Stellen und dem TLfDI nach § 7 Abs. 6 ThürDSG der Verwaltungsrechtsweg eröffnet. Danach ist das Verfahren entsprechend der Verwaltungsgerichtsordnung zu führen. Örtlich zuständig ist das Verwaltungsgericht Weimar, da der TLfDI seinen Sitz in dessen Bezirk hat. Der TLfDI ist bei einem Klageverfahren beteiligungsfähig. Dabei ist ein Vorverfahren in § 20 Abs. 6 BDSG ausgeschlossen worden. In der Begründung zu § 9 Abs. 1 Satz 1 heißt es: „Der Rechtsschutz besteht gegen rechtsverbindliche Beschlüsse des Landesbeauftragten im Sinne von Art. 78 Abs. 1 der DS-GVO und § 7 Abs. 6 ThürDSG …].“ Damit wurde den öffentlichen Stellen (Behörden) ein Klagerecht eingeräumt. Gemäß § 9 Abs. 1 Satz 2 ThürDSG i. V. m § 20 BDSG ist andererseits auch ein Klagerecht des TLfDI installiert worden. In diesem Sinne führte Herr Abgeordneter Dittes in der 119. Sitzung des Thüringer Landtags am 24. Mai 2018 (Plenarprotokoll 6/119, S. 10202) aus: „Wir haben in der Beschlussempfehlung des Ausschusses klargestellt, dass auch der Datenschutzbeauftragte des Landes ein Klagerecht in Verwaltungsstreitsachen hat. Das Gesetz in der Entwurfsfassung der Landesregierung sah ja schon den Verwaltungsgerichtsweg vor. Uns war es aber auch wichtig, im Gesetz deutlich zu machen, dass der Verwaltungsgerichtsweg nicht nur durch betroffene Behörden und öffentliche Stellen gegangen werden kann, sondern auch durch den Datenschutzbeauftragten, wenn beispielsweise durch

Behörden Anordnungen des Datenschutzbeauftragten nicht Folge geleistet worden ist. Hierdurch wurde Art. 58 Abs. 5 DS-GVO vollumfänglich entsprochen. Dieser bestimmt, dass jeder Mitgliedstaat durch Rechtsvorschriften vorsieht, dass seine Aufsichtsbehörde befugt ist, Verstöße gegen diese Verordnung den Justizbehörden zur Kenntnis zu bringen und gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben oder sich sonst daran zu beteiligen, um die Bestimmungen dieser Verordnung durchzusetzen.

VI. Strafvorschriften nach BDSG

Der TLfDI hat als Aufsichtsbehörde nach § 42 Abs. 3 BDSG die Befugnis, Strafanträge zu stellen. In § 42 Abs. 1 und 2 BDSG sind Freiheitsstrafen von bis zu drei Jahren geregelt. Wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von betroffenen Personen unberechtigt an Dritte übermittelt oder auf andere Art und Weise zugänglich macht, muss mit einer Freiheitstrafe von bis zu drei Jahren oder mit einer empfindlichen Geldstrafe rechnen. Diese Strafen werden verhängt, soweit gewerbsmäßig gehandelt wird (Abs. 1). Wer personenbezogene Daten, die nicht allgemein zugänglich sind, unberechtigt verarbeitet, sie durch unrichtige Angaben erschleicht in der Absicht sich oder andere zu bereichern oder jemand anderen damit zu schädigen muss mit einer Freiheitstrafe von bis zu zwei Jahren oder mit einer Geldstrafe rechnen (Abs. 2).

5.28 Kitas und die DS-GVO – Kinderleichter Datenschutz?

Mit der neuen Datenschutz-Grundverordnung (DS-GVO) bleiben zwar grundsätzlich die bereits bestehenden Anforderungen des Datenschutzes erhalten, zusätzlich müssen einige wesentliche Neuregelungen von den Kindertagesstätten aber beachtet und umgesetzt werden.

Derzeit herrscht in Thüringer Kitas Verunsicherung bei der Umsetzung der DS-GVO. Der TLfDI weist in dieser Angelegenheit erneut darauf hin, dass sich die bisherigen datenschutzrechtlichen Regelungen mit dem Inkrafttreten der DS-GVO nicht völlig anders gestalten; jedoch sind einige Änderungen zu beachten. Für die Kitas bedeutet das in der Regel eine Anpassung der Einwilligungserklärungen an die neuen datenschutzrechtlichen Standards. Gemäß Art. 7 DS-GVO ist ausdrücklich auf das Recht, eine Einwilligung jederzeit widerrufen zu

können, hinzuweisen. Der Widerruf der Einwilligung muss dabei so einfach sein, wie die Erteilung der Einwilligung. Die bisherig grundsätzlich zu verwendende Schriftform der Einwilligung ist zwar nicht mehr vorgeschrieben, die Kita muss aber nachweisen können, dass die Sorgeberechtigten in die Verarbeitung personenbezogener Daten eingewilligt haben. Eine schriftliche Einwilligung ist deshalb weiterhin dringend zu empfehlen. Die häufigsten Einwilligungen, die hierbei eingeholt werden, betreffen das Fotografieren der Kita-Kinder. Haben die Sorgeberechtigten nicht zuvor in das Erstellen von Fotoaufnahmen der Kinder eingewilligt, dürfen die betroffen Kinder nicht fotografiert werden. Bereits vor Geltung der DS-GVO rechtswirksam erteilte Einwilligungen behalten ihre Gültigkeit, sofern diese der Art nach den Bedingungen der DS-GVO entsprechen (Erwägungsgrund 171 der DS-GVO), also die betroffenen Personen auch über ihr Widerrufsrecht ausdrücklich belehrt wurden.

Ein weiteres großes Thema ist die Frage der Zulässigkeit einer dienstlichen Nutzung des Messenger-Dienstes „WhatsApp“ in der Kita. Häufig wird der Dienst sowohl für die Kommunikation als auch zum Austausch von Fotografien und Videoaufnahmen der betreuten Kinder genutzt. Das Kita-Personal und die Sorgeberechtigten kommunizieren und tauschen sich dabei in einer zu diesem Zweck erstellten WhatsApp-Gruppe aus. In diesem Zusammenhang verweist der TLfDI darauf, dass die Verarbeitung personenbezogener Daten mit WhatsApp als Messenger-Dienst keine Datensicherheit gewährleisten kann. Die Nutzung des Messenger-Dienstes ist nicht zur Aufgabenerfüllung der Kita erforderlich und sollte daher eingestellt bzw. unterlassen werden. Allerdings war die dienstliche Verwendung einschlägiger Messenger-Dienste bereits nach der alten Rechtslage, und damit vor der Anwendung der DS-GVO, unzulässig. Zwar werden alle mit WhatsApp versendeten Inhalte mit einer Ende-zu-Ende Verschlüsselung übertragen, der Dienst selbst liest aber regelmäßig die auf dem Smartphone abgelegten Kontaktdaten, also Daten von Dritten, die dem Nutzer des Messenger-Dienstes in der Regel keine Einwilligung erteilt haben, sowie weitere Metadaten, z. B. Geräte- und Verbindungsdaten, Standortdaten, Statusinformationen usw., aus. Ohne eine solche Einwilligung begeht der Dienste-Nutzer gegenüber seinen übrigen Kontaktpersonen eine deliktische Handlung, die zu einer kostenpflichtigen Abmahnung führen kann (vergleiche Amtsgericht Bad Hersfeld, Az.: F120/17 EASO). Damit liegt ein Verstoß gegen Art. 5

Abs. 1 Buchstabe a) DS-GVO („Gebot der Verarbeitung auf rechtmäßige Weise“) vor.

In genau diesem Punkt wurde der Datenschutz mit der DS-GVO dahingehend verschärft, dass Verantwortliche, in diesem Fall Kitas, für die Einhaltung der in Art. 5 Abs. 1 DS-GVO beschriebenen Grundsätze zur Verarbeitung personenbezogener Daten verantwortlich sind und zudem nach Art. 5 Abs. 2 DS-GVO im Sinne der Rechenschaftspflicht die Einhaltung dieser Grundsätze nachweisen müssen. Danach müssen alle personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Weitere wichtige Grundsätze im Umgang mit personenbezogenen Daten sind die Zweckbindung, die Datenminimierung, die Gewähr für die Richtigkeit, die Begrenzung der Speicherdauer auf die zur Aufgabenerfüllung der Stelle erforderliche Zeitspanne, sowie die Gewährleistung der Integrität und die Vertraulichkeit der Daten. Es handelt sich hierbei um ein sehr gewichtiges und umfängliches Gebot der DS-GVO, denn Kitas müssen die darin beschriebenen Pflichten nicht nur erfüllen, sondern gleichzeitig auch die Einhaltung dieser Pflichten nachweisen.

Zu empfehlen ist, die Form des Nachweises in Form einer schriftlichen Dokumentation zu erbringen. Hierzu gehört nach Art. 30 DS-GVO die Führung eines Verzeichnisses aller Verarbeitungstätigkeiten (Mustervorlagen sind unter https://www.tlfdi.de/mam/tlfdi/themen/muster_verarbeitungsverzeichnis_auftragsverarbeiter.pdf auf der Seite des TLfDI abrufbar) sowie die Darlegung der getroffenen technischen und organisatorischen Datenschutzvorkehrungen gemäß Art. 24 DS-GVO.

Weiterhin sind nach Art. 13 und 14 DS-GVO umfangreiche Informationspflichten bei der Erhebung personenbezogener Daten vorgesehen, eine faire und transparente Verarbeitung personenbezogener Daten zu gewährleisten. Nach Art. 12 Abs. 5 DS-GVO sind Informationen gemäß der Art. 13 und 14 DS-GVO grundsätzlich unentgeltlich sowie in präziser, verständlicher und leicht zugänglicher Form zur Verfügung zu stellen. Die anfragende Kita wurde auf zwei vom TLfDI herausgegebene Musterbögen zu Art. 13 und 14 DS-GVO unter: https://www.tlfdi.de/tlfdi/datenschutz/kommunales hingewiesen.

Mit der Anwendung der DS-GVO wurde zudem das bisherige Verfahrensverzeichnis durch das Verzeichnis über Verarbeitungstätigkeiten nach Art. 30 DS-GVO ersetzt. Hierbei können die Kitas prüfen, ob das alte Verzeichnis weitergeführt werden kann. In diesem Fall muss in einer Adaptionsverfügung für Verfahrensverzeichnisse nachgewiesen werden, dass das bisherige Verfahrensverzeichnis dem Niveau des Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO entspricht. Ansonsten muss zur Anpassung an die neue Rechtsgrundlage ein Verzeichnis von Verarbeitungstätigkeiten erstellt werden. Auch diese Musterblätter können unter dem o. g. Link des TLfDI abgerufen werden.

Hat die Kita eine Homepage, sind neben dem Impressum auch die bisherigen Datenschutzerklärungen zu prüfen und eventuell zu ergänzen. Wie dies in der Praxis auszusehen hat, kann aus der online Datenschutzerklärung des TLfDI unter https://www.tlfdi.de/mam/tlfdi/datenschutzerklarung_.pdf entnommen werden.

Im Übrigen können die zahlreichen Hinweise und Formulierungshilfen des TLfDI unter https://www.tlfdi.de/tlfdi/europa/europaeische-dsgvo als Hilfestellung dienen.

5.29 Demokratie und Datenschutz: Umgang mit Wahlwerbung im öffentlichen und nicht-öffentlichen Bereich

Für Formen politischer Beteiligung in der Demokratie wie Wahlen, Abstimmungen, Bürgerbegehren oder Bürgerentscheide dürfen Meldebehörden nach § 50 Abs. 1 des Bundesmeldegesetzes (BMG) personenbezogene Daten von potentiellen Wählern an Parteien und Wählergruppen übermitteln. Wer damit nicht einverstanden ist, kann eine Übermittlungssperre nach § 50 Abs. 5 des BMG bei der zuständigen Meldebehörde einrichten lassen.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichten im Berichtszeitraum Anfragen zur Zulässigkeit von Melderegisterauskünften zum Zwecke der Wahlwerbung. Die Betroffenen wurden im Vorfeld einer anstehenden demokratischen Wahl von Kandidaten angeschrieben, um für ihr Programm und um die Stimme des Betroffenen zu werben.
Eine Verarbeitung personenbezogener Daten ist nach Art. 6 Abs. 1 Satz 1 Buchstabe c) der Datenschutz-Grundverordnung (DS-GVO) zulässig, soweit es für die Verarbeitung eine Rechtsgrundlage gibt. Die Anwendung des Art. 6 Abs. 1 Buchstabe e) DS-GVO wäre hier ebenfalls denkbar. Für diese Regelungen sieht Art. 6 Abs. 3 DS-GVO eine Begriffsbestimmung mit Öffnungsklausel vor. Hier spielt die Zweckbindung eine zentrale Rolle. Die Rechtsgrundlage für die Verarbeitungen gemäß Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO wird festgelegt durch das Recht des Mitgliedsstaats, dem der Verantwortliche, im vorliegende Fall also die Meldebehörde, unterliegt. Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt sein. Gemäß § 50 des Bundesmeldegesetzes (BMG) ist es möglich, Melderegisterauskünfte in besonderen Fällen zu erhalten. Nach § 50 Abs. 1 des BMG darf eine Meldebehörde Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen, im Zusammenhang mit Wahlen und Abstimmungen auf staatlicher und kommunaler Ebene, bis zu sechs Monaten vor der jeweiligen Wahl oder Abstimmung Auskünfte aus dem Melderegister über Daten von Gruppen von Wahlberechtigten erteilen, soweit für deren Zusammensetzung das Lebensalter bestimmend ist. Zu den übermittelten Daten gehören Name, Vorname sowie gegebenenfalls der akademische Titel und eine gültige Adresse. Die Geburtsdaten der Wahlberechtigten dürfen dabei nicht mitgeteilt werden. Die Person oder Stelle, der die Daten übermittelt

werden, darf diese nur für die Werbung bei einer Wahl oder Abstimmung verwenden und hat sie spätestens einen Monat nach der Wahl oder Abstimmung zu löschen oder zu vernichten.
Betroffene haben nach § 50 Abs. 5 des BMG jederzeit das Recht, dieser Datenweitergabe mit einem Sperrvermerk zu widersprechen bzw. eine Übermittlungssperre einzurichten. Hierzu müssen sich die Betroffenen an das zuständige Einwohnermeldeamt wenden. Dort können sich Betroffene zur Übermittlungssperre beraten lassen und erhalten in der Regel entsprechende Formulare für einen Sperrvermerk.
Mit Blick auf die oben erläuterten datenschutzrechtlichen Bestimmungen für Verantwortliche in Bezug auf Wahlwerbung im öffentlichen Bereich, wurde dem TLfDI im Berichtszeitraum ein ähnlicher Fall eines Verantwortlichen im nicht-öffentlichen Bereich zugetragen, bei dem ein Vorstandsmitglied eines Vereins personenbezogene Mitgliederdaten für die eigene Wahlwerbung zweckentfremdete (siehe Beitrag 5.32). Das Vorstandsmitglied schrieb die betroffenen Personen explizit als Vereinsmitglieder an. Die Kontaktdaten wurden der Vereinsdatenbank entnommen und erneut gespeichert, um die Mitglieder als potentielle Wähler anzuschreiben. Dabei wurde die Vereinsarbeit mit dem politischen Amt vermischt. Bei diesem Verhalten spricht man von einem Exzess (detailliert siehe Beitrag 5.33). Die Datenübermittlung vom Vereinsmitglied an die werbende Person ist unzulässig, auch wenn es sich hierbei um dieselbe Person handelt. Das Vorstandsmitglied hat die personenbezogenen Mitgliederdaten an die werbende Person außerhalb des Vereins übermittelt. Hierfür sieht die Datenschutz-Grundverordnung keine Erlaubnistatbestände vor. Die Übermittlung an die werbende Person war weder für die Erfüllung des Vereinszwecks nach Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO erforderlich, noch lag dem Vorstandsmitglied nach Art. 6 Abs. 1 Buchstabe a) DS-GVO eine Einwilligung der Mitglieder vor. Dementsprechend können Vereinsmitglieder auch erwarten, dass ihre personenbezogenen Daten nicht zweckentfremdet werden; dies geht in diesem Fall auch insbesondere aus der Vereinssatzung hervor. Das beschriebene Vorgehen des Vereinsmitglieds verstößt insbesondere gegen den Grundsatz der Zweckbindung aus Art. 5 Abs. 1 Buchstabe b) DS-GVO. Demnach müssen personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Üblicherweise schließen Vereine mit ihren Mitgliedern

Mitgliedsvereinbarungen ab. Diese stellen die Grundlage für eine Datenverarbeitung nach Art. 6 Abs. 1 Buchstabe b) DS-GVO dar. In der Mitgliedsvereinbarung des hier geschilderten Falles wurde eine Datenweitergabe an Dritte zudem ausgeschlossen. Danach lag nicht nur ein Verstoß gegen Art. 5 Abs. 1 Buchstabe b) DS-GVO vor, sondern auch nach Art. 6 Abs. 1 Buchstabe b) DS-GVO. Der TLfDI sanktionierte diese rechtswidrige Zweckentfremdung personenbezogener Daten mit dem Festsetzen eines Bußgelds im vierstelligen Bereich; der Bußgeldbescheid des TLfDI wurde durch das Amtsgericht Erfurt bestätigt.

5.30 Geschäftsmodell Nutzerdaten: Wahlmanipulation und Wahlanalysen mithilfe sozialer Netzwerke?

Auch soziale Netzwerke haben ihr Geschäftsmodell auf die neuen europäischen Datenschutzregeln auszurichten und ihrer gesellschaftlichen Verantwortung nachzukommen. Es bedarf europäischer Initiativen, um monopolartige Strukturen im Bereich der sozialen Netzwerke zu begrenzen und, Transparenz von Algorithmen herzustellen.

Den Wunsch, Einfluss auf das Wahlverhalten von Bürgern bei Wahlen zu nehmen, gibt es wohl schon, seitdem es Wahlen gibt. In Deutschland ist deshalb in § 50 Abs. 1 Bundesmeldegesetz (BMG) geregelt, dass eine Meldebehörde den Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit Wahlen und Abstimmungen auf staatlicher und kommunaler Ebene, in den letzten sechs Monaten vor einer Wahl oder Abstimmung, Auskunft aus dem Melderegister über die in § 44 Abs. 1 Satz 1 bezeichneten Daten, wie Vor-, Familiennamen, Doktorgrad und die Anschrift von Wahlberechtigten erteilen darf. Dies aber nur, wenn der Bürger diesen Melderegisterauskünften nicht widersprochen hat. Der TLfDI weist die Bürger seit Jahren auf ihr Widerspruchsrecht hin, zuletzt am 6. Februar 2019.

(https://www.tlfdi.de/mam/tlfdi/presse/echo/190206_pm_widerspruchsrecht_gegen_wahlwerbung.pdf)

Aber werden zukünftig überhaupt noch Daten aus den Melderegistern zur Wahlwerbung benötigt? Sind Parteien, die die digitale Welt durchforschen und digitale Profile für politische Zwecke erstellen lassen, im Vorteil?
Im April 2018 wies die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) in ihrer Entschließung "Facebook-Datenskandal – Neues Europäisches Datenschutzrecht bei Sozialen Netzwerken durchsetzen!" ausdrücklich nochmal auf das seit 25. Mai 2018 geltende einheitliche europäische Datenschutzrecht, die Datenschutz-Grundverordnung (DS-GVO), hin. Anlass war, dass im März 2018 der Öffentlichkeit bekannt wurde, dass über eine von November 2013 bis Mai 2015 mit Facebook verbundene App nach Angaben des Unternehmens Daten von weltweit 87 Millionen Nutzern, davon 2,7 Millionen Europäern und etwa 310.000 Deutschen, erhoben und an das Analyseunternehmen Cambridge Analytica weitergeben wurden. Die DSK geht in ihrer Entschließung davon aus, das die Daten dort offenbar auch zur Profilbildung für politische Zwecke verwendet wurden. Zudem dokumentieren die Vorgänge um Cambridge Analytica, dass Facebook über Jahre hinweg den Entwicklern von Apps, neben dem Zugriff auf die Daten von Facebook-Nutzern, auch massenhaften Zugriff auf Daten befreundeter Facebook-Nutzer erlaubte. Das geschah ohne eine Einwilligung der Betroffenen. Die DSK wies in ihrer Entschließung darauf hin: „Das Vorkommnis zeigt zudem die Risiken für Profilbildung bei der Nutzung sozialer Medien und anschließendes Mikrotargeting, einer systematischen Marketing Kommunikationsstrategie, das offenbar zur Manipulation demokratischer Willensbildungsprozesse eingesetzt wurde."
Die DSK forderte, dass soziale Netzwerke zukünftig ihr Geschäftsmodell auf die neuen europäischen Datenschutzregeln auszurichten haben und ihrer gesellschaftlichen Verantwortung nachkommen müssen.
Zudem wies sie auch darauf hin, dass die Vorstellung von Facebook zur Einführung der automatischen Gesichtserkennung in Europa erhebliche Zweifel aufkommen lässt, ob das Zustimmungsverfahren mit den gesetzlichen Vorgaben insbesondere zur Einwilligung vereinbar ist. Ferner gilt es, Art. 34 DS-GVO zu beachten, der die Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, regelt. Weiterhin fordert die DSK, dass es eu-

ropäischer Initiativen bedürfe, um monopolartige Strukturen im Bereich der sozialen Netzwerke zu begrenzen und Transparenz von Algorithmen herzustellen. Die gesamte Entschließung finden Sie unter: https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Entschliessungen_Datenschutzkonferenz/Inhalt/95_Konferenz/Facebook-Datenskandal-_-Neues-Europaeisches-Datenschutzrecht-bei-Sozialen-Netzwerken-durchsetzen_/FB-DatenskandalDE.pdf

5.31 Die Nachweispflicht der Verantwortlichen: Anfragen zum Verzeichnis der Verarbeitungstätigkeiten

Jeder Verantwortliche z. B. eines Unternehmens, eines Vereins oder im freiberuflichen Bereich, hat die Pflicht, nach Art. 30 Datenschutz-Grundverordnung (DS-GVO) ein Verzeichnis von Verarbeitungstätigkeiten zu führen. Ausnahmen sind nur unter engen Voraussetzungen möglich. Dieses Verzeichnis von Verarbeitungstätigkeiten dient der Aufsichtsbehörde als Nachweis dafür, dass datenschutzrechtliche Vorgaben der DS-GVO eingehalten und umgesetzt werden. Aufsichtsbehörden können anhand des Verarbeitungsverzeichnisses die Rechtmäßigkeit von Verarbeitungsvorgängen überprüfen.

Nach Art. 30 Datenschutz-Grundverordnung (DS-GVO) führt jeder Verantwortliche, der nicht nur gelegentlich Daten verarbeitet, schriftlich ein Verzeichnis aller Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen. Auftragsverarbeiter (siehe Beitrag 5.20) führen ein Verzeichnis zu allen Kategorien ihrer Verarbeitungstätigkeit, die sie im Auftrag eines Verantwortlichen durchführen. Nach Art. 4 Nr. 7 DS-GVO ist jede natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, Verantwortlicher (z. B. Unternehmen, Freiberufler, Vereine). Er ist Träger der in der DS-GVO verankerten Rechte und Pflichten.
Das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO spielt eine wesentliche Rolle, um datenschutzrechtliche Vorgaben

überhaupt einzuhalten. Nur wer die eigenen Verarbeitungsprozesse kennt, kann gezielt Maßnahmen ergreifen, um eine rechtmäßige Verarbeitung personenbezogener Daten sicherstellen zu können.
Im Zusammenhang mit Art. 30 sind weitere Vorschriften der DS-GVO zu beachten, die eine Dokumentation bzw. Information beim Verantwortlichen oder Auftragsverarbeiter, unabhängig von den Vorgaben dieser Regelung, vorsehen. Zum Beispiel Maßnahmen zur Datensicherheit nach Art. 24 Abs. 1 und Art. 32 DS-GVO oder Maßnahmen zur Erfüllung der Betroffenenrechte nach Art. 12 Abs. 1 DS-GVO. Das Verzeichnis von Verarbeitungstätigkeiten dient dem Datenschutzbeauftragten als Grundlage seiner Aufgabenerfüllung nach Art. 39 DS-GVO. Somit stellt das anzufertigende Verzeichnis eine zusammenfassende Auflistung von Daten dar, die der Verantwortliche aufgrund anderer Vorschriften der DS-GVO sowieso vorhalten muss. Dadurch kann der TLfDI (Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit) als Aufsichtsbehörde die Rechtmäßigkeit der vorgenommenen Verarbeitungsprozesse leichter überprüfen.

Der Inhalt der jeweiligen Verzeichnisse ist in Art. 30 Abs. 1 und 2 DS-GVO festgelegt. Der TLfDI hat auf seiner Homepage Hinweise zur Erstellung eines solchen Verzeichnisses und eine Formulierungshilfe veröffentlicht (https://www.tlfdi.de/tlfdi/europa/europaeischedsgvo/index.aspx). Art. 30 Abs. 1 Buchstabe g) und Art. 30 Abs. 2 Buchstabe d) DS-GVO geben vor, dass das Verzeichnis, wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO enthalten soll. Die Beschreibung der Maßnahmen sollte so konkret erfolgen, dass der TLfDI eine erste Überprüfung der Rechtmäßigkeit vornehmen kann. Für die Bestimmung der zu treffenden Maßnahmen wird auf das Standard-Datenschutzmodell verwiesen, insbesondere Kapitel sieben (https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V1.1.pdf)

und der entsprechende Maßnahmenkatalog im Anhang (https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/).

Unternehmen und Einrichtungen mit weniger als 250 Mitarbeitern müssen gemäß Art. 30 Abs. 5 DS-GVO kein Verzeichnis von Verarbeitungstätigkeiten führen, es sei denn, der Verantwortliche oder Auftragsverarbeiter führt Verarbeitungen personenbezogener Daten durch,

- die ein Risiko für die Rechte und Freiheiten der betroffenen Personen darstellen (z. B. Scoring, Überwachungsmaßnahmen) oder
- die nicht nur gelegentlich erfolgen oder
- die besondere Datenkategorien gemäß Art. 9 Abs. 1 der DS-GVO (z. B. Religionsdaten, Gesundheitsdaten) oder strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 der DS-GVO betreffen.

Bei regelmäßigen oder dauerhaften Standardverfahren, die zum typischen Geschäftsbetrieb gehören (Personalakten, Finanzbuchhaltung, Mitgliederlisten, Kundendatenbanken) findet keine gelegentliche Verarbeitungstätigkeit statt. Von der Verzeichnispflicht können sich Verantwortliche nur befreien, wenn sich ihre durchgeführten Datenverarbeitungen jenseits typischer Verarbeitungstätigkeiten bewegen und somit auch nur vereinzelt vorkommen. Demnach hat jeder Verantwortliche eine Verfahrensverzeichnispflicht, wenn Kunden- oder Beschäftigtendaten verarbeitet werden. Eine Ausnahme von der Pflicht, ein Verzeichnis zu führen, besteht außerdem nicht, wenn die Verarbeitungstätigkeit besondere Datenkategorien im Sinne des Art. 9 Abs. 1 DS-GVO erfasst. Die Sensibilität dieser Daten löst ein hohes Kontrollbedürfnis aus, das eine Befreiung von Art. 30 ausschließt (vergleiche Martini in Paal/Pauly DS-GVO, BDSG, 2. Auflage, Art. 30, Rdnr. 26 ff.).

Verstöße durch eine fehlende oder nicht vollständige Führung eines Verzeichnisses oder das Nichtvorlegen des Verzeichnisses nach Aufforderung des TLfDI als Aufsichtsbehörde können nach Art. 83 Abs. 4 Buchstabe a) DS-GVO mit einer Geldbuße sanktioniert werden.

Den TLfDI erreichten Anfragen, ob die Herausgabe des Verzeichnisses von Verarbeitungstätigkeiten von Dritten vom Verantwortlichen

gefordert werden kann. Nach Erwägungsgrund 82 soll die Pflicht zur Vorlage des Verzeichnisses über Verarbeitungstätigkeiten gegenüber den Aufsichtsbehörden ermöglichen, dass diese die betreffenden Verarbeitungsvorgänge anhand des Verzeichnisses kontrollieren können. Der Verantwortliche muss nach Art. 30 Abs. 4 DS-GVO das Verzeichnis dem TLfDI auf Verlangen vorlegen. Es ist nicht dafür gedacht, dass Privatpersonen oder Wettbewerber in dieses Verzeichnis Einblick nehmen.

5.32 Datenschutz in Vereinen: Pflichten, Rechte und allgemeine Ausführungen

Vereine unterliegen allen Regelungen der Datenschutz-Grundverordnung (DS-GVO), weil sie nach Art. 4 Nr. 7 DS-GVO als verantwortlich gelten. Zwei wichtige Eckpunkte dieser Verantwortung sind die transparente Aufstellung von Verarbeitungstätigkeiten und, beim Betreiben einer Website, das vertragliche Abwickeln einer datenschutzkonformen Auftragsverarbeitung mit dem jeweiligen Hoster. Zudem besteht gegenüber Mitgliedern und Dritten eine Informationspflicht nach Art. 13 und Art. 14 DS-GVO.

Bei der Datenverarbeitung in Vereinen fallen verschiedene Kategorien von Daten an, wie z. B. Mitgliederdaten, Adressdaten, Kontaktdaten, Grundstücksdaten mit Personenbezug, möglicherweise auch Daten zur Zahlung von Mitgliedsbeiträgen sowie Bankdaten. Die Verarbeitung dieser Daten ist nur rechtmäßig, wenn sie nach Art. 6 Abs. 1 der DS-GVO zulässig ist.
In der Regel kann diese Zulässigkeit aus Art. 6 Abs. 1 Buchstabe b) DS-GVO hergeleitet werden, da die Verarbeitung für die Erfüllung eines Vertrags erforderlich ist, z. B. bei einer Mitgliedsvereinbarung oder einem Pachtvertrag.
Die Datenverarbeitung in Vereinen kann nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO auch infolge einer Einwilligung der betroffenen Person rechtmäßig sein, wenn die Datenverarbeitung nicht wie oben beschrieben zur Erfüllung der Mitgliedsvereinbarung oder des Pachtvertrages erforderlich ist (Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO).

Nach Art. 6 Abs. 1 Satz 1 Buchstabe f) der DS-GVO kann die Verarbeitung personenbezogener Daten rechtmäßig sein, wenn sie zur Wahrung der berechtigten Interessen des Vereins erforderlich ist, die sich auch aus der Vereinssatzung ergeben können. Dies kann zum Beispiel bei der Veröffentlichung von Fotos zutreffen, die bei Veranstaltungen im Rahmen der Vereinsarbeit entstanden sind (siehe Beitrag 5.21). Bei einer Datenverarbeitung aus berechtigtem Interesse dürfen die Grundrechte und Grundfreiheiten der betroffenen Personen, die den Schutz personenbezogener Daten erfordern, nicht überwiegen. Diese Interessenabwägung muss vor der beabsichtigten Datenverarbeitung vorgenommen werden. Andernfalls besteht die Gefahr einer unbefugten Datenverarbeitung. Soweit sich der Verantwortliche auf eine Datenverarbeitung nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO beruft, muss er die betroffenen Personen über seine berechtigten Interessen informieren, die er mit der Verarbeitung verfolgt (Art. 13 Abs. 1 Buchstabe d), Art. 14 Abs. 2 Buchstabe b) DS-GVO). Darüber hinaus muss der Verantwortliche die Einhaltung des Grundsatzes der Rechtmäßigkeit der Datenverarbeitung nach Art. 5 Abs. 1 Buchstabe a) DS-GVO nachweisen können (vergleiche Schantz in Simitis, Hornung, Spiecker Datenschutzrecht (DS-GVO/BDSG), Art. 6, Rdnr. 87).
Verantwortlicher für die Datenverarbeitung ist die natürliche oder juristische Person oder Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten nach Art. 4 Nr. 7 DS-GVO entscheidet. Welche Verpflichtungen jeder Verein zu erfüllen hat, ist in einer Handreichung aufgeführt (https://www.tlfdi.de/tlfdi/europa/europaeischedsgvo/index.aspx).

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichten im Berichtszeitraum vermehrt Beschwerden darüber, dass ein Vereinsmitglied personenbezogene Daten für eigene Zwecke verwendet hat. Beispielsweise wurden die Mitgliederdaten genutzt, um Werbung in eigener Angelegenheit zu versenden. Das Vereinsmitglied übermittelte dabei die personenbezogenen Mitgliederdaten an eine Person außerhalb des Vereins, auch wenn es sich dabei um dieselbe Person handelt. Dieses Vorgehen wird Exzess genannt. Das werbende Vereinsmitglied wird in solch einem Fall eigener Verantwortlicher und unterliegt damit auch

allen nachfolgend erläuterten in der DS-GVO verankerten Rechten und Pflichten. Diese Art der Datenübermittlung an einen Dritten ist nicht rechtmäßig und kann vom TLfDI sanktioniert werden. Zum einen liegt von den betroffenen Vereinsmitgliedern keine erforderliche Einwilligungserklärung nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO vor. Zum anderen ist das Versenden von Werbung in eigener Sache für die Durchführung der Vereinsmitgliedschaft nicht erforderlich, Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO. Demnach erfolgt die Kontaktaufnahme des werbenden Vereinsmitglieds ohne Rechtsgrundlage.

Als Verantwortlicher unterliegt selbstverständlich jeder Verein den Pflichten der Datenschutz-Grundverordnung und muss somit auch den Informationspflichten aus Gründen der Transparenz nach Art. 13 und Art. 14 DS-GVO nachkommen. Informationspflichten sind gegenüber den Vereinsmitgliedern und gegenüber Dritten (z. B. Spendengeber) zu erfüllen und umfassen den Umgang mit personenbezogenen Daten. Formulierungsvorschläge zu den Informationen nach Art. 13 und 14 DS-GVO finden Sie unter https://www.tlfdi.de/tlfdi/europa/europaeischedsgvo/index.aspx. Hier steht auch das Kurzpapier Nr. 10 „Informationspflichten bei Dritt- und Direkterhebung“ der Datenschutzkonferenz des Bundes und der Länder zur Verfügung.

Ein Beispiel für eine Datenverarbeitung im Auftrag stellt das Nutzen von Dienstleistungen eines Server-Betreibers (z. B. Hosting Website) dar. In solchen Fällen ist zu beachten, dass der Verein nur Auftragsverarbeiter einsetzen darf, die nach Art. 28 Abs. 1 DS-GVO eine hinreichende Garantie für eine datenschutzkonforme Datenverarbeitung gewährleisten. Die Auftragsverarbeitung darf nur auf der Grundlage eines bindenden Vertrages erfolgen. Dieser Vertrag muss die in Art. 28 Abs. 3 DS-GVO festgelegten Anforderungen erfüllen. Als Hilfestellung hat der TLfDI eine Formulierungshilfe für einen Vertrag zur Auftragsdatenverarbeitung unter der nachfolgend genannten Internetadresse zur Verfügung gestellt.

Weitere Informationen finden Sie in Kurzpapier Nr. 13 der Datenschutzkonferenz mit dem Titel „Auftragsverarbeitung“ (https://www.tlfdi.de/mam/tlfdi/gesetze/dsk_kpnr_13_auftragsverarbeitung.pdf).

Laut Art. 30 der DS-GVO hat jeder Verantwortliche, und somit auch jeder Verein, ein Verzeichnis aller Verarbeitungstätigkeiten zu führen. Das Verarbeitungsverzeichnis muss schriftlich oder in einem elektronischen Format geführt werden. Der Verein ist verpflichtet, der Aufsichtsbehörde (TLfDI) das Verzeichnis auf Anfrage zur Verfügung zu stellen. Ein Einsichtsrecht für betroffene oder nicht betroffene Personen besteht nach der DS-GVO nicht. Differenzierter ist die Rechtslage nach dem Thüringer Informationsfreiheitsgesetz (ThürIFG) bei öffentlichen Stellen zu betrachten: Bei Verzeichnissen von Verarbeitungstätigkeiten öffentlicher Stelle (also nicht bei Vereinen) handelt es sich um amtliche Informationen nach § 3 Nr. 1 ThürIFG, worauf grundsätzlich ein Recht auf Informationszugang besteht. Einem Informationszugang können jedoch Ausschlussgründe, die in den §§ 7 bis 9 ThürIFG normiert sind, entgegenstehen. Dies könnte z. B. bei Art. 30 Abs. 1 lit. g) DS-GVO - technische und organisatorische Maßnahmen (TOMs) – der Fall sein (siehe dazu auch das Anwendungsbeispiel für ein Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 DS-GVO, Seite 7 - https://www.tlfdi.de/mam/tlfdi/datenschutz/muster_verarbeitungsv.pdf). Mit der Problematik der Einsichtnahme des Verzeichnisses der Verarbeitungstätigkeiten öffentlicher Stellen nach den Informationsfreiheits- bzw. Transparenzgesetzen wird sich auch der Arbeitskreis der Informationsfreiheitsbeauftragten in Deutschland in seiner nächsten Sitzung befassen.

Folgende Kriterien muss solch ein Verzeichnis erfüllen:

- Name und Kontaktdaten des Vereins sowie seines Vertreters
- Zwecke der Datenverarbeitung

- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind bzw. noch offengelegt werden
- möglicherweise Angaben über Drittlandtransfer einschließlich Angabe des Drittlandes sowie Dokumentierung geeigneter Garantien
- wenn möglich Fristen für die Löschung der verschiedenen Datenkategorien
- wenn möglich Beschreibung der technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 DS-GVO

Wie ein Verzeichnis von Verarbeitungstätigkeiten formuliert werden kann, hat der TLfDI anhand eines Beispiels unter https://www.tlfdi.de/mam/tlfdi/themen/muster_verarbeitungsverzeichnis_verantwortlicher.pdf dokumentiert.

Der TLfDI hat zudem eine Stellungnahme zum Umgang mit Fotoaufnahmen im Rahmen der Öffentlichkeitsarbeit von Vereinen zur Verfügung gestellt. (https://tlfdi.de/mam/tlfdi/datenschutz/umgang_mit_fotoaufnahmen_im_rahmen_der_offentlichkeitsarbeit_von_vereinen_.pdf). Demnach ist die Veröffentlichung von Fotos, auf denen abgebildete Personen im Vordergrund stehen, ausschließlich nur mit der Einwilligung der betroffenen Personen möglich. Dies fällt in den Anwendungsbereich von Art. 6 Abs. 1 Buchstabe a) DS-GVO. Hiervon abzugrenzen ist die Verwertung von Aufnahmen, auf denen sich eine Vielzahl von Personen zumeist zusätzlich als sogenanntes Beiwerk oder im Rahmen von Übersichtsaufnahmen befindet, z. B. Zuschauerränge bei Sportveranstaltungen oder Publikumsaufnahmen im Hintergrund künstlerischer Darbietungen. Für die Verbreitung und öffentliche Zurschaustellung von Fotos war bisher § 22f des Kunsturhebergesetzes (KUG)

anzuwenden. Inwieweit das Kunsturhebergesetz neben der Datenschutz-Grundverordnung anwendbar bleibt, ist derzeit noch nicht rechtskräftig geklärt.
Ungeachtet der Diskussion, ob das KUG im Rahmen des Art. 85 Abs. 1 DS-GVO bereits von der deutschen Anpassungsgesetzgebung erfasst ist, ist das Ergebnis in der praktischen Auswirkung ähnlich. Die Wertungen des KUG fließen im Rahmen der Interessenabwägung der betroffenen Personen nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO ein (Landgericht Frankfurt/Main vom 13. September 2018 (AZ: 2-03 O 83/18)). Demnach ist die Verarbeitung von personenbezogenen Daten rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen eines Vereins erforderlich ist, sofern nicht nach Art. 6 Abs. 1 Satz 1 Buchstabe f) der DS-GVO die Interessen oder Grundrechte und Grundfreiheiten betroffener Personen, die den Schutz personenbezogener Daten erfordern, überwiegen. Solange eine Ansammlung von Personen dargestellt wird, ohne dass eine Person oder wenige Personen im Fokus des Motivs stehen, werden im Regelfall keine schutzwürdigen Interessen verletzt, weil demzufolge lediglich die Sozialsphäre und nicht die Persönlichkeitssphäre der abgebildeten Personen betroffen ist. Hierfür ist von jedem Verein individuell vor der geplanten Datenverarbeitung eine Interessenabwägung auszuarbeiten, die die Risiken für die Rechte und Freiheiten der betroffenen Personen berücksichtigt.
Ein besonderer Schutz gilt bei der Ablichtung von Kindern. Im Zweifel fällt die Interessenabwägung immer zu Gunsten der Kinder aus, weshalb bereits das Erstellen von Aufnahmen nur auf eine Einwilligung der sorgeberechtigten Person bzw. Personen gestützt werden kann.
In aller Regel ist für Vereine nur dann ein Datenschutzbeauftragter (DSB) nach der Maßgabe des Art. 37 DS-GVO zu benennen, wenn mehr als zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind. Dabei ist ständig beschäftigt, wer z. B. permanent die Mitgliederverwaltung führt oder die Lohnabrechnung vornimmt.
Für weitere Informationen möchten wir auf die Orientierungshilfe „Datenschutz im Verein nach der DS-GVO“ des Landesbeauftragten

für den Datenschutz Baden-Württemberg verweisen: https://www.tlfdi.de/tlfdi/europa/europaeischedsgvo/index.aspx

5.33 Die DS-GVO, ein Freibrief für zügellose Videoüberwachung im nicht-öffentlichen Bereich?

Mit dem Inkrafttreten der Datenschutz-Grundverordnung erreichten den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit zahlreiche Anfragen zum Datenschutzrecht beim Betreiben von Videokameras. Viele Bürger und Bürgerinnen kritisierten eine „fehlende Regelung in der neuen Datenschutz-Grundverordnung“, die der Videoüberwachung einen klaren datenschutzrechtlichen Rahmen setzt. Sie befürchteten, dass das Fehlen eines solchen Abschnitts als Carte blanche für ungezügeltes Videoüberwachen zu verstehen ist. Insbesondere erreichten den Thüringer Landesbeauftragten für Datenschutz und Informationsfreiheit Anfragen zu Videoüberwachungsaspekten wie Kameraattrappen, Hinweispflichten und Dashcam Nutzung in Autos. Was muss man generell beim neuen Datenschutzrecht hinsichtlich des Betreibens von Videokameras beachten? Dieser Tätigkeitsberichtsbeitrag fasst daher alle wichtigen Punkte zum Thema Videoüberwachung durch nicht-öffentliche Stellen (Privatpersonen und Unternehmen) nach der DS-GVO zusammen.

Auch wenn die Datenschutz-Grundverordnung (DS-GVO) keine spezifische Regelung zur Videoüberwachung enthält, stellt diese eine Datenverarbeitung dar, die an den Vorschriften zum Datenschutzrecht, hier anhand von Art. 6 Abs. 1 Buchstabe f) DS-GVO, zu messen ist. Der nationale Gesetzgeber hat zwar mit § 4 Bundesdatenschutzgesetz (BDSG) eine dem alten § 6b BDSG entsprechende Norm für Videoüberwachungen im öffentlich zugänglichen Räumen geschaffen, jedoch besteht hier auf theoretischer Ebene Streit, ob diese Norm im nicht-öffentlichen Bereich überhaupt aufgrund fehlender Öffnungsklausel und des Anwendungsvorrangs der DS-GVO Beachtung finden

kann. Bedeutung erlangt dies erst, wenn eine Prüfung der der DS-GVO und neuen BDSG Vorschriften zu unterschiedlichen Ergebnissen kommen würde, wovon nur sehr selten auszugehen ist.

I. Anwendungsbereich

Nicht alle Videoüberwachungen fallen unter das Datenschutzrecht. Hier gilt auch weiterhin die Ausnahme nach Art. 2 Abs. 2 Buchstabe c) der DS-GVO, dass Verarbeitungen, die in Ausübung persönlicher oder familiärer Tätigkeiten durchgeführt werden, nicht mithilfe der DS-GVO zu bemessen sind. Dies ist z. B. der Fall, wenn Aufnahmen lediglich im privaten Bereich verbleiben, also z. B. als Erinnerung an bestimmte private Erlebnisse. Sie dürfen ebenfalls nicht in Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen werden. Sobald im privaten Bereich eine Videoüberwachung Beweiszwecken dienen soll, wie beispielsweise bei einer Kameraüberwachung des eigenen Grundstücks, ist dies nicht mehr der reinen persönlichen oder familiären Tätigkeit zuzuordnen, da die persönliche und familiäre Sphäre aufgrund einer möglichen Übermittlung an die Strafverfolgungsbehörden verlassen wird. Das Datenschutzrecht kommt dann vollständig zur Anwendung. Überwacht eine Kamera das Nachbargrundstück oder den Eingangsbereich eines Hauses geht dies ebenfalls über den persönlichen und familiären Bereich hinaus. Auch eine Veröffentlichung von Aufnahmen führt zur Anwendung des Datenschutzrechts, was vielen Personen nicht klar ist.
Die DS-GVO gilt zudem nach Art. 2 Abs. 1 DS-GVO für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten, sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.
Videoüberwachungen in Echtzeit, digitale Videoüberwachungssysteme, Kamera-Monitor-Systeme fallen alle in den Anwendungsbereich der DS-GVO, da es sich hierbei entweder um eine automatisierte oder teilweise automatisierte Videoüberwachung handelt.

II. Prüfung der Rechtmäßigkeit der Videoüberwachung

Sofern also der Anwendungsbereich der DS-GVO zutrifft, sind Videoüberwachungen von nicht-öffentlichen Stellen anhand von Art. 6 Abs. 1 Buchstabe f) der DS-GVO zu bemessen. Dabei ist zu beachten, dass jede durchgeführte Videoüberwachung eine Einzelfallprüfung darstellt!

Nur in seltenen Fällen kann die Zulässigkeit der Videoüberwachung auf eine Einwilligung nach Art. 6 Abs. 1 Buchstabe a) der DS-GVO in Verbindung mit Art. 7 der DS-GVO gestützt werden. Zudem stellt das Passieren eines gekennzeichneten Überwachungsbereichs keine Einwilligung im Sinne des Art. 4 Nr. 11 der DS-GVO dar.
Die nach Art. 6 Abs. 1 Satz 1 Buchstabe f) der DS-GVO durchzuführende Zulässigkeitsprüfung erfolgt nach dem bisher im BDSG festgelegten Kriterien:

- Wahrung berechtigter Interessen
- Erforderlichkeit
- Interessenabwägung.
- Transparenz der Videoüberwachung

Im Rahmen des berechtigten Interesses verbleibt es wie bisher dabei, dass dieses Interesse ideeller, wirtschaftlicher oder rechtlicher Natur sein kann. Sofern die Videoüberwachung zur Gefahrenabwehr und zu Beweissicherung hinsichtlich möglicher Straftaten eingesetzt werden soll, ist vom Betreiber eine sogenannte konkrete Gefahrenlage nachzuweisen. Hierbei werden vom Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) konkrete Tatsachen gefordert, die eine Gefahrenlage rechtfertigen wie z. B. Beschädigungen oder Vorkommnisse aus der Vergangenheit, Vorlage der entsprechenden polizeilichen Tagebuchnummern bzw. staatsanwaltschaftlichen Aktenzeichen. Eine abstrakte Gefahrenlage ist nur in bestimmten Ausnahmefällen anzunehmen. Hierbei handelt es sich um Orte, die kriminalstatistisch typischerweise, im Hinblick auf Vermögens- und Eigentumsdelikte, potentiell als besonders gefährdet einzustufen sind wie z. B. Geschäfte, die wertvolle Ware verkaufen (Juweliere, Tankstellen etc.). Neu im Bereich des berechtigten Interesses ist, dass nun auch Drittinteressen zu berücksichtigen sind. Dritte sind nach Art. 4 Nr. 10 DS-GVO sowohl private und juristische Personen, die jedoch nicht der Verantwortlicher, Auftragsverarbeiter und betroffene Person gleichzeitig sein kann. Jedoch ist derzeit noch nicht ganz klar, in welchem Fall ein zulässiges Drittinteresse vorliegt. Hier kommt es auch auf den jeweiligen Einzelfall an.
Weiterhin muss die durchgeführte Videoüberwachung für den festgelegten Zweck, geeignet und erforderlich sein. Eine Erforderlichkeit in diesem Sinn kann nur dann bestätigt werden, wenn der beabsichtigte Zweck nicht mit einem anderen (wirtschaftlich und organisatorisch) zumutbaren Mittel erreicht werden kann, die weniger stark in die Rechte möglicher betroffener Personen eingreifen. Dabei müssen vor

Installation einer Videoüberwachungsanlage mögliche alternative Maßnahmen voneinander abgewogen werden (Sicherheitsschlösser, einbruchssichere Fenster und Türen, Umzäunung, bessere Ausleuchtung des Geländes etc.). Bei der Erforderlichkeit muss auch der räumliche und zeitliche Umfang der Videoüberwachung berücksichtigt werden. Zudem ist zu untersuchen, ob eine Aufzeichnung tatsächlich notwendig ist oder ob ein Beobachten (Monitoring) auch ausreichend ist. Hier gibt es viele Aspekte die vorab durchdacht werden müssen.
Am Ende der Prüfung ist dann eine einzelfallorientierte Interessenabwägung zwischen den berechtigten Interessen des Kamerabetreibers und den schutzwürdigen Interessen der betroffenen Personen durchzuführen. Bei dieser Interessenabwägung darf keine abstrakte oder auf vergleichbare Fälle durchzuführende Betrachtung erfolgen, sondern es ist eine Abwägung im konkreten Einzelfall durchzuführen. Hierbei kommt es infolge des Erwägungsgrunds 47 der DS-GVO zu einer Relativierung des bisher strikt objektiven Ansatzes. Mit der DS-GVO gilt nun als Maßstab, dass die „vernünftigen Erwartungen der betroffenen Personen, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen“ sind. Dabei sind zunächst die subjektiven Erwartungen einer betroffenen Person im Einzelfall abzuwägen. Zudem ist zu hinterfragen, was ein objektiver Dritter vernünftigerweise erwarten kann oder darf. Entscheidend ist daher, ob die Videoüberwachung in bestimmten Bereichen der Sozialsphäre typischerweise akzeptiert oder abgelehnt wird. Videoüberwachung im Nachbarschaftskontext und im Individualbereich wie z. B. Wohnräume, Sportausübung/Fitness, oder in ärztlichen Behandlungs- und Warteräumen ist in der Regel unzulässig. Ausnahmslos nicht akzeptiert ist eine Videoüberwachung, die die Intimsphäre verletzt, z. B. in Sanitär- und Saunabereichen.
Die oben aufgeführten Punkte sind vor der Inbetriebnahme einer Videoüberwachung durch den Kamerabetreiber bzw. den Verantwortlichen zu prüfen. Sollte der TLfDI eine Beschwerde zu einer Videoüberwachung erhalten, werden diese einzelnen Prüfungsschritte im Rahmen der Rechtmäßigkeit der Verarbeitung überprüft.

III. Transparenzanforderungen / Hinweis auf die Videoüberwachung

Mit der DS-GVO sind bei Videoüberwachungen nun auch höhere Transparenzanforderungen vom Kamerabetreiber zu beachten. Neben der rechtmäßigen Verarbeitung fordert die DS-GVO in Art. 5 Abs. 1

Buchstabe a), dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden müssen.
Es gelten hierbei nun umfangreichere Informationspflichten des Verantwortlichen nach Art. 12 ff. der DS-GVO. Im Rahmen der Videoüberwachung kommt Art. 13 DS-GVO zur Anwendung. Zwei Mustervorlagen für Hinweisschilder, die der Transparenzpflicht gemäß DS-GVO entsprechen, stellt der TLfDI auf seiner Website zur Verfügung. Neu ist, dass eine intransparente Videoüberwachung grundsätzlich nicht im Einklang mit Art. 5 und Art. 13 der DS-GVO steht. Die Aufsichtsbehörde kann gemäß Art. 58 Abs. 2 Buchstabe f) der DS-GVO die Videoüberwachung vorübergehend beschränken oder endgültig untersagen. Mangelnde Transparenz stellt zudem ein Bußgeldtatbestand nach Art. 83 Abs. 5 der DS-GVO dar.

IV. Speicherdauer / Löschungsgebot

Eine konkrete auf die Videoüberwachung bezogene Regelung zur Speicherdauer enthält die DS-GVO nicht. Daher ist auf allgemeine Regelungen zurückzugreifen. Nach Art. 17 Abs. 1 Buchstabe a) der DS-GVO sind die Daten der Videoüberwachung unverzüglich zu löschen, wenn sie ihren ursprünglichen Erhebungs- und Verarbeitungszweck erfüllt haben und eine weitere Speicherung den schutzwürdigen Interessen betroffener Personen entgegensteht. Sofern die Videoüberwachung zur Beweissicherung dient, dürfte grundsätzlich innerhalb von ein bis zwei Tagen geklärt werden können, ob eine Sicherung des Materials notwendig ist. Hierbei sind die beiden Grundsätze der Datenminimierung und Speicherbegrenzung laut Art. 5 Abs. 1 Buchstabe c) und e) der DS-GVO zu berücksichtigen. Demzufolge sollte wie bisher eine Löschung erhobener personenbezogener Daten in der Regel spätestens nach 48 Stunden erfolgen. Eine automatisierte periodische Löschung z. B. durch Selbstüberschreiben der Aufnahmen wird dem Löschungsgebot am wirksamsten gerecht.

V. Technische und organisatorische Gestaltung bzw. Maßnahmen

Bei der Beschaffung, der Installation und dem Betrieb von Videoüberwachungssystemen ist vom Verantwortlichen auf die sichere und datenschutzfreundliche Gestaltung gemäß Art. 32 und Art. 25 der DS-GVO zu achten. Dabei ist zu prüfen, inwieweit eine Videoüberwachung zeitlich eingeschränkt werden kann und ob Bereiche ausgepixelt bzw. geschwärzt werden können. Dabei ist bei der Beschaffung der notwendigen Hardware auf einen „eingebauten Datenschutz“ zu

achten. Nicht benötigte Funktionalitäten wie z. B. freie Schwenkbarkeit, Zoomfähigkeit, Funkübertragung, Internetveröffentlichung, Audioaufnahme (!) etc. sollten durch die beschaffte Technik nicht unterstützt oder zumindest bei der Inbetriebnahme deaktiviert werden. Vom Verantwortlichen sind technische und organisatorische Maßnahmen zu treffen die im Einklang mit dem aufgeführten Katalog unter § 9 Anlage 1 des alten BDSG stehen. Hierzu gehören Regelungen wie Zugangskontrolle, Zugriffskontrolle, Eingabekontrolle, Auftragskontrolle u. v. m.

VI. Verzeichnis von Verarbeitungstätigkeiten

Seitens des Verantwortlichen ist nach Art. 30 Abs. 1 DS-GVO ein sog. Verzeichnis von Verarbeitungstätigkeiten zu führen. Dieses löst das bisherige Verfahrensverzeichnis nach § 4 Buchstabe e) des BDSG ab. Videoüberwachungen sind zudem nicht mehr zu melden. Jedoch ist das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 3 und 4 der DS-GVO schriftlich zu führen und auf Anfrage der Aufsichtsbehörde vorzulegen. Im Verarbeitungsverzeichnis soll die Videoüberwachung ausgewiesen und dokumentiert werden und dargelegt werden welchem Zweck die Verarbeitung jeweils dient. Ein entsprechendes Muster wurde von allen Aufsichtsbehörden des Bundes und der Länder bereitgestellt und ist auf der Website des TLfDI mit entsprechenden den Hinweisen abrufbar.

Sofern vom TLfDI eine unrechtmäßige Verarbeitung personenbezogener Daten mittels Videoüberwachungskameras festgestellt wird, kann dieser nach Art. 58 Abs. 2 Buchstabe d) und f) der DS-GVO eine weitere Verarbeitung verbieten, beschränken oder den Verantwortlichen anweisen die Verarbeitung auf rechtskonforme Weise vorzunehmen. Darüber hinaus kann der TLfDI ein Bußgeld nach Art. 83 Abs. 5 der DS-GVO verhängen.

Im Bereich der Videoüberwachungen gibt es bestimmte Sonderformen, wie z. B. die Videoüberwachung mittels Dashcams an Fahrzeugen, die ebenfalls nach den o. g. Kriterien zu beurteilen sind. Dashcams rückten im Berichtszeitraum besonders in den Fokus, da der Bundesgerichtshof über die Beweisverwertbarkeit von Videoaufnahmen mittels Dashcam in einem Unfallhaftungsprozess entscheiden musste. Die Aufsichtsbehörden des Bundes und der Länder gehen davon aus, dass eine durchgehende anlasslose Aufzeichnung mithilfe einer im oder an einem Fahrzeug angebrachten Dashcam gegen das Datenschutzrecht verstößt, da hier die Interessenabwägung immer zu

Lasten des Kamerabetreibers ausgeht. Es überwiegen hier die Interessen von Passanten oder anderen Verkehrsteilnehmern nicht überwacht zu werden. Der Bundesgerichtshof hatte in seiner Entscheidung vom 15. Mai 2018 (Aktenzeichen: VI ZR 233/17) zwar eine Beweisverwertbarkeit von Aufnahmen im Zivilprozess nicht verneint, jedoch betont, dass der anlasslose Einsatz von dauerhaft aufzeichnenden Dashcams datenschutzrechtlich unzulässig ist. Daher widerspricht die Auffassung der Aufsichtsbehörden nicht der höchstrichterlichen Rechtsprechung, so dass weiterhin entsprechende Verbote oder Bußgelder verhangen werden können.

5.34 Umgang mit Werbung und Direktwerbemaßnahmen nach DS-GVO

Die Zulässigkeit von Direktwerbemaßnahmen ist nicht mehr speziell geregelt, wie das im bisherigen Bundesdatenschutzgesetz der Fall gewesen ist. Sie ergibt sich vielmehr aus den allgemeinen Verarbeitungsgrundsätzen der DS-GVO.

Mit der Datenschutz-Grundverordnung (DS-GVO) sind alle detaillierten Regelungen des bisherigen Bundesdatenschutzgesetzes der alten Fassung (BDSG a. F.) zur Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung weggefallen. Insbesondere Regelungen wie den § 28 Abs. 3 und Abs. 4 sowie § 29 BDSG gibt es in der DS-GVO nicht mehr.
Die Grundlage für die Zulässigkeit von Werbemaßnahmen bildet nunmehr allein der Art. 6 der DS-GVO. Hier ist neben der Einwilligung gemäß Art. 6 Abs. 1 Satz 1 Buchstabe a) der DS-GVO insbesondere Buchstabe f) desselben Artikels Abs. 1 Satz 1 der DS-GVO als Rechtsgrundlage heranzuziehen. Die Verarbeitung muss danach zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich sein, sofern nicht die Interessen der betroffenen Person überwiegen. Bei dieser Interessenabwägung ist auf die vernünftigen Erwartungen des Einzelnen einzugehen, die auf seiner Beziehung zum Verantwortlichen beruhen. Zudem ist auch die Frage zu stellen, was vernünftigerweise erwartet werden kann, also ob die Verarbeitung zu Werbezwecken in bestimmten Bereichen typischerweise akzeptiert oder abgelehnt wird.

So ist in der Regel davon auszugehen, dass solche Werbemaßnahmen von der Erwartungshaltung des Kunden gedeckt sind, wenn beispielsweise im Nachgang einer Bestellung, dem Kunden ein Werbeschreiben oder ein Katalog zu weiteren Produkten des Verantwortlichen zugesendet werden. Andere Kontaktwege wie z. B. Telefon, E-Mail und Fax, regelt zusätzlich das Wettbewerbsrecht (§ 7 Gesetz gegen den unlauteren Wettbewerb [UWG]), um zu spezifizieren wann von einer unzumutbaren Belästigung der Betroffenen auszugehen ist. Diese Wertung ist dann auch im Hinblick auf die Interessenabwägung bezüglich des Art. 6 Abs. 1 Satz 1 Buchstabe f) der DS-GVO zu berücksichtigen. So gibt das UWG vor, dass bei Anrufen zu Werbezwecken eine Einwilligung vom Verbraucher erforderlich ist. Die Nutzung von Telefonnummern ohne vorherige Einwilligung kann daher in keinem Fall auf ein berechtigtes Interesse des Werbenden gestützt werden. Eine Einwilligung in derartige Werbemaßnahmen ist nur dann wirksam, wenn sie freiwillig und, bezogen auf den bestimmten Fall, informiert abgegeben wird. Das Transparenzgebot verlangt, dass die Art der Werbung, die Produkte und Dienstleistungen, die beworben werden sollen und das werbende Unternehmen angegeben werden. Für die Einwilligungserklärung ist von der DS-GVO keine besondere Form vorgesehen, es wird allerdings empfohlen, aufgrund der Nachweispflicht des Verantwortlichen, eine Einwilligungserklärung wenigstens in Textform einzuholen. Für elektronisch abgegebene Willenserklärungen ist das sogenannte „Double-Opt-in"-Verfahren zu nutzen. Hierbei muss der Einwilligende zunächst seine E-Mail-Adresse angeben. An diese wird dann eine Bestätigungsmail gesandt um zu verifizieren, dass derjenige auch die Verfügungsgewalt über das Mailkonto hat. In dieser Bestätigungsmail befindet sich dann ein Link, der wiederum zur eigentlichen Einwilligungserklärung führt. Diese kann daraufhin bestätigt werden. Der Nachweis der Einwilligung erfordert hier die Protokollierung des gesamten „Opt-in"-Verfahrens sowie den Inhalt der Einwilligung. Bei der Nutzung von besonderen Kategorien von Daten ist immer eine Einwilligung einzuholen, da der Art. 9 der DS-GVO keine Erlaubnisnorm für die werbliche Nutzung von besonderen Datenkategorien enthält. Dies ist insbesondere für werbende Institutionen im Gesundheitswesen zu beachten (Apotheken, Sanitätshäuser und Optiker).

Das auch bisher schon geltende Koppelungsverbot für Werbemaßnahmen ist auch in der DS-GVO verankert. Danach ist bei der Beurteilung, ob eine Einwilligung in Werbemaßnahmen freiwillig erteilt

wurde, darauf zu achten, ob die Erfüllung eines Vertrages oder die Erbringung einer Dienstleistung von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig gemacht wird, die jedoch für die eigentliche Vertragserfüllung nicht erforderlich sind, zum Beispiel, wenn der Abschluss eines Kaufvertrages von der Einwilligung in den Erhalt von E-Mail Newslettern abhängig gemacht würde. Der betroffenen Person steht gemäß Art. 21 Abs. 2 der DS-GVO in jedem Fall ein Widerspruchsrecht gegen werbliche Maßnahmen zu. Auf dieses Widerspruchsrecht ist durch den Werbenden in verständlicher und von anderen Informationen getrennter Form, hinzuweisen. Auch ein Recht auf Löschung der Daten ist zu berücksichtigen. Jedoch sollte in einem solchen Fall gegebenenfalls eindeutig geklärt werden, was die betroffene Person möchte. Für den Fall der Datenlöschung, kann es möglich sein, dass die Daten erneut, z. B. bei einem zulässigen Einsatz von Fremdadressdaten, für die werbliche Ansprache genutzt werden. Dies kann nur dann ausgeschlossen werden, wenn sich die betroffene Person in einer Sperrdatei aufnehmen lässt. Hier wird sichergestellt, dass vor Verwendung der Adressen für werbliche Zwecke ein Abgleich erfolgt und daher keine erneute Werbung bei der betroffenen Person eingeht. Die Umsetzung des Werbewiderspruchs hat durch den Werbenden unverzüglich zu erfolgen.
Letztlich ist auch bei der Erhebung von Daten für Werbezwecke die Informationspflicht zu beachten. Hier muss über die geplante Verarbeitung transparent informiert werden. Wenn die Daten erst nachträglich durch eine Zweckänderung für Werbezwecke genutzt werden sollen, ist ebenfalls eine erneute Information an die betroffenen Personen zu geben. Inhaltlich ergeben sich auch bei einem beschränkten Platzangebot auf Werbepostkarten oder Zeitschriftenbeilagen dieselben Anforderungen an Art. 13 und Art. 14 der DS-GVO wie sonst auch. Möglich erscheint jedoch, dass in diesen Fällen die zu erfüllende Informationspflicht in zwei Stufen erfolgen kann, wobei die Mindestanforderungen bereits in der ersten Stufe umzusetzen sind. Diese beziehen sich auf die Mitteilung von Name und Kontaktdaten des Verantwortlichen und dessen Datenschutzbeauftragten, Zweck und rechtliche Grundlage der Verarbeitung, möglicherweise die Begründung des berechtigten Interesses an der Verarbeitung, eine eventuelle Übermittlung in Drittstaaten, das Widerspruchsrecht nach Art. 21 der DS-GVO und einen Hinweis darauf, wo die weiteren Pflichtinformationen nach Art. 13 Abs. 1 und Abs. 2 der DS-GVO zu finden sind. Dies kann auch

mittels QR-Code oder Internet-Link erfolgen. Diese führen dann zu den weiteren Pflichtangaben nach Art. 13 der DS-GVO.

5.35 Ungebetener Zugriff: Warum WhatsApp ungefragt Kontaktdaten im Telefonbuch ausließt

Wer "WhatsApp" nutzt, lässt eine fortwährende Datenweitergabe zu, ohne zuvor von betroffenen Personen aus dem eigenen Telefon-Adressbuch hierfür jeweils eine Erlaubnis eingeholt zu haben. Damit begeht der WhatsApp Nutzer gegenüber diesen Personen eine deliktische Handlung. Siehe hierzu auch Beitrag 5.28 und https://www.heise.de/newsticker/meldung/Thueringens-Datenschuetzer-Whatsapp-wird-meist-rechtswidrig-genutzt-3983437.html.

WhatsApp scheint derzeit einer der beliebtesten Instant-Messaging-Dienste zu sein. Allerdings ist die Nutzung aus Sicht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) problematisch, da WhatsApp standardmäßig die kompletten Kontaktdaten eines Kommunikationsgerätes ausliest. Somit auch Kontaktdaten von Personen aus dem eigenen Telefonbuch, die gar nicht bei WhatsApp registriert sind. Begründet wird dies damit, dass man kundenorientiert bei Kontaktaufnahme sofort den Namen, also nicht die Telefonnummer, anzeigen möchte. Wenn man diese Einstellung deaktiviert, werden dann allerdings nicht mehr die Namen, sondern nur die Telefonnummern des Kontaktes angezeigt.
Problemtisch ist aus Sicht des TLfDI, dass eben auch Kontaktdaten von Nicht-WhatsApp-Mitgliedern aus dem Kontaktbereich des Gerätes ausgelesen werden, wofür es keine Einwilligung der betroffenen Personen gibt.
Mit der Ansicht ist der TLfDI nicht allein. So hat bereits am 20. März 2017 das Amtsgericht in Bad Hersfeld (AZ F 111/17 EASO) entschieden:
„Wer durch seine Nutzung von "WhatsApp" diese andauernde Datenweitergabe zulässt, ohne zuvor von seinen Kontaktpersonen aus dem eigenen Telefon-Adressbuch hierfür jeweils eine Erlaubnis eingeholt

zu haben, begeht gegenüber diesen Personen eine deliktische Handlung und begibt sich in die Gefahr, von den betroffenen Personen kostenpflichtig abgemahnt zu werden.“

6. Fälle öffentlicher Bereich


© alphaspirit – stressed spam

6.1 Unabhängigkeit der Justiz: Sonderstellung der Gerichte im Datenschutz

Nicht immer kann der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) tätig werden, dies ist u. a. der Fall bei Verstößen gegen den Datenschutz, die dem Bereich der Justiz zuzuordnen sind.

Ein Bürger wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

(TLfDI), weil ein Gericht aus Thüringen über das Verfahren hinausgehend sensible Daten des Beschwerdeführers sowie eine Stellungnahme ohne dessen Einverständnis an Dritte übermittelt habe. Laut Beschwerdeführer habe die Übermittlung keine Relevanz für das Verfahren gehabt.
Auf die Thüringer Gerichte findet das neue Thüringer Datenschutzgesetz (ThürDSG) nach § 2 Abs. 9 ThürDSG wie folgt Anwendung:

Für den Rechnungshof gelten die Bestimmungen über die Aufsichtsbehörde, den Datenschutzbeauftragten sowie das Führen von Verzeichnissen nach Art. 30 der Verordnung (EU) 2016/679 nur, soweit er in Verwaltungsangelegenheiten tätig wird. Für die Gerichte gilt Satz 1 entsprechend mit der Maßgabe, dass § 50 auch bei Verarbeitungstätigkeiten, die in Zusammenhang mit der Mitwirkung an der Strafverfolgung, der Verfolgung von Ordnungswidrigkeiten und der Vollstreckung stehen, keine Anwendung findet.

Da der Sachverhalt der zugrundliegenden Beschwerde den Bereich der Justiz betraf und es sich nicht um eine Verwaltungsangelegenheit gemäß § 2 Abs. 9 ThürDSG handelte, konnte der TLfDI kraft Gesetzes in dieser Angelegenheit nicht tätig werden. Der TLfDI hatte dies dem Beschwerdeführer mitgeteilt und ihm empfohlen sich an den dortigen Datenschutzbeauftragten des Amtsgerichts zu wenden.

6.2 Müssen auch Landtagsabgeordnete einen Datenschutzbeauftragten bestellen?

Müssen auch Landtagsabgeordnete einen Datenschutzbeauftragten bestellen? Mit dieser Frage sah sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) immer wieder konfrontiert. Die klare Antwort darauf lautet: Nein, denn nach Art. 2 Abs. 2 Buchstabe a) Datenschutz-Grundverordnung (DS-GVO) findet die DS-GVO keine Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt. Darunter ist auch das Parlamentsrecht des Thüringer Landtages zu fassen.

Vermehrt wandten sich Landtagsabgeordnete mit der Frage an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), ob ein Datenschutzbeauftragter für das jeweilige Wahlkreisbüro zu bestellen ist.

Mit Art. 37 Abs. 1 DS-GVO führt der europäische Gesetzgeber erstmals eine europaweit geltende Pflicht zur Benennung eines Datenschutzbeauftragten ein. Danach benennen der Verantwortliche und der Auftragsverarbeiter auf jeden Fall und unverzüglich einen Datenschutzbeauftragten, wenn

a) die Verarbeitung von Daten einer Behörde oder öffentlichen Einrichtung durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln,
b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, die aufgrund von Art, Umfang und/oder Zweck eine regelmäßige und systematische Überwachung von betroffenen Personen erfordert,
c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 besteht.

Behörden und öffentliche Stellen müssen somit immer einen Datenschutzbeauftragten bestellen (Art. 37 Abs. 1 DS-GVO).

Allerdings findet die DS-GVO nach Art. 2 Abs. 2 Buchstabe a) DS-GVO keine Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrecht fällt. Darunter ist auch das Parlamentsrecht des Thüringer Landtages zu fassen. Diese Regelung ist auch bei der Klärung der Frage zu beachten, ob Abgeordnete des Thüringer Landtages einen Datenschutzbeauftragten, z. B. in ihrem Wahlkreisbüro zu bestellen haben

Zwar regelt § 13 des Thüringer Datenschutzgesetzes (ThürDSG) die Bestellung eines Datenschutzbeauftragten in öffentlichen Stellen näher. Jedoch: Auch nach § 2 Abs. 6 des ThürDSG gelten die Bestimmungen des ThürDSG für den Landtag nur, soweit er in Verwaltungsangelegenheiten tätig wird. Die Beschlussempfehlung (Drucksache 6/5722) des Innen- und Kommunalausschusses bezüglich des Geset-

zesentwurfs der Landesregierung zum Thüringer Datenschutz-Anpassungs-und-Umsetzungsgesetz EU enthält unter § 2 Abs. 6 ThürDSG folgende Fassung:

„[…] Die Verarbeitung personenbezogener Daten bei der Wahrnehmung parlamentarischer Aufgaben durch den Landtag sowie der parlamentarischen Tätigkeit der Abgeordneten einschließlich der Fraktionen unterliegen nicht den Bestimmungen dieses Gesetzes. Der Landtag erlässt insoweit eine seiner verfassungsrechtlichen Stellung entsprechende Datenschutzordnung.“

Diese Regelung ist auch mit den Vorgaben der DS-GVO vereinbar, weil diese unter anderem für parlamentarische Angelegenheiten unter Berücksichtigung von Art. 2 Abs. 2 Buchstabe a) DS-GVO keine Anwendung finden kann.
Aufgrund dessen besteht für Landtagsabgeordnete keine Pflicht, einen Datenschutzbeauftragten zu bestellen, und keine Zuständigkeit des TLfDI zu kontrollieren, ob datenschutzrechtliche Regelungen bei der parlamentarischen Tätigkeit des Landtags eingehalten werden. Deshalb muss auch keine Meldung eines Datenschutzbeauftragten an den TLfDI durch Landtagsabgeordnete für ihr Wahlkreisbüro erfolgen.

6.3 Die Tücken von Hektik im Umgang mit personenbezogenen Daten

Ein Bürger wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil er von einer öffentlichen Stelle eine E-Mail erhielt, die jedoch nicht für ihn als Empfänger bestimmt gewesen ist. Eine Prüfung des Sachverhalts ergab, dass durch anfallenden Arbeitsstress versehentlich eine falsche E-Mail-Adresse, nämlich die des Beschwerdeführers, in das Empfängerfeld kopiert wurde.

Im Berichtszeitraum wandte sich ein Beschwerdeführer an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil er von einer öffentlichen Stelle fälschlicherweise eine E-Mail erhielt. Diese war nicht an ihn gerichtet, sondern an eine ihm fremde Person. Um dem Sachverhalt nachzugehen, hat der

TLfDI zunächst die betreffende öffentliche Stelle, also den Absender der E-Mail, um eine Erklärung zum Sachverhalt gebeten.
In dieser Stellungnahme wurde gegenüber dem TLfDI angezeigt, dass eine Mitarbeiterin die Absenderadresse kopiert hatte und diese wiederum für die Beantwortung der Mail genutzt habe, indem sie diese in das Empfängerfeld einfügte. Laut Verantwortlichem war dabei nicht ersichtlich, dass es sich bei der verwendeten E-Mail-Adresse um die des Beschwerdeführers handelte. Um den Sachverhalt aus datenschutzrechtlicher Sicht abschließend prüfen zu können, hatte der TLfDI eine Vor-Ort-Überprüfung vorgenommen. Auf diese Weise sollte geklärt werden, ob die Mitarbeiterin aufgrund von Arbeitsstress eine falsche E-Mail-Adresse kopiert und in das Empfängerfeld eingefügt hatte.
Die Überprüfung vor Ort ergab Folgendes: Die falsche E-Mail-Adresse war vermutlich beim Erstellen des Antwortschreibens durch die Kopier-Funktion vom Bearbeiter eingefügt worden und dieser überprüfte vor dem Absenden der E-Mail nicht nochmals, ob alle Angaben stimmig waren.
Der TLfDI kam schließlich zu dem Ergebnis, dass die E-Mail versehentlich an den Beschwerdeführer versandt wurde. Das Ergebnis teilte der TLfDI dem Antragsteller mit und informierte ihn darüber, dass die öffentliche Stelle künftig einen noch sorgfältigeren Umgang mit dem Versenden von E-Mails pflegen werde. Der TLfDI sah daher im Rahmen seines Ermessens von einer weiteren Verfolgung der Angelegenheit ab.
Damit es nicht erneut zu einem solchen Vorfall kommt, hatte der TLfDI die betreffende öffentliche Stelle ausdrücklich dazu angehalten, dass künftig beim Versand von E-Mails noch sensibler darauf zu achten sei, dass alle Angaben übereinstimmen.

6.4 Sind Rosmarin und Pfefferminz die Drogen von heute?

Nachfragen zur Löschung bestehender Betäubungsmitteleinträge (BTM-Eintrag) erreichen den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) regelmäßig. Nach einer Konkretisierung des „Freeze-in“-Erlasses durch das Thüringer Ministerium für Inneres und Kommunales, erreichte der TLfDI im vorliegenden Fall eine Löschung der betroffenen personenbezogenen Daten.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte 2018 eine kuriose Eingabe eines Bürgers, der sich über die Landespolizeiinspektion (LPI) Gotha beschwerte.
In der Vergangenheit wurde der Beschwerdeführer des Öfteren von der Thüringer Polizei kontrolliert. Den Grund für die Polizeikontrollen sah der Betroffene in der Speicherung seiner personenbezogenen Daten bei der Thüringer Polizei. Anlass dieser Datenspeicherungen war eine Verkehrskontrolle der LPI Gotha, bei der Rosmarin und Pfefferminz beim Beschwerdeführer beschlagnahmt wurden. Ob es sich hierbei tatsächlich um illegale Betäubungsmittel handelt, obliegt wohl dem Auge des Betrachters.
Auf Nachfrage des TLfDI teilte die LPI Gotha mit, man habe das Löschersuchen des Betroffenen an die zuständige Autobahnpolizeistation West in Schleifreisen abgegeben. Von dort kam die Antwort, dass tatsächlich gegen den betroffenen Bürger ein Ermittlungsverfahren geführt wurde wegen des Verstoßes gegen das Betäubungsmittelgesetz. Die Staatsanwaltschaft Erfurt stellte dieses Verfahren jedoch wieder ein.
Aufgrund des bis dato bestehenden „Freeze-in“-Erlasses des Thüringer Ministeriums für Inneres und Kommunales (TMIK) konnte bisher keine Löschung der gespeicherten personenbezogenen Daten erfolgen. Aus diesem Grund war der BTM-Eintrag des Betroffenen im polizeilichen Informationssystem vorerst „eingefroren“. Ein solcher „Freeze-in“-Erlass ist eine Anordnung des TMIK, die das Aussondern und Löschen von Akten, Unterlagen, Dateien und sonstigen sächlichen Beweismitteln verhindert, die dem Untersuchungsausschuss 6/1 – Rechtsterrorismus und Behördenhandeln zur Aufarbeitung des Handelns des „Nationalsozialistischen Untergrunds“ und Thüringer Sicherheits- und Justizbehörden – dienen. Nach einer Anpassung des „Freeze-in“-Erlasses im Juni 2018 ist das Löschen personenbezogener Daten unkomplizierter und konnte im beschriebenen Fall erfolgreich durchgesetzt werden.

6.5 Schwärzen von Ausweiskopien: Ein Datenschutz-Knigge für Identitätsfeststellungen

Anfragen besorgter Bürger, welche Anforderungen für Ausweiskopien zur Identitätsfeststellung gelten, erreichen den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) regelmäßig. Die Vorlage einer Kopie des Bundespersonalausweises stellt nach Ansicht des TLfDI das geeignetste und zugleich mildeste Mittel für den Betroffenen dar, um seinen rechtlichen Anspruch auf Auskunftserteilung zu erwirken. Einzelne Datenfelder auf der Personalausweiskopie kann der Antragsteller zudem schwärzen, da sie für die Identifizierung nicht erforderlich sind.

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte im Berichtszeitraum die Beschwerde eines Bürgers, der mit der Identitätsüberprüfung zur Weiterbearbeitung seines schriftlichen Auskunftsersuchens beim Landeskriminalamt Thüringen nicht einverstanden war. Sein Antrag auf Auskunft wurde laut Beschwerdeführer abgelehnt, weil auf der Ausweiskopie u. a. die Ausweisnummer geschwärzt wurde.
Mit der Problematik, welche Anforderungen für Ausweiskopien zur Identitätsfeststellung gelten, hat sich der TLfDI in der Vergangenheit bereits mehrfach auseinandergesetzt. (vergleiche u. a. 12. Tätigkeitsbericht zum Datenschutz: öffentlicher Bereich, Nr. 5.1, 8.7 und 8.8): Dabei vertritt der TLfDI die Auffassung, dass Daten, die nicht zur Identifizierung benötigt werden, von dem Betroffenen auf der Ausweis-Kopie geschwärzt werden können. Dies gilt insbesondere für die Zugangs- und Seriennummer des jeweiligen Ausweises.
Die rechtlichen Vorgaben zur Erhebung und Verwendung personenbezogener Daten aus dem Ausweis durch öffentliche Stellen regelt § 14 Nr. 2 Personalausweisgesetz (PAuswG) und verweist damit auf die §§ 18 bis 20 des Personalausweisgesetzes. Die Personalausweisnummer ist im Personalausweisgesetz hier unter dem Begriff der Seriennummer, und hier in § 2 Abs. 8 des Personalausweisgesetzes geregelt. Gemäß § 20 Abs. 3 des Personalausweisgesetzes dürfen die Seriennummern, die Sperrkennwörter und die Sperrmerkmale von öffentlichen Stellen und nicht-öffentlichen Stellen nicht so verwendet werden, dass mit ihrer Hilfe ein automatisierter Abruf personenbezo-

gener Daten oder eine Verknüpfung von Dateien möglich ist. Umgekehrt folgt daraus grundsätzlich, dass eine nicht automatisierte Erhebung und Verwendung der Seriennummer grundsätzlich zulässig ist. Fraglich ist jedoch in jedem konkreten Einzelfall, ob die Erhebung und Verwendung der Seriennummer eines Personalausweises erforderlich im Sinne des Verhältnismäßigkeitsprinzips ist (hergeleitet aus Art. 20 Abs. 3 Grundgesetz).

Eine Stellungnahme des Landeskriminalamts Thüringen konnte für Aufklärung sorgen. Das Landeskriminalamt Thüringen hat gegenüber dem TLfDI eingeräumt, dass gegenüber dem Beschwerdeführer irrtümlicherweise die auf dem Ausweis aufgedruckte Zugangs- und Seriennummer eingefordert wurde. Allerdings teilte das Landeskriminalamt Thüringen auch mit, dass auf der vorgelegten Ausweisekopie lediglich der Name und Vorname des Bürgers zweifelsfrei erkennbar waren. Weite Teile darüber hinaus waren geschwärzt und der Rest aufgrund der Datenübermittlung per Fax nicht lesbar.

Allerdings ist es für eine datenschutzrechtlich gesicherte Auskunftserteilung erforderlich, zumindest eine gut lesbare Kopie des Personalausweisdokuments vorzulegen bzw. einzureichen. Dies dient der eindeutigen Zuordnung der gespeicherten Daten zur jeweiligen Person und soll missbräuchliche Auskunftsbegehren verhindern. Hierzu werden nach Auskunft des Landeskriminalamt Thüringen regelmäßig folgende Daten benötigt: Name, Anschrift, Geburtsdatum und Gültigkeitsdauer. Aufgrund der Weisungslage des Thüringer Ministerium für Inneres und Kommunales vom 16. Juni 2016 ist vor der Bearbeitung des Auskunftsantrags noch die Unterschrift auf dem Antrag mit der Unterschrift auf dem Personalausweis zu vergleichen.

Alle anderen auf dem Personaldokument befindlichen Daten (zum Beispiel Ausweisnummer, Lichtbild, persönliche Merkmale, Staatsangehörigkeit) können Antragsteller grundsätzlich schwärzen.

Gegenüber einer einfachen Ausweis-Kopie besitzt eine beglaubigte Kopie in Bezug auf einen Identitätsnachweis keinen Mehrwert, da sie letztlich nur bestätigt, dass die Kopie mit dem Original übereinstimmt. Eine beglaubigte Personalausweiskopie stellt nicht uneingeschränkt sicher, dass tatsächlich keine unberechtigte Person Kenntnis vom Inhalt des Auskunftsersuchens erlangt.

Die Vorlage einer einfachen Kopie muss durch den Antragsteller jedoch akzeptiert werden. Im vorliegenden Fall wurde dem Beschwerdeführer letztlich freigestellt, sich mit einer gut leserlichen – aber auch

geschwärzten – Personalausweisekopie erneut an das Landeskriminalamt Thüringen zu wenden.

6.6 Zur Erfassung von Zeugen im polizeilichen Informationssystem der Polizei

In den polizeilichen Informationssystemen der Thüringer Polizei werden eine Vielzahl personenbezogener Daten erfasst, so auch die Daten von Zeugen. Wie man als Zeuge in das Vorgangsverarbeitungssystem der Polizei gelangt, war Ausgangspunkt einer Frage, der der TLfDI nachgegangen ist.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt im Berichtszeitraum eine Anfrage von einem Bürger, der wissen wollte, wie eine andere Person als Zeuge in das Vorgangsverarbeitungsprogramm der Polizei gelangt. Da diese andere Person selber anonym bleiben wollte, konnte der TLfDI in diesem Fall lediglich eine allgemeine Anfrage zur grundsätzlichen Verfahrensweise bei der Aufnahme von Personen als Zeugen an die Polizei stellen.
Als Zeuge wird eine natürliche Person bezeichnet, die aufklärend zu einem Sachverhalt eigene Wahrnehmungen bekunden kann, also ein Zeugnis ablegt. Personenbezogene Daten von Zeugen werden bei der Thüringer Polizei im sogenannten Integrationsverfahren Polizei (kurz: IGVP) gespeichert. Das IGVP ist das sogenannte Vorgangsbearbeitungssystem der Polizei.
Die Beamten erheben personenbezogene Daten im Rahmen der Strafverfolgung innerhalb der ihnen zustehenden Befugnisse, z. B. die Befragung von Personen zum Sachverhalt. Diese Daten werden regelmäßig im IGVP hinterlegt. Polizisten kategorisieren im IGVP nach Personenart und legen somit sogenannte „Personenrollen“ fest; als solche kommen Zeugen, Auskunftspersonen, Mitteiler, Geschädigte und Anzeigeerstatter in Betracht. Die Auswahl der Personenart ist ein Pflichtfeld. Die Einschätzung, inwieweit ein Zeuge, dessen Daten erfasst wurden, tatsächlich sachdienliche Hinweise geben kann, ist nur im konkreten Einzelfall zu treffen. Neben den Zeugen, die die Beamten direkt als solche erheben, weil sich die Situation vor Ort so dargestellt hat, benennen nicht selten auch Anzeigeerstatter einen Zeugen, der

den strafrechtlich relevanten Sachverhalt vermeintlich beobachtet hat, zum Zeitpunkt der Anzeigenaufnahme jedoch nicht mehr vor Ort ist.
lm vorliegenden Fall hatte die Polizei im Zuge der Strafverfolgung gemäß § 163 Abs. 1 der Strafprozessordnung den Sachverhalt zu erforschen und demnach auch einen möglichen, aber noch unbekannten Zeugen aufzunehmen. Ob die Speicherung der personenbezogenen Daten im vorliegenden konkreten Fall berechtigt war, konnte der TLfDI nicht aufklären, da die anfragende Person nicht selbst Betroffener war.
Somit konnte der TLfDI in diesem Fall leider nicht weiter behilflich sein.

6.7 Vertrauen ist gut, Kontrolle ist besser – Dolmetscherverzeichnis der Thüringer Polizei

Eine Einwilligung von Dolmetschern in eine Überprüfung ihrer Zuverlässigkeit kann im Polizeibereich grundsätzlich keine legitimierende Grundlage für den Eingriff in das Recht auf informationelle Selbstbestimmung darstellen. Eine Überprüfung von Dolmetschern auf ihre Zuverlässigkeit erfordert eine spezialgesetzliche Ermächtigungsgrundlage.

Dolmetscher sind auch im Polizeibereich als Sprachmittler eine maßgebliche und verantwortungsvolle Schnittstelle. Ermittelnde Beamte müssen ihnen ein hohes Maß an Vertrauen entgegenbringen, wenn ihnen die zu übersetzende Sprache völlig unbekannt ist. Die Tätigkeit eines Dolmetschers kann maßgeblich dazu beitragen, entlastende oder belastende Erkenntnisse in einem Fall zu liefern. Die Thüringer Polizei führt hierfür ein sogenanntes Dolmetscherverzeichnis. In diesem werden Daten eines geprüften und für die Polizeiarbeit benötigten Dolmetschers für eine Fremd- bzw. Gebärdensprache bereitgestellt. Die Überprüfung der Zuverlässigkeit erfolgt bislang auf Grundlage einer Einwilligung.
Liegen Erkenntnisse über die Unzuverlässigkeit eines Dolmetschers vor, darf dieser nicht bzw. nicht mehr für die Polizei tätig werden und wird aus dem Dolmetscherverzeichnis entfernt.
Obwohl der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) die Absicht zur Eignungsprüfung von

Dolmetschern grundsätzlich nachvollziehen kann, stößt dieses Verfahren jedoch datenschutzrechtliche Bedenken an.
Allein eine Einwilligung betroffener Dolmetscher in eine Zuverlässigkeitsprüfung kann grundsätzlich keine legitimierende Grundlage für den Eingriff in das Recht auf informationelle Selbstbestimmung darstellen. Solche Überprüfungen der Zuverlässigkeit greifen in das Grundrecht auf informationelle Selbstbestimmung ein. Grundrechtseingriffe dürfen insbesondere im Polizeibereich grundsätzlich nicht unter Umgehung gesetzlicher Vorschriften durchgeführt werden. Die Einwilligung ist zwar grundsätzlich als Rechtsgrundlage möglich, hier aber insoweit problematisch, da es sich insbesondere bei angestellten Dolmetschern um keine echte Freiwilligkeit der Einwilligung handeln kann. Denn eine Einwilligung wird stets erteilt werden, um als Dolmetscher weiterhin beschäftigt zu werden. Es ist durchaus für den TLfDI verständlich, dass Dolmetscher als Sprachmittler eine maßgebliche Rolle bei Ermittlungsverfahren einnehmen und die Polizei ihnen ein hohes Maß an Vertrauen entgegenbringen muss.
Dennoch bedürfen derartige Zuverlässigkeitsprüfungen grundsätzlich einer spezialgesetzlichen Ermächtigungsgrundlage. Wenn aber auf solche Zuverlässigkeitsüberprüfungen nicht verzichtet werden kann, dann empfiehlt der TLfDI entsprechende, datenschutzkonforme Regelungen dafür zu schaffen.
Dieser Fall konnte vom TLfDI im Berichtzeitraum noch nicht abgeschlossen werden. Aus diesem Grund wird der TLfDI im kommenden Bericht über den weiteren Verlauf in dieser Sache informieren.

6.8 Datenschutzrechtliche Kontrolle der Rechtsextremismus-Datei beim Thüringer Landeskriminalamt und beim Amt für Verfassungsschutz

Zur Bekämpfung des gewaltbezogenen Rechtsextremismus wird beim Bundeskriminalamt eine standardisierte zentrale Datei geführt, die sogenannte Rechtsextremismus-Datei. Das Landeskriminalamt und das Amt für Verfassungsschutz sind unter den Voraussetzungen des Rechtsextremismus-Datei-Gesetzes (RED-G) verpflichtet, polizeiliche oder nachrichtendienstliche Erkenntnisse unter anderem über Personen, Vereinigungen und Gruppierungen, die dem rechtsextremistischen Milieu zuzuordnen sind, in dieser Datei zu speichern. Die Datei wurde durch den Thüringer Landesbeauftragten für den Datenschutz

und die Informationsfreiheit im Berichtszeitraum bei beiden Behörden geprüft.

In diesem Jahr führte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) beim Thüringer Landeskriminalamt und beim Amt für Verfassungsschutz eine Kontrolle der Rechtsextremismus-Datei (RED) durch. Hintergrund für die Kontrolle ist § 11 Abs. 2 des Rechtsextremismus-Datei-Gesetzes (RED-G). Danach ist der Landesdatenschutzbeauftragte im Rahmen seiner Zuständigkeit verpflichtet, die Durchführung des Datenschutzes zu kontrollieren. Dazu nahm der TLfDI Stichproben von den durch das Landeskriminalamt und dem Amt für Verfassungsschutz getätigten Eingaben und Abfragen in der Rechtsextremismus-Datei.
Die datenschutzrechtliche Verantwortung für die in der Datei gespeicherten Daten, namentlich für die Rechtmäßigkeit der Erhebung, die Zulässigkeit der Eingabe sowie die Richtigkeit und Aktualität der Daten, trägt die Behörde, die die Daten eingegeben hat. Die Verantwortung für die Zulässigkeit der Abfrage von Daten aus der Datei trägt die abfragende Behörde.
Das Bundeskriminalamt hat bei jedem Zugriff zum Zweck der Datenschutzkontrolle den Zeitpunkt, die Angaben, die die Feststellung der aufgerufenen Datensätze ermöglichen, sowie die für den Zugriff verantwortliche Behörde und den Zugriffszweck zu protokollieren.
Sowohl beim Landeskriminalamt als auch beim Amt für Verfassungsschutz konnte der TLfDI feststellen, dass die RED selten genutzt wird und grundsätzlich nicht wirklich für die verantwortlichen Stellen einen großen Nutzen aufweist. Dieses Ergebnis steht im Einklang mit der folgenden Feststellung aus dem Bericht zur Evaluierung des RED-G nach Art. 3 Abs. 2 des Gesetzes zur Verbesserung der Bekämpfung des Rechtsextremismus vom 20. August 2012. Vorgelegt vom Institut für Gesetzesfolgenabschätzung und Evaluation im November 2015 (Bundestags-Drucksache 18/8060) wird dort festgestellt: „Knapp die Hälfte der Sicherheitsbehörden gab an, dass die RED nicht zu einer Verbesserung des Informationsaustausches zwischen den Sicherheitsbehörden geführt habe“ (BT-Drucksache 18/8060, Seite 125, Nr. 7.1 (3) des Evaluationsberichtes).
Da die datenschutzrechtliche Prüfung der Datei beim Landeskriminalamt und beim Amt für Verfassungsschutz im Berichtszeitraum noch nicht abgeschlossen werden konnte, wird der TLfDI im kommenden Tätigkeitsbericht erneut darüber informieren.

Gemäß § 10 Abs. 3 RED-G berichtet das Bundeskriminalamt dem Deutschen Bundestag alle drei Jahre über den Datenbestand und die Nutzung der Rechtsextremismus-Datei. Dieser Bericht ist auch auf der Internetseite des Bundeskriminalamtes zu veröffentlichen. Der nächste Bericht wird im Jahr 2020 veröffentlicht werden. Es bleibt abzuwarten, ob sich im Rahmen des nächsten Berichts herausstellt, dass sich die Einrichtung dieser Datei wirklich bewährt hat.

6.9 Ein Messenger-Dienst für die Thüringer Polizei

Neben anderen Bundesländern plant nun auch das Thüringer Ministerium für Inneres und Kommunales (TMIK) die Einrichtung eines Messenger-Dienstes für die Thüringer Polizei. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wird die Implementierung des Messenger-Dienstes in Zusammenarbeit mit dem Thüringer Ministerium für Inneres und Kommunales (TMIK) datenschutzrechtlich begleiten.

Aus der Thüringischen Landeszeitung erfuhr der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), dass das Thüringer Ministerium für Inneres und Kommunales (TMIK) die Einrichtung eines Messenger-Systems plant. Dieses soll einem schnellen Nachrichtenaustausch und einer Verbesserung der Infrastruktur in den Dienststellen dienen.
Aus der Drucksache 6/4951 unter II. d) war hierzu folgendes zu entnehmen:
Unter Beteiligung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit soll unter Beachtung bereits bestehender Entwicklungen im Rahmen der IT-Kooperation ein internes Messenger-System für die Thüringer Polizei konzipiert werden, das auf mobilen Endgeräten eine gesicherte verschlüsselte Kommunikation von Textnachrichten und Versendung von Multimediadateien ermöglicht, um insbesondere bei größeren Einsätzen, Vermissten- und Fahndungsmeldungen einen datenschutzkonformen Austausch zu ermöglichen. Ein kooperatives Vorgehen auf Basis länderübergreifender Erfahrungswerte und Lösungsansätze wird als zielführend erachtet.

(siehe http://www.parldok.thueringen.de/ParlDok/dokument/65361/th%c3%bcringer-polizei-4-0-mit-digitalisierung-und-modernisierung-fit-f%c3%bcr-die-zukunft-neufassung-.pdf)

Weiterhin wird in der Drucksache 6/4951 unter II. f) der Ausbau der Internet-Nutzung wie folgt thematisiert:
Im Einvernehmen mit dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit soll durch eine datenschutzkonforme und datensichere Regelung der Internetzugang für die Thüringer Polizei erleichtert werden. So sollen internetzugängliche Computerarbeitsplätze ausgebaut und den Bediensteten, insbesondere im Polizeibildungszentrum Meiningen und bei der Bereitschaftspolizei Thüringen, WLAN-Netzwerke zur Verfügung gestellt werden. (am angegebenen Orte)
Die Nachfrage beim TMIK ergab, dass die Einführung eines internen Messengers durch das TMIK dort im Gesamtkontext der Digitalisierungsbestrebungen der Thüringer Polizei betrachtet wird. Der Konzeptentwurf des TMIK beinhalte nach eigenen Angaben auch die Einführung eines polizeilichen Messengers. Grundlage für das weitere Vorgehen sei das Vorliegen einer belastbaren Erhebung der bestehenden Bedarfe. Diese würden derzeit identifiziert und beschrieben. Aus Gründen der Wirtschaftlichkeit werde vom TMIK derzeit geprüft, inwiefern bereits durch Polizeien des Bundes und der Länder oder in polizeilichen IT-Kooperationen entwickelte Messenger geeignet seien, den fachlichen Bedarf der Thüringer Polizei abzudecken. Eine Konzipierung und Entwicklung eines eigenen Messengers werde insbesondere unter dem Aspekt der bundesweit angestrebten Harmonisierung polizeilicher IT nicht präferiert.
Daneben wird auch in Bayern derzeit die Einführung von Smartphones mit einem Messenger-Dienst als einsatzunterstützendes Kommunikationsmittel geplant. Der TLfDI wird weiter über die Entwicklung in dieser Angelegenheit in seinem nächsten Tätigkeitsbericht informieren.

6.10 Der Polizeibeamte als Zeuge

Die Erfassung personenbezogener Daten eines Polizeibeamten, der in seiner amtlichen Eigenschaft als Zeuge auftritt, erfolgt unter den gesetzlichen Voraussetzungen des § 68 der Strafprozessordnung. Dabei kann er aus datenschutzrechtlichen Gründen während einer Vernehmung anstelle des Wohnortes seinen Dienstort angeben.

In dem Vorgangsbearbeitungssystem der Polizei (IGVP) werden bei der Bearbeitung von Fällen auch personenbezogene Daten von Polizeibeamten vermerkt, die z. B. als Zeugen oder Anzeigeerstatter in Betracht kommen würden. Dazu werden der Nachname, der Dienstgrad und die Anschrift der entsprechenden Dienststelle im IGVP erfasst.
Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichten Hinweise, dass zukünftig insbesondere die Privatanschrift der jeweiligen Beamten vermerkt werden soll.
Daraufhin bat der TLfDI die entsprechende Polizeidienststelle um eine Stellungnahme, aus welchem Grund nun detailliertere personenbezogene Angaben erforderlich werden würden. Es stellte sich dabei heraus, dass es keine Änderung der bisherigen Verfahrensweise gegeben hat. Ein datenschutzrechtlicher Verstoß war somit nicht festzustellen.
Allerdings erfolgt die Erfassung personenbezogener Daten eines Polizeibediensteten, der in amtlicher Eigenschaft tätig wird, unter Berücksichtigung des § 68 der Strafprozessordnung (StPO). Dieser regelt die Vernehmung zur Person sowie die Beschränkung von Angaben und den Zeugenschutz. Gemäß § 68 Abs. 1 StPO beginnt die Vernehmung damit, dass ein Zeuge zu Vornamen, Nachnamen, Geburtsnamen, Alter, Beruf und Wohnort befragt wird. Ein Zeuge, der in Wahrnehmung seiner amtlichen Eigenschaft handelt, kann statt des Wohnortes den Dienstort angeben.
Besteht ein begründeter Anlass zur Besorgnis, dass durch die Offenbarung der Identität oder des Wohn- oder Aufenthaltsortes des Zeugen Leben, Leib oder Freiheit des Zeugen oder einer anderen Person gefährdet wird, kann ihm nach § 68 Abs. 3 StPO gestattet werden, Angaben zur Person nicht oder nur über eine frühere Identität zu machen. Er hat jedoch in der gerichtlichen Hauptverhandlung auf Nachfrage

anzugeben, in welcher Eigenschaft ihm die Tatsachen, die er bekundet, bekannt geworden sind.

6.11 Kontrolle in Polizeidienststelle: TLfDI stellt mangelhaften Datenschutz fest

Öffentliche Stellen, die selbst personenbezogene Daten verarbeiten, haben grundsätzlich die technischen und organisatorischen Maßnahmen zu treffen, um die Ausführung der Bestimmungen des Datenschutzgesetzes zu gewährleisten. Dabei ist unter anderem sicherzustellen, dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit). Unverschlossene und für jeden zugänglich aufbewahrte personenbezogene Daten (in diesem Fall Streifenberichte der Polizei) stellen grundsätzlich einen beanstandungswürdigen Datenschutzverstoß dar. Darüber hinaus war aus datenschutzrechtlicher Sicht klärungsbedürftig, inwieweit die bislang geführten Streifenberichte überhaupt datenschutzrechtlich zulässig sind.

Im Januar 2018 führten zwei Mitarbeiter des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) in einer Thüringer Polizeidienststelle eine datenschutzrechtliche Kontrolle gemäß der §§ 37, 38 des Thüringer Datenschutzgesetz alte Fassung (ThürDSG a. F.) durch. Während der Kontrolle stellten die Mitarbeiter des TLfDI fest, dass sich in der Polizeidienststelle in einem Vorraum der Mitarbeiterräume unverschlossen und für jedermann einsehbare Ordner befanden, in denen ausgefüllte Streifenberichte der vergangenen Jahre abgeheftet waren. In dem Vorraum wurden neben den besagten Ordnern auch Führungs- und Einsatzmittel sowie die Postfächer für die Beamten der Fahndungs- und Ermittlungsgruppe aufbewahrt. Der Raum war während der Regeldienstzeit zugänglich. Die als Formular vorgefertigten Streifenberichte wurden von den Bediensteten während ihrer Schichten ausgefüllt. Darunter befanden sich unter anderem Eingabefelder zum Tag, Datum, zur Dienstschicht (Beginn/Ende), zur Besatzung, zu Maßnahmen & Ergebnisse sowie auf der Rückseite Eingabefelder zu Zeit, Ort, Sachverhalt und Maßnahmen.
Bezüglich der Freifelder auf der Rückseite stellte der TLfDI fest, dass dort fast durchgängig die vollständigen Namen der Fahrzeugführer, deren Geburtsdaten sowie das Fahrzeugkennzeichen aufgeschrieben

wurden. Dies geschah vermeintlich unabhängig davon, ob ein Verstoß festgestellt oder eine Maßnahme durch die Bediensteten der Polizeidienststelle ergriffen wurde. Bei den Daten der Fahrzeugführer handelte es sich um personenbezogene Daten gemäß § 3 Abs. 1 ThürDSG a. F.
Bezüglich des Feldes „Maßnahmen/Ergebnisse“ auf der Vorderseite des Vordrucks war für den TLfDI erkennbar, dass die Bediensteten händisch eine Strichliste führten, wie viele Strafanzeigen und Ordnungswidrigkeiten sie am Einsatztag veranlassten.
Damit war eindeutig und kontrollierbar ersichtlich, wie viele „Maßnahmen/Ergebnisse“ von den jeweiligen Beschäftigten während ihrer Schicht durchgeführt wurden. In Kombination mit der Rückseite des Streifenberichts ergab sich demnach ein detailgetreues Bild, welche Bedienstete an welchem Tag wie viele Fahrzeuge kontrollierten.
Die Aufbewahrung detaillierter Streifenberichte in einem für jeden Bediensteten zugänglichen Raum stellte einen datenschutzrechtlichen Verstoß gegen die technisch- organisatorischen Maßnahmen nach § 9 ThürDSG a. F. dar und wurde gemäß § 39 Abs. 1 ThürDSG a. F. beanstandet. Gemäß § 9 ThürDSG a. F. haben öffentliche Stellen, die selbst personenbezogene Daten verarbeiten, grundsätzlich die technischen und organisatorischen Maßnahmen zu treffen, um die Ausführung der Bestimmungen dieses Gesetzes zu gewährleisten. Dabei ist unter anderem zu gewährleisten, dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit). Die Ordner wurden daraufhin aus diesem Raum entfernt.
Bei einem Ordner war die Aufbewahrungsfrist bereits überschritten. Der TLfDI konnte dazu feststellen, dass hier eine Unachtsamkeit vorlag. In seinem Ermessungsrahmen sah der TLfDI in diesem Fall von einer förmlichen Beanstandung ab. Er wies aber ausdrücklich auf die sorgfältige Prüfung und Einhaltung der einschlägigen Prüf- und Aufbewahrungsfristen hin.
Auf Nachfrage des TLfDI, aus welchem Grund und auf welcher Rechtsgrundlage die Streifenberichte generell geführt wurden, führte die verantwortliche Stelle zunächst aus, dass diese zum Zweck der Einsatzdokumentation der Streifenbesatzung angelegt wurden. Die Datenerhebung erfolgte ihrer Ansicht nach auf Grundlage des § 32 Polizeiaufgabengesetz alte Fassung (PAG a. F.).

Hierzu teilte der TLfDI mit, dass nach § 31 PAG a. F. die Polizei personenbezogene Daten nur erheben kann, soweit dies durch dieses Gesetz oder besondere Rechtsvorschriften über die Datenerhebung der Polizei zugelassen ist.
Nach § 32 PAG a. F. kann die Polizei personenbezogene Daten über die in den §§ 7, 8 und 10 PAG a. F. genannten Personen und über andere Personen erheben, wenn dies erforderlich ist:

- zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten (§ 2 Abs. 1 PAG a. F.),
- zum Schutz privater Rechte (§ 2 Abs. 2 PAG a. F.),
- zur Vollzugshilfe (§ 2 Abs. 3 PAG a. F.) oder
- zur Erfüllung ihr durch andere Rechtsvorschriften übertragenen Aufgaben (§ 2 Abs. 4 PAG a. F.); zudem dürfen §§ 12 bis 47 PAG a. F. die dort aufgeführten Befugnisse der Polizei nicht gesondert regeln.

Die aufgeführte lediglich allgemeine Einsatzdokumentation einer Streifenbesatzung fiel nach Ansicht des TLfDI unter keinen der in § 32 PAG a. F. genannten Fälle. Insofern würde auch § 40 PAG a. F. hinsichtlich der Speicherung der Daten nicht greifen, da dieser voraussetzt, dass die Daten vorher rechtmäßig erlangt wurden, z. B. aufgrund einer gesetzlichen Regelung.
Weiterhin teilte die verantwortliche Stelle in ihrer Stellungnahme dem TLfDI mit, dass auf den Streifenberichten nur die Ergebnisse der jeweiligen Streifenwagenbesatzung erfasst wurden und eine Aufschlüsselung nach einzelnen Beschäftigten nicht möglich wäre.
Hierzu teilte der TLfDI mit, dass die Streifenwagenbesatzung augenscheinlich immer aus je zwei Personen besteht. Diese zwei Personen waren mit Klarnamen auf den Dokumenten mitsamt den von ihnen getätigten Maßnahmen erfasst. Tatsächlich war nicht erkennbar, wer von den zwei Personen welche Maßnahmen getätigt hat. Dennoch ergibt sich ein Gesamtbild, wie viele Maßnahmen insgesamt von den beiden Personen der jeweiligen Streifenwagenbesatzung getätigt wurden, was mögliche Rückschlüsse auf deren Arbeitsweise (Anzahl kontrollierter Fahrzeuge/Fahrzeugführer) zulassen konnte.
Die Namen hätten nach Auffassung des TLfDI grundsätzlich nur dann genannt werden können, wenn dies für die Aufgabenerfüllung der verantwortlichen Stelle erforderlich ist. Denkbar wäre, dass die Beamten namentlich bekannt sein müssen, um gegebenenfalls als Zeugen bei festgestellten Delikten oder Gesetzesverstößen zur Verfügung zu stehen. Dabei stellte sich jedoch die Frage, ob die Streifenberichte die

einzige Dokumentationsmöglichkeit des Einsatzes darstellen. Ist die Dokumentation anderweitig geregelt, so wäre die Angabe der Streifenwagenbesatzung in Klarnamen schwer zu begründen. Weiterhin käme es im vorliegenden Zusammenhang in Betracht, dass möglicherweise Dienstaufsichtsbeschwerden oder disziplinarische Maßnahmen anstehen könnten. Soweit die konkreten Bediensteten hierzu ermittelt werden müssten, wäre ein Rückgriff auf die Streifenberichte möglicherweise zulässig, wenn beispielsweise die Zusammenführung des Einsatzplans mit dem Dienstplan der einzelnen Beschäftigten nicht möglich ist oder nicht zum Erfolg führt.
Die verantwortliche Polizeidienststelle teilte daraufhin mit, dass die Streifenberichte nach Betrachtung aller Gesichtspunkte nicht als einzige Möglichkeit zur Dokumentation des Einsatzes sowie zu nachfolgenden eventuell notwendigen Recherchen in Dienstaufsichts- oder Disziplinarangelegenheiten darstellen würden. Sie seien unter der Prämisse „Streifenberichte hat es schon immer gegeben“ geführt worden. Der TLfDI bat daraufhin das Thüringer Ministerium für Inneres und Kommunales um eine Prüfung, inwieweit das Führen der Streifenlisten mit den darauf zu notierenden Daten bei der Thüringer Polizei generell zulässig und erforderlich ist. Nach einer ersten Bewertung bestanden auch von Seiten des Thüringer Innenministeriums Bedenken gegen die Zulässigkeit und Erforderlichkeit derart konkreter Dokumentationen mit personenbezogenen Daten. Daraufhin bat das Thüringer Innenministerium die Landespolizeidirektion um eine Festlegung einer für alle der Landespolizeidirektion nachgeordneten Behörden geltenden einheitlichen und datenschutzkonformen Verfahrensweise. Das Führen der beschriebenen Strichlisten warf ebenfalls seitens des Innenministeriums Fragen auf. Die vom Thüringer Innenministerium beteiligte Landespolizeidirektion teilte mit, dass der Prüfbericht des TLfDI und die Nachfrage des Innenministeriums dort zum Anlass genommen wurden, die nachgeordneten Behörden zur Erforderlichkeit solcher Berichte an sich zu sensibilisieren und Hinweise an die nachgeordneten Stellen zu geben. Danach ist das Erstellen von Streifenberichten zum Tätigkeitsnachweis der Streifenbesatzung, zur Dokumentation von Wirksamkeiten sowie das Notieren von Personen und Kennzeichen nicht erforderlich, weil hierzu keine Rechtsgrundlage vorliegt und der Tätigkeitsnachweis bereits u. a. auf den Dienstnachweisen abgebildet wird.

6.12 Auskunftspflicht Thüringer Behörden: Voraussetzungen zum Melden von „Selbstverwaltern und Reichsbürgern“ an das Amt für Verfassungsschutz

Öffentliche Einrichtungen des Freistaates Thüringen sind verpflichtet, dem Amt für Verfassungsschutz (AfV) Informationen, die ihnen zu sogenannten Reichsbürgern und Selbstverwaltern bekannt geworden sind, zu übermitteln. Das Übermitteln solcher Informationen ist erforderlich, wenn deren informativer Gehalt relevant für die Erfüllung der Aufgaben des AfV ist. In diesem Zusammenhang kann das Amt für Verfassungsschutz bei öffentlichen Einrichtungen des Freistaates Thüringen auch entsprechende Informationen anfordern, wenn die oben genannten Voraussetzungen dafür gegeben sind. Öffentlichen Einrichtungen haben zudem auch eine Auskunftspflicht gegenüber der Waffenbehörde, soweit dies waffenrechtliche Sachverhalte betrifft und die Daten nicht wegen überwiegender öffentlicher Interessen geheim gehalten werden müssen. Die betreffenden Datenübermittlungen sind datenschutzrechtlich nicht zu bemängeln und werden in ähnlicher Weise auch in anderen Bundesländern praktiziert.

Eine Thüringer Kommune setzte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) davon in Kenntnis, dass das Thüringer Landesverwaltungsamt (TLVwA) von ihr erwarte, dass sie Verdachtsfälle von sogenannten Reichsbürgern und Selbstverwaltern an das Amt für Verfassungsschutz (AfV) melde. Hierzu sollte ein Formblatt verwendet werden auf dem sowohl personenbezogene Daten des Verdächtigen als auch des Meldenden eingetragen und an das Thüringer Landesverwaltungsamt übermittelt werden. Die Kommune bat um Prüfung, ob die von ihr verlangte Vorgehensweise rechtmäßig sei.
Die betreffende Datenübermittlung war vom TLfDI datenschutzrechtlich nicht zu beanstanden, wie sich aus § 21 in Verbindung mit § 20 Abs. 2 Nr. 1 und Nr. 6 des Thüringer Datenschutzgesetzes alte Fassung (ThürDSG a. F) in Verbindung mit §§ 19 und 20 Abs. 1 Thüringer Verfassungsschutzgesetz (ThürVerfSchG) ergab (siehe dazu auch den Beitrag aus dem 12. Tätigkeitsbericht zum Datenschutz, Nr. 6.1, Seite 84 ff.). Das Amt für Verfassungsschutz begründete seine Zuständigkeit mit bestimmten Verhaltensweisen des betroffenen Personen-

kreises, die es als hinreichende tatsächliche Anhaltspunkte für Bestrebungen gegen die freiheitliche demokratische Grundordnung bewertete (§ 4 Abs. 1 S. 1 Nr. 1 ThürVerfSchG).

Insbesondere in Standesämtern, Staatsangehörigkeitsbehörden, Meldebehörden und Pass- und Ausweisbehörden kommt es gelegentlich vor, dass bestimmte Besucher eine fundamental ablehnende Haltung zur Existenz der Bundesrepublik Deutschland äußern und sich dadurch als sogenannte „Reichsbürger" bzw. „Selbstverwalter“ zu erkennen geben.
Die Zulässigkeit der Datenübermittlung zu „Reichsbürgern und Selbstverwaltern“ an das Amt für Verfassungsschutz beim Thüringer Ministerium für Inneres und Kommunales im Freistaat Thüringen ergibt sich aus § 19 Abs. 1 Thüringer Verfassungsschutzgesetz (ThürVerfSchG). Danach haben öffentliche Stellen des Freistaates relevante Informationen dem Amt für Verfassungsschutz zu übermitteln, wenn diese für die Erfüllung der Aufgaben des Amtes für Verfassungsschutz nach § 4 Abs. 1 ThürVerfSchG erforderlich sind.
Ferner teilte der TLfDI der Kommune mit, dass die Kommunen und Landkreise eine Datenübermittlung an die Waffenbehörden auf § 43 Abs. 2 Waffengesetz stützen können. Danach haben Landesbehörden eine Auskunftspflicht gegenüber der Waffenbehörde, soweit dies waffenrechtliche Sachverhalte betrifft und soweit die Daten nicht wegen überwiegender öffentlicher Interessen geheim gehalten werden müssen.

6.13 Mikrozensus in der Justizvollzugsanstalt: Datenschutz für Gemeinschaftsunterkünfte

In Gemeinschaftsunterkünften wird nicht der vollständige Merkmalskatalog für den Mikrozensus erhoben. Die Erhebung ist auf Basisdaten zur Abgrenzung des Wohnstatus in der Gemeinschaftsunterkunft sowie zu Demografie, Staatsangehörigkeit und den Hauptstatus beschränkt.

Im März 2018 wurde eine Anfrage einer Justizvollzugsanstalt (JVA) an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) herangetragen. Im Zusammenhang mit der Erhebung von Daten durch das Thüringer Ministerium für Migration,

Justiz und Verbraucherschutz für eine Repräsentativstatistik über die Bevölkerung und die Arbeitsmarktbeteiligung sowie die Wohnsituation der Haushalte bat man um datenschutzrechtliche Bewertung dieser Angelegenheit.
Demnach wurde die Justizvollzugsanstalt vom Thüringer Landesamt für Statistik gemäß § 13 Mikrozensusgesetz (MZG) um Auskunft zu Untergebrachten aufgefordert.
Im März 2018 war die Datenschutz-Grundverordnung (DS-GVO) zwar in Kraft, aber noch nicht zur Anwendung gekommen, sodass folgende datenschutzrechtliche Situation bestand:
Gemäß § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) war zum damaligen Zeitpunkt die Verarbeitung und Nutzung personenbezogener Daten durch öffentliche Stellen des Freistaates Thüringen dann zulässig, wenn dies eine Rechtsvorschrift erlaubt bzw. anordnet oder soweit der Betroffene eingewilligt hat. Verarbeiten umfasste gemäß § 3 Abs. 3 ThürDSG auch das Übermitteln von personenbezogenen Daten.
Der Mikrozensus ist eine repräsentative Haushaltsbefragung der amtlichen Statistik in Deutschland. Danach werden im Rahmen einer Stichprobe jährlich von einem Prozent der Bevölkerung nach einem konstanten und einem jährlich wechselnden variablen Frageprogramm gemäß §§ 6 bis 9 MZG eine Vielzahl von Daten erhoben. Für den Mikrozensus besteht gemäß § 13 Abs. 1 MZG Auskunftspflicht zu den Erhebungsmerkmalen und Hilfsmerkmalen, sofern nicht die Freiwilligkeit der Auskunftspflicht gemäß § 13 Abs. 7 MZG geregelt ist.
In Gemeinschaftsunterkünften nach § 10 MZG werden Angaben lediglich im beschränkten Umfang zu folgenden Erhebungsmerkmalen erhoben:

- Gemeinde und Gemeindeteil
- Art der Gemeinschaftsunterkunft
- Kalendermonat und Kalenderjahr der Geburt
- Geschlecht
- Familienstand
- Staatsangehörigkeiten
- Nutzung als Haupt- oder Nebenwohnung
- Bestehen einer Wohnung im Ausland
- Hauptstatus

Hilfsmerkmale bei der Erhebung nach § 10 MZG sind dabei Angaben zur Gemeinschaftsunterkunft sowie personenbezogene Daten der Justizvollzugsinsassen:

- Name der Gemeinschaftsunterkunft
- Vor- und Familienname der Leitung der Gemeinschaftsunterkunft
- Kontaktdaten der Leitung der Gemeinschaftsunterkunft
- Vor- und Familienname einer von der Leitung der Gemeinschaftsunterkunft benannten Ansprechperson
- Kontaktdaten der Ansprechperson
- Vor- und Familiennamen der Personen, über die die Auskunft erteilt wird
- Anschrift des Gebäudes
- Baualtersgruppe des Gebäudes

Diese Hilfsmerkmale dienen den Statistikämtern, die Befragung organisiert durchzuführen. Die Angaben zu den Hilfsmerkmalen sind gemäß § 14 MZG von den Angaben zu den Erhebungsmerkmalen unverzüglich zu trennen, nachdem die Überprüfung der Erhebungs- und der Hilfsmerkmale auf ihre Schlüssigkeit und Vollständigkeit abgeschlossen ist; die Angaben zu den Hilfsmerkmalen sind gesondert aufzubewahren. Die Erhebungsunterlagen einschließlich der Hilfsmerkmale sind spätestens nach Abschluss der Aufbereitung der letzten Folgeerhebung zu vernichten oder zu löschen (§ 14 Abs. 3 MZG). In der Begründung zum Gesetzentwurf (DS 18/9418 vom 17. August 2016) zu § 10 (Erhebungsmerkmale in Gemeinschaftsunterkünften) wird darauf verwiesen, dass in Gemeinschaftsunterkünften nicht der vollständige Merkmalskatalog erhoben wird, sondern sich in Gemeinschaftsunterkünften die Erhebung auf Basisdaten zur Abgrenzung des Wohnstatus in der Gemeinschaftsunterkunft sowie zu Demografie, Staatsangehörigkeit und den Hauptstatus beschränkt. In der o. g. Begründung ist zudem die Justizvollzugsanstalt als Einrichtung als eine beispielhafte „Art der Gemeinschaftsunterkunft“ explizit aufgeführt.
Im Ergebnis hat der TLfDI die vom Thüringer Landesamt für Statistik geforderte Datenübermittlung der o. g. Erhebungs- und Hilfsmerkmale über die in der betroffenen JVA gemeldeten Justizvollzugsinsassen gemäß § 4 Abs. 1 ThürDSG in Verbindung mit § 13 MZG für datenschutzrechtlich zulässig angesehen.
Rechtsgrundlage für die Mikrozensusbefragung ist mit Anwendung der DS-GVO zum 25. Mai 2018 Art. 6 Abs. 1 Buchstabe c) in Verbindung mit den Regelungen des Mikrozensusgesetzes.

6.14 Die richterliche Unabhängigkeit – Grenzen des Datenschutzes

Gemäß Art. 55 Abs. 3 der Datenschutz-Grundverordnung (DS-GVO) sind die Datenschutz-Aufsichtsbehörden nicht zuständig für die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen personenbezogener Daten. Die Umsetzung des Thüringer Gesetzgebers erfolgte hierzu in § 9 Abs. 9 des Thüringer Datenschutzgesetzes. Demnach gelten für Gerichte die Bestimmungen des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) als Aufsichtsbehörde, die Bestimmungen zum Datenschutzbeauftragten sowie das Führen von Verzeichnissen zu Verarbeitungstätigkeiten nur, soweit sie in Verwaltungsangelegenheiten tätig werden.

Damit die Unabhängigkeit der Gerichte bei der Ausübung ihrer richterlichen Aufgaben unangetastet bleibt, sollen laut Erwägungsgrund 20 der DS-GVO die Aufsichtsbehörden nicht für die Verarbeitung personenbezogener Daten durch Gerichte im Rahmen ihrer justiziellen Tätigkeit zuständig sein. Art. 55 der DS-GVO normiert diesen Grundsatz mit der Folge, dass die Datenschutz-Aufsichtsbehörden die Gerichte nicht kontrollieren können, wenn diese im Rahmen ihrer richterlichen Tätigkeiten personenbezogene Daten verarbeiten. Das heißt jedoch nicht, dass für die Gerichte die DS-GVO nicht gilt. Auch die Gerichte müssen weiterhin den Datenschutz beachten. Daran hat auch die Anwendbarkeit der DS-GVO nichts geändert. Für Gerichte gelten die Bestimmungen über die Aufsichtsbehörde, die Bestimmung über den Datenschutzbeauftragten sowie die Bestimmungen zum Führen von Verzeichnissen von Verarbeitungstätigkeiten nur in Verwaltungsangelegenheiten.
Was bedeutet das nun für die Gerichte? Diese Frage erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) aus dem Geschäftsbereich der Arbeitsgerichtsbarkeit. Hierzu konnte der Landesdatenschutzbeauftragte mitteilen, dass auch sie in einem ersten Schritt zunächst prüfen müssen, ob und welche Regelungen zu den Datenverarbeitungsvorgängen im Bereich der Arbeitsgerichtsbarkeit vorliegen (Bestandsaufnahme). Ist dieser Schritt erledigt müsse anschließend geprüft werden welche Datenverarbeitungsprozesse anzupassen sind. In einem dritten Schritt steht dann die

Umsetzung dieser Prozesse an. Auch die Gerichte müssen u. a. grundsätzlich den Informationsverpflichtungen der Art. 13 und 14 der DS-GVO nachkommen. Ein lediglich allgemeiner Aushang mit den Informationen der Art. 13 und 14 der DS-GVO entspricht, nach Auffassung des TLfDI, grundsätzlich nicht den Anforderungen aus Art. 12 der DS-GVO. Gemäß Art. 12 der DS-GVO sind die Informationen in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ zu übermitteln. Diese Voraussetzungen sind beispielsweise nicht erfüllt, wenn die betroffene Person einen Brief erhält und dann das Schwarze Brett im Gericht aufsuchen muss, um die Informationen nach Art. 13 oder 14 der DS-GVO zu erhalten.
Die Informationspflichten bürden den verantwortlichen Stellen in der praktischen Umsetzung einen größeren Verwaltungsaufwand auf. Sie sind aber unerlässlich um den betroffenen Personen Klarheit darüber zu verschaffen, was mit ihren personenbezogenen Daten geschieht.

6.15 Braucht der Personalrat einen eigenen Datenschutzbeauftragten?

Die Personalvertretung einer Dienststelle fällt unter den Begriff des Verantwortlichen im Sinne von Art. 4 Nr. 7 der Datenschutz-Grundverordnung. Infolgedessen hat die Personalvertretung auch einen eigenen Datenschutzbeauftragten zu bestellen.

Im Zuge der Umsetzung der Datenschutz-Grundverordnung (DS-GVO) stellen sich dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) derzeit viele spannende datenschutzrechtliche Fragen. So zum Beispiel die Frage, ob die Personalvertretung einer Dienststelle einen eigenen Datenschutzbeauftragten bestellen muss.
Der TLfDI vertritt hierzu, wie auch einige andere Landesdatenschutzbeauftragte, die Rechtsaufassung, dass die Personalvertretung einer Dienststelle unter den Begriff des Verantwortlichen im Sinne von Art. 4 Nr. 7 DS-GVO fällt. Verantwortlicher ist demnach die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. In der

Regel werden die Mittel für die Aufgabenerfüllung durch den Personalrat selbst bestimmt. So entscheidet er beispielsweise wie er Mitarbeiterdaten verwaltet, die ihm zur Prüfung vorgelegt werden.
Folglich hat die Personalvertretung auch einen eigenen Datenschutzbeauftragten zu bestellen.
Es sollte die gesetzliche Möglichkeit eingeräumt werden, dass der behördliche Datenschutzbeauftragte der Dienststelle in Personalunion auch das Amt des Datenschutzbeauftragten der Personalvertretung übernimmt, wenn dazu Einvernehmen zwischen Dienststelle und Personalvertretung besteht. Der Personalvertretung würden somit keine übermäßig rechtlichen oder tatsächlichen Hürden bei der Besetzung des Amtes ihres eigenen Datenschutzbeauftragten auferlegt werden.
Der TLfDI unterbreitete deshalb im Rahmen der Anhörung zur Änderung des Thüringer Gesetzes zur Anpassung personalvertretungsrechtlicher Vorschriften (Gesetzentwurf der Landesregierung – Drs. 6/5575 –) folgenden Änderungsvorschlag zum Personalvertretungsgesetz:

§ 80 Abs. 1 erhält folgende Fassung:
(1) Die Personalvertretung hat als Verantwortlicher die Vorschriften über den Datenschutz einzuhalten. Sie hat dazu einen Datenschutzbeauftragten zu bestellen; Personalvertretung und Dienststelle können im Einvernehmen einen gemeinsamen Datenschutzbeauftragten bestellen.

Inwieweit die Ergänzung des TLfDI im Gesetzgebungsverfahren angenommen wird, bleibt abzuwarten.

6.16 Beschwerde über Internatsmitarbeiterin wegen Weitergabe dienstlicher Informationen

Bei Anhörungen im Rahmen einer Dienstaufsichtsbeschwerde kommen regelmäßig auch personenbezogene Daten Dritter zur Sprache. Angehörige, Rechtsanwälte oder Gewerkschaftssekretäre der betroffenen Tarifbeschäftigten können als deren Bevollmächtigte an einer solchen Anhörung teilnehmen, wenn die Aufnahme nachteiliger Beschwerden oder Behauptungen in die Personalakte des Betroffenen beabsichtigt ist. In diesem Fall muss die Behörde den Bevollmächtig-

ten vor der Offenbarung von personenbezogenen Daten Dritter ausdrücklich darüber belehren, dass er zur Verschwiegenheit bezüglich dieser Daten verpflichtet ist.

Die Eltern eines Schülers (Beschwerdeführer) beschwerten sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über eine Mitarbeiterin des kommunalen Schulinternates ihres Sohnes (Mitarbeiterin).
Dem vorangegangen war eine Dienstaufsichtsbeschwerde der Beschwerdeführer über die Mitarbeiterin. Daraufhin gab die Dienstaufsichtsbehörde der Mitarbeiterin und deren Ehemann Gelegenheit zu einem Anhörungsgespräch zu der Dienstaufsichtsbeschwerde.
Nachfolgend zeigte die Mitarbeiterin die Beschwerdeführer als Reaktion auf deren Dienstaufsichtsbeschwerde wegen Verleumdung an. Gleichzeitig schrieb der Ehemann der Mitarbeiterin, der infolge der Teilnahme am Anhörungsgespräch Kenntnis von der Angelegenheit erlangt hatte, einen Brief an die Beschwerdeführer.
Der TLfDI bat die für das Internat zuständige Behörde um Bestätigung des geschilderten Sachverhalts. Der TLfDI teilte der Behörde mit, dass es sich bei der Datenübermittlung an die Staatsanwaltschaft und der Offenbarung dienstlicher personenbezogener Daten gegenüber dem Ehemann der Mitarbeiterin um Verstöße gegen datenschutzrechtliche Vorschriften handeln könne. Zugleich forderte er die Behörde auf, mitzuteilen, auf welchen Rechtsgrundlagen die o. g. Datenübermittlungen erfolgten und inwieweit diese erforderlich gewesen seien.
Nachfolgend bestätigte die Behörde den Ablauf des Geschehens. Die Behörde setzte den TLfDI darüber in Kenntnis, dass sie das Hinzuziehen des Ehemanns der Mitarbeiterin zur Anhörung „ als Vertrauensperson und Beistand“ seiner Ehefrau bewilligt habe.
Daraufhin entgegnete der TLfDI, dass eine Hinzuziehung des Ehemanns nur zulässig sei, wenn bei dem Gespräch eine Aufnahme von für die angestellte Mitarbeiterin nachteiligen „Beschwerden und Behauptungen tatsächlicher Art“ in ihre Personalakte beabsichtigt gewesen sei. Auch müsse die Behörde dafür sorgen, dass der Bevollmächtigte nicht in Eigeninitiative ein Schreiben an die Eltern verfasst. Ein solches Vorgehen sei in keinem Fall von einer Bevollmächtigung gemäß § 3 Abs. 5 Tarifvertrag für den öffentlichen Dienst gedeckt.
Hierauf teilte die Behörde mit, dass sie eine Aufnahme der Dienstaufsichtsbeschwerde in die Personalakte der Mitarbeiterin beabsichtige.

Die Behörde räumte ein, dass ein bevollmächtigter Dritter auf die Vertraulichkeit und Verschwiegenheit hätte hingewiesen werden müssen. Allerdings sei während des Gesprächs nicht erkennbar gewesen, dass der Ehemann über eine moralische Unterstützung hinaus selbst aktiv werden würde.
Der TLfDI stellte gegenüber der Behörde fest, dass, soweit im Rahmen des Gespräches personenbezogene Daten (insbesondere Name des Sohnes bzw. dessen Eltern oder Namen von anderen Schülern) an den anwesenden Ehemann der beteiligen Internatsmitarbeiterin bekanntgegeben wurden, es sich um einen datenschutzrechtlichen Verstoß in Form einer unzulässigen Weitergabe personenbezogener Daten handelt. Als milderes Mittel wäre beispielsweise eine pseudonymisierte Besprechung des Sachverhaltes ausreichend gewesen.
In diesem Zusammenhang belehrte der TLfDI die Behörde darüber, dass nach § 7 Thüringer Datenschutzgesetz (ThürDSG) in Verbindung mit Art. 58 Abs. 1 Buchstabe a) Datenschutz-Grundverordnung (DS-GVO) die der Kontrolle des TLfDI unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte zu erteilen haben und dass die Aufsichtsbehörde nach fristlosem Ablauf eine behördliche Anweisung nach Art. 58 Abs. 1 Buchstabe a) DS-GVO erlassen könne.
Die Behörde teilte auf Verlangen des TLfDI mit, dass sie bei dem betreffenden Gespräch dem bevollmächtigen Ehemann tatsächlich personenbezogene Daten der Beschwerdeführer, ihres Sohnes bzw. von anderen Personen bekannt gegeben habe. Jedoch sei eine ausdrückliche Belehrung des bevollmächtigten Ehemannes zur Verschwiegenheitspflicht unterblieben.
Abschließend stellte der TLfDI gegenüber der Behörde fest, dass es sich bei der Weitergabe personenbezogener Daten an Dritte in der beschwerdegegenständlichen Angelegenheit um einen Verstoß gegen datenschutzrechtliche Vorschriften nach § 22 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) alter Fassung handelte. Da das ThürDSG in seiner alten Fassung jedoch mit Bekanntgabe der DS-GVO am 25. Mai 2018 seine Gültigkeit verloren hatte, konnte der TLfDI eine Beanstandung der Vorgehensweise der Behörde nicht mehr aussprechen. Der TLfDI sah daher das Verfahren als abgeschlossen an.
Vorsorglich wies der TLfDI die Behörde noch darauf hin, dass der Vorfall nach dem neuem Recht der DS-GVO eine Verwarnung nach Art. 58 Abs. 2 DS-GVO nach sich gezogen hätte.

6.17 Der lachende Dritte? Mangelhafter Datenschutz in Führerscheinstelle

Die Beschwerde eines Bürgers betraf datenschutzrechtliche Mängel in einer Führerschein- und Zulassungsstelle eines Landkreises. Die dortige Bearbeitung personenbezogener Daten in Anwesenheit unberechtigter Dritter stellte einen Verstoß gegen datenschutzrechtliche Regelungen dar. In einem solchen Fall hat die verantwortliche Stelle umgehend geeignete technisch-organisatorische Maßnahmen, etwa bauliche Veränderungen, zu veranlassen, um eine unberechtigte Kenntnisnahme von personenbezogenen Daten künftig auszuschließen.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt einen Hinweis zu technisch-organisatorischen Mängeln in der Führerschein- und Zulassungsstelle eines Landkreises. Demnach würden in einem Büro dieser Zulassungsstelle zwei Mitarbeiter die Anliegen von zwei anwesenden Bürgern parallel bearbeiten. Die Antragsteller, die somit unmittelbar nebeneinandersitzen, könnten auf diese Weise die Unterlagen des jeweils anderen einsehen und die entsprechenden Gespräche mitverfolgen.
Da bei der Bearbeitung der Anträge Dritten personenbezogene Daten (wie z. B. Daten beim Kraftfahrt-Bundesamt) offenbart werden, verlangte der TLfDI von der betreffenden Zulassungsstelle eine Stellungnahme zum Sachverhalt. Zudem bat der TLfDI um Darlegung, auf welche Weise die technisch-organisatorischen Maßnahmen gemäß § 9 Thüringer Datenschutzgesetz (ThürDSG) in der Führerscheinstelle umgesetzt werden können.
Daraufhin teilte das Landratsamt dem TLfDI mit, dass das betreffende Büro durch Trennwände geteilt werden solle, um eine visuelle Kenntnisnahme der Unterlagen anderer Antragssteller künftig auszuschließen. Nachdem die hierfür erforderlichen Vermessungen bereits durchgeführt worden seien, wurde laut Zulassungsstelle eine geeignete Firma mit der Bauausführung beauftragt.
Zugleich wies die betreffende Zulassungsstelle auf die bisherige Praxis hin, dem Bürger nonverbal am PC-Monitor bestimmte Auskünfte durch Eindrehen des PC-Monitors zu visualisieren. Aufgrund der Beschwerde habe das Landratsamt veranlasst, im Regelfall die Anliegen vorsprechender Bürger ohne die Anwesenheit Dritter zu bearbeiten.

Sollte jedoch, etwa zu Stoßzeiten, eine beschleunigte Bearbeitung nötig sein, werde man, nach Eintreten eines zweiten Antragsstellers in das Büro, beide Antragsteller auffordern, ihr Einverständnis in eine gleichzeitige Bearbeitung ihrer Anliegen im gleichen Büro bzw. bei geöffneter Tür zum Nachbarbüro zu geben. Wird ein solches Einverständnis nicht erteilt oder ist eine Ablehnung zu erwarten aufgrund der besonders sensiblen Daten (Vermögensstand, Erkrankungen, besondere Problemlagen), die besprochen werden sollen, werde man dem Betroffenen anbieten, solange zu warten, bis sein Anliegen separat bearbeitet werden könne.
Um jedoch die Sicherheit der Bediensteten bei unbeherrschten aggressiven Bürgern zu gewährleisten, werde man auch weiterhin an einer doppelten Personal-Besetzung der Büros bzw. an der geöffneten Zimmertür zum Nachbarbüro festhalten.
Die betreffende Stelle kündigte an, die Mitarbeiter der Führerschein- und Zulassungsstelle auf den oben genannten, geänderten Verfahrensablauf hinzuweisen.
Der TLfDI teilte dem Verantwortlichen abschließend mit, dass er aufgrund der mitgeteilten Maßnahmen die Angelegenheit als abgeschlossen ansehe.

6.18 Datenschutz bei der Einbürgerung: Dürfen Antragsteller die Angabe ihrer Daten verweigern?

Eine Einwilligung in die Verarbeitung personenbezogener Daten liefert in besonderen Fällen keine gültige Rechtsgrundlage. Dies ergibt sich aus dem Erwägungsgrund 43 der Datenschutz-Grundverordnung (DS-GVO), wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere dann, wenn es sich bei dem Verantwortlichen um eine Behörde handelt und es deshalb eventuell unwahrscheinlich ist, dass eine Einwilligung freiwillig gegeben wurde.

Nach Wirksamwerden der DS-GVO zum 25. Mai 2018 beschäftigte das Amt für Migration folgendes Problem: Von Antragstellern würden beispielsweise seitens des Amtes für Migration bei der Antragstellung auf Einbürgerung bestimmte Daten benötigt (z. B. Personalien, Lebenslauf, Einkommensverhältnisse etc.). Aus Sicht des Amtes für

Migration läge hier aber keine gesetzliche Verpflichtung des Antragstellers vor, diese Daten gegenüber der Einbürgerungsbehörde offenzulegen. Zudem sei davon auszugehen, dass der Einbürgerungsbewerber die zur Antragsbearbeitung benötigten Daten mitteilen werde, da er ein Interesse am Einbürgerungsverfahren habe.
In dieser Hinsicht sah es das Amt für Migration kritisch, dass der Einbürgerungsbewerber seine Einwilligung zur Verarbeitung der Daten widerrufen könnte und damit nach Meinung des Amtes die entsprechenden Daten zu löschen seien. Im Widerspruch dazu gäbe es aber in Thüringen eine Richtlinie zur Aufbewahrung von Schriftgut, nach der komplette Einbürgerungsvorgänge dauerhaft aufzubewahren seien.
Der Bitte des Amtes für Migration um Hinweise zur datenschutzrechtlichen Verfahrensweise kam der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) mit folgenden Informationen nach:
Gemäß Europäischer Datenschutz-Grundverordnung ist eine Verarbeitung rechtmäßig, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat (Art. 6 Abs. 1 Buchstabe a) DS-GVO). Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche gemäß Art. 7 Abs. 1 DS-GVO nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat. Um sicherzustellen, dass die Einwilligung freiwillig erfolgt ist, liefert aber die Einwilligung in besonderen Fällen, in denen zwischen betroffener Person und Verantwortlichen ein klares Ungleichgewicht besteht, keine gültige Rechtsgrundlage (Erwägungsgrund 43 der DS-GVO). Das trifft insbesondere dann zu, wenn es sich bei dem Verantwortlichen um eine Behörde handelt und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde. Weil in Folge die Rechtmäßigkeit der oben genannten Verarbeitung nach Einschätzung des TLfDI ohnehin nicht auf die Einwilligung gestützt werden kann, stellt sich das geschilderte Problem des Widerrufs der Einwilligung nicht. Unabhängig davon finden sich in der Kommentarliteratur (Kühling/Buchner, DS-GVO/BDSG Kommentar, 2018, Art. 7, Rdnr. 37) auch Hinweise auf eine Einschränkung dieses Widerrufs und zwar dann, wenn die weitere Speicherung der Daten z. B. zur Geltendmachung und Verteidigung von Rechtsansprüchen, aber auch für im öffentlichen Interesse liegende Archivzwecke erforderlich ist.

Der TLfDI hat dem Amt abschließend mitgeteilt, dass im Bereich der Einbürgerungsverfahren zur Aufgabenerfüllung spezialgesetzliche Regelungen (§§ 30 ff. Staatsangehörigkeitsgesetz) zur Anwendung kommen, die eine Verarbeitung der personenbezogenen Daten der Einbürgerungsbewerber, unabhängig von einer Einwilligung, erlauben.

6.19 Wahlwerbung: Wann Parteien Melderegisterauskünfte einholen dürfen und was man dagegen tun kann

Es ist datenschutzrechtlich nicht zu beanstanden, dass die Meldebehörde gemäß Art. 6 Abs. 1 Buchstabe e) DS-GVO in Verbindung mit § 50 Abs. 1 Bundesmeldegesetz (BMG) im Zusammenhang mit Wahlen den Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen Auskunft aus dem Melderegister über die in § 44 Abs. 1 Satz 1 BMG bezeichneten Daten (einfache Melderegisterauskunft) von Gruppen von Wahlberechtigten – auch von der Gruppe der Jungwähler – erteilt.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) empfiehlt allen wahlberechtigten Bürgern, die eine solche Auskunft nicht wünschen, ihr Recht gemäß § 50 Abs. 5 BMG und damit ihre Widerspruchsmöglichkeit gegen diese Datenübermittlung wahrzunehmen.

Ein empörter Vater teilte dem TLfDI mit, dass seine minderjährige Tochter persönliche Post von einem Oberbürgermeisterkandidaten bekommen habe. Nun stelle er sich die Frage, wie die Partei an die Daten seiner Tochter gekommen sei und ob die Meldebehörde der Stadt Erfurt ohne sein Einverständnis personenbezogene Daten an Parteien oder Kandidaten herausgäbe. Er bat den TLfDI zu prüfen, ob hier nicht ein klarer Verstoß gegen das Datenschutzgesetz vorläge.
Zur Zeit der Anfrage war die Europäische Datenschutz-Grundverordnung in Kraft, aber noch nicht zur Anwendung gekommen, sodass der TLfDI den Beschwerdeführer wie folgt informierte:
Dem TLfDI obliegt die Kontrolle der Thüringer Meldebehörden. Diese dürfen nur innerhalb des gesetzlich vorgegebenen Rahmens die personenbezogenen Daten der Betroffenen verarbeiten. Das Verarbeiten umfasst dabei gemäß § 3 Abs. 4 des Thüringer Datenschutzgesetzes auch das Übermitteln und Nutzen der personenbezogenen Daten.

Nach § 50 Abs. 1 BMG darf die Meldebehörde Parteien und anderen Trägern von Wahlvorschlägen bis zu sechs Monaten vor einer Wahl oder Abstimmung auf staatlicher und kommunaler Ebene Auskunft aus dem Melderegister über die in § 44 Abs. 1 Satz 1 BMG bezeichneten Daten (Familienname, Vornamen, Doktorgrad und derzeitige Anschriften) von wahlberechtigten Gruppen erteilen.
Die Wahlberechtigung für Kommunalwahlen beginnt nach dem Thüringer Kommunalwahlgesetz mit der Vollendung des 16. Lebensjahres. Zulässig sind demnach auch Auskünfte über alle am Wahltag z. B. 16- bis 22-jährigen Wähler („Jungwählerlisten“). Die den Wahlvorschlagsträgern übermittelten Daten unterliegen dabei einer strengen Zweckbindung. Sie dürfen nur zum Zweck der Wahlwerbung verwendet werden und sind spätestens einen Monat nach der Wahl zu löschen oder zu vernichten (§ 50 Abs. 1 Satz 3 BMG).
Im vorliegenden Fall hatte die Tochter als Betroffene allerdings das Recht, gemäß § 50 Abs. 5 BMG dieser Übermittlung der Daten (für zukünftige Fälle) zu widersprechen. Die Meldebehörde hat die Pflicht, bei der Anmeldung eines Wohnungsbezugs sowie einmal jährlich durch ortsübliche Bekanntmachung, z. B. im Amtsblatt, auf dieses Widerspruchsrecht hinzuweisen. Der TLfDI hat zudem auf seiner Internetseite ein entsprechendes Formblatt „Widerspruch gegen Datenübermittlung aus dem Melderegister“ (www.tlfdi.de/mam/tlfdi/info/anlage_widerspruch_gegen_datenuebermittlung.pdf) zur Verfügung gestellt. Da die 16- und 17-Jährigen für die Thüringer Kommunalwahlen wahlberechtigt sind, kann auch davon ausgegangen werden, dass sie die erforderliche Einsichtsfähigkeit zu der weniger weitreichenden Entscheidung darüber besitzen, ob sie der Weitergabe ihrer Daten zu Zwecken der Wahlwerbung widersprechen wollen.
Die Übermittlung der Adress-Daten der Tochter durch das Meldeamt an den Oberbürgermeisterkandidaten hat der TLfDI im Ergebnis für datenschutzrechtlich zulässig angesehen.

Ergänzung:
Mit Anwendung der DS-GVO darf die Meldebehörde die o. g. Auskunft gemäß Art. 6 Abs. 1 Buchstabe e) der DS-GVO in Verbindung

mit § 50 Abs. 1 BMG erteilen; am o. g Widerspruchsrecht gemäß § 50 Abs. 5 BMG hat sich nichts geändert.

6.20 Datenerhebung für Mikrozensus: …und jährlich grüßt das Statistische Bundesamt?

Private Haushalte werden für eine Mikrozensus-Befragung zufällig und nach mathematisch-statistischen Regeln für die Mikrozensus-Befragung ausgewählt. Wenn es der Zufall will, können private Haushalte wiederholt betroffen sein, die bei früheren Befragungen bereits ausgewählt wurden.

Ein Beschwerdeführer wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er beschwerte sich beim TLfDI darüber, dass er vom Thüringer Landesamt für Statistik (TLS) eine Aufforderung zur Mikrozensusbefragung für 2018 erhalten habe, er aber bereits seit 2010 und in den Folgejahren als Auskunftspflichtiger in die Haushaltsbefragung einbezogen worden sei. Zudem sei ihm auch bewusst, dass private Haushalte für die Mikrozensus-Befragung grundsätzlich zufällig und nach mathematisch-statistischen Regeln ausgewählt werden. Eine erneute Einbeziehung in den Mikrozensus 2018 fände der Betroffene aber zumindest „komisch“ und ziehe die Möglichkeit in Erwägung, dass seine personenbezogenen Auswahl-Daten der letzten Befragung nicht gelöscht, sondern im Mikrozensus 2018 erneut verwendet werden können. Der Beschwerdeführer sah sich in seiner Haltung bestätigt, da nach seiner Kenntnis nicht nur er, sondern auch benachbarte Haushalte wiederholt in die Haushaltsbefragung einbezogen worden seien.
Er bat den TLfDI um Überprüfung der Angelegenheit.
Nach Stellungnahme des TLS hat der TLfDI den Beschwerdeführer wie folgt informiert:
Die Adresse des Beschwerdeführers war in den Jahren 2007 bis 2010 im Rahmen des Mikrozensus auskunftspflichtig. Durch das für die Stichprobenziehung zuständige Statistische Bundesamt wurde diese Adresse ab 2016 zudem und wiederum in die ab 2018 geltende Stichprobe zum Mikrozensus einbezogen. Der Mikrozensus läuft dabei nach Angaben des TLS wie folgt ab: Die Auswahlgrundlage des Mik-

rozensus beruht auf einem stichprobenartigen, einstufigen Grundkonzept, das zu einer sogenannten „Klumpen-Stichprobe“ führt. Klumpen stehen dabei für Auswahleinheiten bzw. künstlich abgegrenzte Flächen (Auswahlbezirke), die sich aus ganzen Gebäuden oder Gebäudeteilen zusammensetzen. In der sogenannten Anschriftengrößenklasse 1 (Gebäude mit 1 bis 4 Wohnungen) werden die Klumpen zusammenfassend in der Reihenfolge mehrerer Hausnummern, auch straßenübergreifend gebildet. Bis einschließlich 2015 basierte die Stichprobe für die neuen Bundesländer auf Grundlage des Bevölkerungsregisters „Statistik". Dazu wurden die Angaben aus dem Zentralen Einwohnerregister der ehemaligen DDR bezüglich der Zahl der Personen und der Zahl der Familienhaushalte pro Hausnummer verdichtet. Bestandteil dieser Stichprobe war in den Jahren 2007 bis 2010 die Anschrift des Beschwerdeführers.
Mit dem Zensus 2011 liegt eine neue Auswahlgrundlage für Bevölkerungsstichproben vor. Seit 2011 wird die Auswahlgrundlage und die hierfür zulässigen Merkmale für Gebäude-, Wohnungs- und Bevölkerungsstichproben nach § 23 des Zensusgesetzes geregelt. Die Bildung von Auswahlbezirken und die Ziehung von maximal 20 Vorratsstichproben erfolgte noch nach demselben früheren stichprobenmethodischen Grundkonzept und muss spätestens vier Jahre nach dem Zensusstichtag 9. Mai 2011 erfolgt sein, da die verarbeiteten Datensätze nach Ablauf des Zensusstichtags gelöscht werden müssen. Vor diesem Hintergrund mussten die Vorratsstichproben der Grundauswahl für den Mikrozensus spätestens bis zum 9. Mai 2015 gezogen werden. Dieser aktuelle Auswahlplan ist 2016 in Kraft getreten und beinhaltet wiederum alle bewohnbaren Flächen – unabhängig davon, ob diese bereits in den Vorjahren befragt wurden. Da sich mit der neuen Zufallsstichprobe ab dem Jahr 2016 auch der Zuschnitt der Auswahlbezirke verändert hat, kann es vorkommen, dass eine bis einschließlich 2015 im Auswahlplan vorhandene Wohnung ab 2016 erneut in die Stichprobe gelangt, wie im Fall des Beschwerdeführers. Dies wird vom Gesetzgeber auch nicht ausgeschlossen, sondern es wird im Mikrozensusgesetz 2005 lediglich auf die höchstens viermalige Befragung innerhalb von fünf aufeinanderfolgenden Jahren verwiesen. Die Vorratsstichproben wurden zentral im Statistischen Bundesamt für alle Bundesländer gezogen. Die gezogenen Vorratsstichproben wurden nach der Ziehung aufgeteilt und den Statistischen Landesämtern zur Verfügung gestellt. Der Gesetzgeber und das stichprobenmethodi-

sche Grundkonzept lassen es somit zu, dass eine bis einschließlich 2015 im Auswahlplan vorhandene Wohnung ab 2016 erneut in die Stichprobe gelangt und dass Auswahlbezirke aus Zusammenfassungen von Hausnummern der gleichen Straße bestehen können. Eine Zuordnung der Erhebungsmerkmale zu Personen und Anschriften ist nach dem Grundsatz der Trennung, der gesonderten Aufbewahrung und Löschung gemäß § 14 Mikrozensusgesetz und § 12 Bundesstatistikgesetz nicht möglich.
Das TLS hat zudem versichert, dass nur die anonymisierten Angaben für die Ergebniserstellung verwendet und alle Erhebungsunterlagen nach Abschluss der Aufbereitung der letzten Erhebung vernichtet werden.
Da ohne Zweifel die Datenerhebungen im Zusammenhang mit dem Mikrozensus einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen darstellen, ist der zu erhebende Datenumfang nicht von einer Behörde, sondern vom Gesetzgeber selbst in §§ 6 ff. Mikrozensusgesetz festgelegt. Diese Angaben unterfallen besonderen Geheimhaltungsvorschriften, dem Statistikgeheimnis und dürfen nicht personenbezogen ausgewertet oder der Verwaltung z. B. für Datenabgleiche zur Verfügung gestellt werden. Das TLS hat im vorliegenden Fall aber plausibel dargelegt, dass durch veränderte mathematische Auswahlverfahren die wiederholte Einbeziehung von Haushalten in die Stichproben möglich ist.
Der TLfDI konnte in Folge keinen Datenschutzverstoß erkennen.

6.21 Auftragsverarbeitungsvertrag: Einer für alle?

Eine Fachaufsichtsbehörde kann einen Auftrag zur Datenverarbeitung auch mit Wirkung für die ihr untergeordneten Stellen des Landes erteilen.

Eine Auftragsdatenverarbeitung liegt immer dann vor, wenn eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Nr. 8 der Datenschutz-Grundverordnung [DS-GVO]).
An den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde mit der Umsetzung der Datenschutz-Grundverordnung die Frage herangetragen, ob nun nach

neuem Recht jede einzelne Behörde im Rahmen einer Auftragsdatenverarbeitung immer selbst einen Vertrag zur Verarbeitung von Auftragsdaten mit dem Thüringer Landesrechenzentrum abschließen muss.
Der TLfDI konnte in diesem Fall auf die gesetzliche Regelung zur Auftragsdatenverarbeitung verweisen. Diese war im alten Thüringer Datenschutzgesetz in § 8 Abs. 2 Satz 5 Thüringer Datenschutzgesetz - alt- (ThürDSG -alt-) geregelt. Im Zuge der Anpassung des Thüringer Datenschutzgesetzes an die Datenschutz-Grundverordnung fand sich die entsprechende Regelung nunmehr unter „neuer Hausnummer“ in § 19 Abs. 2 ThürDSG wieder.
Die Regelung des § 19 Abs. 2 Thüringer Datenschutzgesetz (ThürDSG) lautet: „Der Auftrag kann auch durch die Fachaufsichtsbehörde mit Wirkung für ihre Aufsicht unterliegenden Stellen des Landes erteilt werden; diese sind von der Auftragserteilung zu unterrichten“.
Somit ist es weiterhin möglich, dass eine zuständige Fachaufsichtsbehörde einen Auftrag zur Datenverarbeitung mit einem Auftragnehmer schließen kann, der Wirkung auf die ihrer Aufsicht unterliegenden Stellen hat.

6.22 Schulverwaltung Spezial: Bildung für die digitale Welt - Der Weg ins neue Zeitalter

Im Februar 2018 erreichte den TLfDI eine Anfrage der bundesweit erscheinenden Fachzeitschrift „SchulVerwaltung“ für Schulleitungen und Schulverwaltungen. Der Bitte entsprechend erläutert der TLfDI in einem ausführlichen Artikel für eine Sonderausgabe dieser Zeitschrift, welche medienpädagogischen und datenschutzrechtlichen Herausforderungen auf Lehrerbildung und Schulen im Kontext von Digitalisierung und Datenschutz- Grundverordnung zukommen.

Dass die engagierten Bemühungen des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um die Medienbildung für Schülerinnen und Schüler Beachtung finden, beweist eine Anfrage der Herausgeber der Zeitschrift „SchulVerwaltung“ vom Frühjahr 2018. Beabsichtigt war eine Sonderausgabe dieser Fachzeitschrift für Schulentwicklung und Schulmanagement, die bundesweit

monatlich erscheint und sowohl Schulen als auch Schulaufsicht erreicht. Inhaltlich solle sich diese Sonderausgabe den heutigen Herausforderungen für Schulen in einer zunehmend digitalisierten Gesellschaft widmen und den Stellenwert entsprechender Bildungsangebote beleuchten. Der TLfDI wurde hier in seiner Rolle als Vorsitzender des Arbeitskreises „Datenschutz und Bildung“ der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder um einen entsprechenden Beitrag gebeten. Seit April 2018 heißt der Arbeitskreis „Datenschutz-/Medienkompetenz“
Im mehrseitigen Artikel „Schule und Datenschutz – Wie machen wir das passend?“ weist schon der Titel darauf hin, dass es hier noch viel zu tun gibt im Hinblick auf die Passfähigkeit der beiden Kategorien. Datenschutz ist oft negativ besetzt. Schulen sind Teil unserer Gesellschaftsstruktur, ihre Akteure machen sicher im Durchschnitt keine Ausnahme, was ihre Einstellungen zu Datenschutzfragen anbelangt. Bei der Sensibilisierung von Lehrkräften anzusetzen und über Weichenstellungen in der Lehrerbildung die Sichtweisen von Lehrkräften auf den Privatsphärenschutz zu schärfen, ist ein wichtiges Gebot der Stunde. Es gilt, Selbstkompetenz zu entwickeln, die auf die Kompetenzen ihrer Schülerinnen und Schüler durchzuschlagen vermag. Gegenwärtige Ausbildungscurricula für die Hochschulen haben allerdings diesbezüglich noch viel Luft nach oben.
Die Lehrerausbildung ist nicht die einzige Herausforderung, um Schülerinnen und Schüler fit zu machen für ihr Leben in der Welt von morgen. Die Individualisierung des Lernens mit digitalen Werkzeugen steht zu Recht hoch im Kurs. Die Materialien dafür stecken in der Wolke, statt im Schulrucksack. Schul-Cloud für alle ist ein vereinbartes Koalitionsziel der jetzigen Bundesregierung. Dass dabei eine Unmenge lern- und schülerbezogener Daten verarbeitet werden müssen, ist unerlässlich. Alles wunderbar, solange diese Daten in der Schule bleiben und niemals in Form detaillierter Schülerprofile Grundlage von „InApp-Verkäufen“ der Lernmittelanbieter werden können. Der Hunger nach verwertbaren Daten ist bekanntlich eine starke Triebkraft im 21. Jahrhundert, die auch die Schultür eindrücken will. Da gilt es schon bei der Entwicklung entsprechender Softwarelösungen genau hinzuschauen, ob die Datenverarbeitung hier immer rechtskonform gewährleistet ist. „Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz“ postuliert die Datenschutz-Grundverordnung (DS-GVO) im Erwägungsgrund 38.

Apropos DS-GVO, der TLfDI stellte in besagtem Artikel klar, dass sich mit der Datenschutz-Grundverordnung alte und neue Pflichten für die Schulen und Schulträger ergeben. Neu ist beispielweise die Erweiterung der Betroffenenrechte, z. B. die umfangreiche Informationspflicht der Schule, wenn sie Daten bei Eltern und Schülern erhebt. Hinzu kommt, dass staatliche Schulen als öffentliche Stellen einen behördlichen Datenschutzbeauftragten benennen müssen. Der ist unter anderem dann gefordert, wenn die neuen Anforderungen an einen Auftragsverarbeiter, z. B. für das Verwalten der Schul-Cloud (siehe oben), umgesetzt werden müssen. Klare Botschaft: Die DS-GVO erfordert auch Lernen von Schule und Schulverwaltung.
Der ausführliche Artikel des TLfDI ist in der Ausgabe SchulVerwaltung Spezial, Ausgabe 4/2018, erschienen.

6.23 „Bildungslücke“ im Datenschutz: Stärkung der Kommunikation zwischen Berufsschule und Ausbildungsstätte

Noten und Zeugnisse sind personenbezogenen Daten, die von einer Berufsschule an einen Ausbildungsbetrieb nur auf Grundlage einer Rechtsvorschrift übermittelt werden dürfen. Eine Einwilligung der betroffenen Auszubildenden kommt wegen fehlender Freiwilligkeit aufgrund des bestehenden Unter- und Überordnungsverhältnisses gegenüber der Schule und dem Ausbildungsbetrieb nicht in Betracht.

An den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde die Frage herangetragen, ob die berufsbildenden Schulen auf Anfrage der Ausbildungsbetriebe oder auch regelmäßig Noten und Angaben zum Leistungsstand der Auszubildenden übermitteln dürfen. Die Übermittlung dieser personenbezogenen Daten ist gemäß Art. 6 Abs. 1 Buchstabe e) Datenschutz-Grundverordnung (DS-GVO) nur rechtmäßig, wenn, wie im vorliegenden Fall, berufsbildende Schulen als Verantwortliche im Rahmen einer rechtlichen Verpflichtung handeln. Es muss also eine Rechtsgrundlage vorliegen, die die Übermittlung vorsieht oder voraussetzt. Weder die eigenen Recherchen des TLfDI, noch die des Thüringer Ministeriums für Bildung, Jugend und Sport (TMBJS) oder verschiedener Berufsbildungsausschüsse sowie Berufsschulen führten zum Ergebnis, dass eine regelmäßige Übermittlung der Berufsschulen von Noten und Leistungsstand an Dritte zu rechtfertigen ist; keine derzeit

existierende Rechtsgrundlage kann die Zulässigkeit einer solchen Datenübermittlung begründen. Darüber hinaus wurde auch geprüft, ob die nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO normierte Einwilligung als Erlaubnistatbestand für die Datenübermittlung heranzuziehen ist. Dieser Lösungsvorschlag musste aber verworfen werden, da im Ausbildungsverhältnis eine freiwillige und somit wirksame Einwilligung wegen des bestehenden Unter- und Überordnungsverhältnisses zwischen dem Auszubildenden einerseits und der beruflichen Schule sowie dem Ausbildungsbetrieb andererseits mangels Freiwilligkeit nicht möglich ist. Der TLfDI hatte deshalb gegenüber dem TMBJS vorgeschlagen, die berufsschulrechtlichen Vorschriften durch einen entsprechenden Passus zu ergänzen, der den Berufsschulen die Übermittlung von Zensuren und Leistungsständen der Auszubildenden an die jeweiligen Ausbildungsbetriebe erlaubt.
Inzwischen hat das TMBJS auch einen Verordnungsentwurf zur Änderung der Thüringer Allgemeine Schulordnung für die berufsbildenden Schulen erstellt, in dem geregelt ist, dass die Schulen die Ausbildenden unter anderem über den Leistungsstand des Schülers sowie über einen deutlichen Abfall der schulischen Leistungen informieren müssen. Der TLfDI hat diesem Verordnungsentwurf im Rahmen der erfolgten Anhörung bereits zustimmend Stellung genommen. Gleichzeitig hat er gegenüber anfragenden Ausbildungsbetrieben klargestellt, dass bis zum Inkrafttreten der Verordnung die Übermittlung von Leistungsständen und Zensuren der Auszubildenden durch die Berufsschulen an die Ausbildungsbetriebe aus datenschutzrechtlicher Sicht weiterhin unzulässig ist.

6.24 Das Klassenzimmer 2.0: modern und sicher? Die Schul-Cloud im Blick der Datenschützer

Vor dem Einsatz einer Online-Lernplattform sind zahlreiche datenschutzrechtliche Aspekte zu beachten. Dabei tauchen Probleme auf, die unter den gegebenen schulrechtlichen Bestimmungen nur schwer gelöst werden können. Insbesondere muss die Schule sicherstellen, dass die meist kommerziellen Anbieter von Lerninhalten keinen Zugriff auf personenbezogene Daten der Lernenden haben.

Viele Schulen wünschen sich neben den herkömmlichen pädagogischen Konzepten auch eine webgestützte Vermittlung digitaler Unterrichtsinhalte in Form sogenannter Online-Lernplattformen. Vorteile werden dabei in der Vielfalt der zur Verfügung stehenden Medien gesehen, auf die die Schülerinnen und Schüler jederzeit, auch außerhalb der Schule, mit privaten Datenendgeräten zugreifen können. Neben Lesetexten und Aufgaben können auch Lehrvideos, Filme, animierte Grafiken oder Ähnliches eingestellt werden. Es besteht auch die Möglichkeit, Tests anzubieten, mit denen, aufgrund automatisierter Auswertungsalgorithmen, Lernschwierigkeiten und Lernfortschritte festgestellt werden können. Eine individuellere Förderung des Lernenden kann somit zielgerichteter anhand abgestimmter Aufgaben angeboten werden. Im Regelfall dient das Verfahren auch der internen Kommunikation zwischen den Lehrkräften und Lernenden.
Ein Anbieter entwickelt seit einiger Zeit eine Online-Lernplattform mit der Perspektive eines bundesweiten Einsatzes in öffentlichen Schulen. Als Vorsitzender der Arbeitskreise Schulen und Bildungseinrichtungen sowie Datenschutz-/Medienkompetenz des Gremiums der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder entschied sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), exemplarisch für die wachsende Anzahl von Online-Lernplattformen die Entwicklung dieser Schul-Cloud aus datenschutzrechtlicher Sicht zu begleiten. Zu diesem Zweck wurde auch eine Unterarbeitsgruppe gebildet, die sich mit allen auftretenden Datenschutzfragen beschäftigt.
In dieser Schul-Cloud werden Lehrinhalte auf Servern abgelegt, die überwiegend im Verantwortungsbereich des Anbieters liegen und den registrierten Nutzern (Lernende), nach erfolgreichen persönlichen Login, zum Abruf über das Internet zur Verfügung stehen. Dabei muss auf den privaten Datenverarbeitungsgeräten, also dem PC, dem Notebook, dem Tablet oder dem Smartphone, keine weitere Software aufgespielt werden. Diese dienen nach dem Einloggen in das System lediglich als Anzeige- und Eingabegeräte. Mit der Schul-Cloud werden keine Schulverwaltungsdaten, wie Noten, Bewertungen von Schülern oder Anwesenheitskontrollen verarbeitet. Der TLfDI betonte gegenüber dem Anbieter ausdrücklich seine Forderung nach einer systemtechnischen Trennung pädagogischer Inhalte von der Schulverwaltungssoftware. Die Konfiguration muss sicherstellen, dass nur die personenbezogenen Daten verarbeitet werden, die für die pädagogische

Aufgabenerfüllung der Schule erforderlich sind. Lediglich berechtigten schulinternen Personen dürfen entsprechende, erweiterte Zugriffsrechte von der Schule eingerichtet werden.
Es ist nicht auszuschließen, dass die Schulbuchverlage und andere Anbieter, die ihre digitalen Medien in einer Schul-Cloud anbieten, ein geschäftliches Interesse an den personenbezogenen Daten der Nutzer haben. Aus diesem Grund fordert der TLfDI möglichst anonymisierte Benutzer-Logins auf der Online-Lernplattform. Die Klarnamen dürfen nur für autorisierte Lehrkräfte und Schüler sichtbar sein. Dies ist gegenwärtig zu gewährleisten, wenn die Cloud anonyme Zugriffe auf bereits eingestellte Inhalte ohne die Kenntnis einzelner Nutzer bietet.
Es gibt hierzu noch im Detail Klärungsbedarf. Dieser schließt derzeit auch schulrechtliche Fragen ein, inwiefern etwa die Schul-Cloud nur mit Einwilligung der betroffenen Personen betrieben werden darf oder, ob die Schule eine verpflichtende Teilnahme vorschreiben kann. Es wird auch vorausgesetzt, dass die Lernenden mit ihren privaten Datenverarbeitungsgeräten die Schul-Cloud nutzen. Die umfassende Finanzierung von Schulgeräten durch das Land wird sich aufgrund der immensen Kosten in absehbarer Zeit nicht erfüllen lassen, sofern noch nicht der Digitalpakt hier neue Wege eröffnet. Es ist aber noch völlig ungeklärt, ob die Verwendung von privaten Geräten (BYOD: bring your own device) von der Schule einfach vorausgesetzt werden kann und welche sicherheitstechnischen Aspekte bei der Nutzung zu beachten sind. Der TLfDI wird die Entwicklung der Schul-Cloud weiter datenschutzkritisch verfolgen. Klar ist und bleibt: Keine personenbezogenen Schüler- und Lehrerdaten gelangen in die Hände von Unbefugten!

6.25 Digitale-Lernplattform – DigLu

Schulpflichtigen Kindern und Jugendlichen, denen es nicht möglich ist, eine bestimmte Schule regelmäßig zu besuchen, sind auch unter diesen Umständen grundlegende Bildungsinhalte im Unterricht zu vermitteln. Digitale Lernkonzepte können aufgrund ihrer größeren Ortsunabhängigkeit dazu beitragen, die betroffenen Kinder und Jugendlichen intensiv zu betreuen und Unterstützung zu leisten.

Es gibt eine Gruppe von Schülerinnen und Schülern, die nicht in der eigentlich für sie zuständigen Schule (Stammschule) unterrichtet werden können. Es handelt sich hierbei um Kinder beruflich Reisender, also um schulpflichtige Kinder und Jugendliche, deren Eltern – etwa aufgrund ihrer Arbeit als Schausteller oder im Zirkus – teilweise wöchentlich den Aufenthalt wechseln. Diese Schülerinnen und Schüler können deshalb nicht regelmäßig dieselbe Schule besuchen und gehen dann in die jeweilige als Stützpunktschule bestimmte Schule vor Ort. Zusätzlich werden Bereichslehrkräfte eingesetzt, die sich speziell um die schulische Betreuung kümmern. In Thüringen stehen zwei Bereichslehrkräfte zur Verfügung, die von der Schulaufsichtsbehörde mit der Beratung und Förderung dieser Kinder und Jugendlichen beauftragt wurden. Bei der Verarbeitung personenbezogener Schüler- und Elterndaten unterliegen die Bereichslehrkräfte den gleichen schuldatenschutzrechtlichen Vorschriften wie alle anderen Lehrkräfte des Landes.
Die Schülerinnen und Schüler bzw. deren Eltern müssen ein sogenanntes Schultagebuch führen. Es handelt sich um einen Ordner, in dem u. a. der Lernfortschritt und der Lernstand dokumentiert werden. Das Schultagebuch dient auch als Grundlage zur Leistungsbewertung und Zeugniserstellung. Der Nachteil dieses Dokuments liegt auf der Hand. Geht das Buch oder gehen einzelne Dokumente hieraus verloren oder wird dieses der Stützpunktschule und der Bereichslehrkraft nur unregelmäßig vorgelegt, gehen zahlreiche Bewertungen über den Lernenden verloren. Die jeweils zuständigen Lehrkräfte wissen dann nicht, ob und falls ja, in welchen Fächern ein besonderer Förderbedarf besteht und wie der individuelle Lernplan aussieht. Darüber hinaus dient das Buch auch der gemäß § 17 des Thüringer Schulgesetzes durchzusetzenden Schulpflichtüberwachung. Schulversäumnisse von der Stützpunktschule müssen darin ebenfalls vermerkt werden.
Da sowohl das Schultagebuch die beschriebenen Nachteile besitzt und das Verfahren auch im Übrigen nicht die erforderliche schulische Betreuung optimal garantiert, engagiert sich das Thüringer Ministerium für Bildung, Jugend und Sport sowie weitere Kultusministerien der Länder bei der Entwicklung eines **elektronischen Schultagebuchs**. Unter Beteiligung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und anderer Landesdatenschutzbeauftragten wird von Vertretern der Kultusministerkonferenz ein Konzept einer Schul- und Verwaltungsplattform „DigLu – Digitales Lernen unterwegs“ in einer Arbeitsgruppe erarbeitet. Ziel

des Verfahrens ist die cloudbasierte Führung des Schultagebuchs in digitaler Form. Diese digitale Plattform ermöglicht einen Informationsaustausch unter allen beteiligten Personengruppen, also insbesondere der jeweiligen Bereichslehrkraft, der Stamm- und der Stützpunktschule sowie dem betroffenen Schüler und seinen Eltern. Angestrebt wird eine bundesweite Einführung des Systems, sodass auch eine bundesländerübergreifende Führung des Schultagebuchs ermöglicht wird. Gleichzeitig soll DigLu auch als digitale Kommunikationsplattform zur Verfügung stehen, etwa um Lehrer-Eltern- oder Lehrer-Schüler-Informationen auszutauschen. Es sind Nutzungserweiterungen vorgesehen, die der schulischen Unterstützung und Förderung der betroffenen Schüler dienen. Die Stammschule soll einen auf den Schüler zugeschnittenen Lernplan einstellen können, der dann durch diesen von jedem Ort aus eingesehen und bearbeitet werden kann. Erledigte Aufgaben können dann z. B. von der Stammschule eingesehen werden und im digitalen Schultagebuch gespeichert werden.
Alle beteiligten Landesdatenschutzbeauftragten prüfen das in der Entwicklung befindliche DigLu Verfahren gemäß Art. 32 Datenschutz-Grundverordnung (DS-GVO) dahingehend, welche technischen und organisatorischen Maßnahmen getroffen werden müssen, um die Einhaltung der Bestimmungen dieser Verordnung und anderer Rechtsvorschriften über den Datenschutz zu gewährleisten. Die angestrebte Cloudlösung verlangt unter anderem die Auswahl eines Cloud Anbieters, bei dem die für das Verfahren verantwortliche Stammschule ihre Kontrollrechte wahrnehmen kann. Wünschenswert ist ein Cloudanbieter in Deutschland oder Europa mit einem entsprechenden Serverstandort. Weitere Forderungen sind die Ende-zu-Ende Verschlüsselung beim Versenden von Dokumenten und Nachrichten unter Verwendung eines sicheren Verfahrens. Welches Schutzniveau dabei als angemessen anzusehen ist, wird maßgeblich vom Schutzbedarf der zu verarbeitenden personenbezogenen Daten bestimmt. Da eine Verarbeitung von personenbezogenen Daten besonderer Kategorien nach Art. 9 DS-GVO (z. B. Gesundheitsdaten) ein sehr hohes Schutzniveau erfordert, wurde von den beteiligten Landesdatenschutzbeauftragten empfohlen, solche Daten nicht in „DigLu“ zu verarbeiten. Im Rahmen der Erstellung eines Rollen- und Berechtigungskonzepts, in dem u. a. die Vergabe von lesenden und schreibenden Zugriffsrechten in der IT-Anwendung festgelegt wird, kann *ohne* die Verarbeitung von o. g. Daten nach Art. 9 DS-GVO aus datenschutzrechtlicher Sicht in einer Ende-zu-Ende-verschlüsselten Verbindung als Zugangssicherung

eine 1-Faktor-Authentisierung, also lediglich die Verwendung eines sicheren Passworts, für ausreichend angesehen werden. Noch nicht abschließend geklärt ist die Frage, wer die Zugriffsrechte an den Stützpunktschulen vergibt und auch wieder entzieht, wenn die Kenntnis der Daten zur Aufgabenerfüllung nicht mehr erforderlich ist.
Der Thüringer Gesetzgeber will die Nutzung solcher digitalen Lernumgebungen rechtlich einbinden und hat in der derzeit als Entwurf vorliegenden Änderung des Thüringer Schulgesetzes einen Absatz eingefügt, der zukünftig die entsprechende Möglichkeit einräumt. Dabei sollen solche Verfahren nicht nur bei Kindern beruflich Reisender, sondern auch bei längeren Aufenthalten von Schulpflichtigen in medizinischen Einrichtungen und Jugendarrestanstalten Verwendung finden. Der TLfDI wird die allgemeine Entwicklung von digitalen Lernplattformen und speziell diejenige von DigLu weiterhin mit datenschutzrechtlicher Expertise begleiten.

6.26 Neue Fragen zur Verarbeitung personenbezogener Daten im Zusammenhang mit "thoska“

Die für jede Thüringer Hochschul- und Studentenkarte (thoska) individuell erzeugte Karten-Identifikationsnummer stellt ein personenbezogenes Datum dar. Hierfür reicht es bereits aus, dass die Möglichkeit einer Verknüpfung mit dem thoska-Inhaber besteht.
Bei der Nutzung der neu hinzugekommenen Funktion von thoska als Nachweis der Fahrberechtigung im öffentlichen Personennahverkehr und der Bahn werden bei Fahrkartenkontrollen durch das hierfür zuständige Personal in zulässiger Weise personenbezogene Daten des Studierenden verarbeitet.

Ein Student beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass das Studierendenwerk Thüringen ihm im Rahmen einer Auskunftseinholung nach Art. 15 Datenschutz-Grundverordnung (DS-GVO) nicht darüber informiert habe, dass dort seine Identifikationsnummer (ID) gespeichert wird, die für jede thoska individuell erzeugt wird. Wie sich herausstellte, ging das Studierendenwerk davon aus, dass dort die thoska-ID als anonymisiertes Datum betrachtet wurde, da man keine Möglichkeit habe, die ID mit dem Namen des Inhabers zu verknüpfen. Der TLfDI gab nach Prüfung des Sachverhalts dem Beschwerdeführer

recht, dass es sich hierbei sehr wohl um ein personenbezogenes Datum im Sinne von Art. 4 Nr. 1 DS-GVO handelt. Ein Datum hat immer dann einen Personenbezug, wenn die dahinterstehende Person, gegebenenfalls auch unter Nutzung weiterer Daten, identifizierbar ist. Dabei ist es unerheblich, ob man den Namen zur Aufgabenerfüllung benötigt oder nicht, es reicht aus, wenn objektiv die Möglichkeit der Verknüpfung besteht.

Als neue Funktion findet thoska nunmehr auch eine Verwendung als eTicket zur kostenfreien Nutzung von Bahn und öffentlichen Personennahverkehr (ÖPNV). Studierende baten den TLfDI in diesem Zusammenhang um Prüfung, welche Daten bei der Fahrkartenkontrolle durch die Kontrolleure verarbeitet werden. Wie die Universität Jena auf Anfrage mitteilte, kann das Kontrollpersonal auf die frei auslesbaren Attribute der Karte Zugriff nehmen. Dies sind, wie bereits oben beschrieben, unter anderem die Karten-ID und die enthaltene eTicket Berechtigung. Weitere Daten erhalten die Unternehmen des ÖPNV in elektronischer Form nicht. Trotzdem gilt auch hier, dass es sich bei der Karten-ID um ein personenbezogenes Datum handelt, zumal das Kontrollpersonal zusätzlich zur elektronischen Kontrolle auch eine Sichtkontrolle von thoska vornimmt und somit ohnehin die dort aufgedruckten Daten (z. B. Vorname, Name, Passbild, Geburtsdatum, Name der Hochschule, Studierendenstatus, Gültigkeit des Semestertickets usw.) zur Kenntnis nehmen kann. Hiergegen bestehen aber aus datenschutzrechtlicher Sicht keine Bedenken: Da die Karten nicht an Dritte übertragbar sind, darf das ÖPNV-Unternehmen im Zweifel nachprüfen, ob die Person, die die Studierendenkarte vorzeigt, auch tatsächlich benutzungsberechtigt ist. Dies ergibt sich aus Nr. 5.8 der Beförderungsbedingungen des Verkehrsverbunds Mittelthüringen und den besonderen Tarifbestimmungen der Jenaer Nahverkehr GmbH „Semesterticket ÖPNV“. Diese Daten werden aber ausschließlich zum Kontrollzeitpunkt durch Sichtung erhoben und nicht gespeichert oder mit den elektronisch ausgelesenen Daten verknüpft.

Hinsichtlich der elektronischen Sicherheit von thoska kann auf den Beitrag des TLfDI unter 14.37 des 11. Tätigkeitsberichts verwiesen werden. Der von thoska genutzte Chip (Mifare DESfire) gilt für den Anwendungsbereich als Hochschulchipkarte weiterhin als ausreichend sicher, um den Schutz personenbezogener Daten der Hochschulangehörigen zu gewährleisten.

6.27 Stellenausschreibung 2.0: E-Mail und Online-Bewerbungen auf öffentliche Stellen

Fordert eine öffentliche Stelle dazu auf, dass sich Bewerber auf eine ausgeschriebene Stelle per E-Mail bewerben sollen, hat sie durch technische und organisatorische Maßnahmen sicherzustellen, dass die Bewerbungen ohne Zugriffsmöglichkeit unbefugter Dritter die zuständige Stelle, also die Personalverwaltung, erreichen. Es muss eine Verschlüsselungsmöglichkeit geboten werden und die Bewerbung muss direkt an die zuständige und empfangsberechtigte Person gelangen.

Zum Thema Bewerbungen per E-Mail hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit bereits in seinem 11. Tätigkeitsbericht unter Punkt 6.10 die erforderlichen Voraussetzungen nach damaliger Rechtslage dargelegt. Hierzu hat sich auch nach Anwendbarkeit der Europäischen Datenschutz-Grundverordnung (DS-GVO) und den nationalen Rechtsvorschriften nichts Grundsätzliches geändert.
Bewerbungsdaten müssen nach Art. 5 DS-GVO vor unbefugter Kenntnisnahme geschützt werden. Bewerbungsdaten unterliegen demselben Schutz wie Personalaktendaten nach § 27 des Thüringer Datenschutzgesetzes (ThürDSG) in Verbindung mit §§ 79 bis 87 des Thüringer Beamtengesetzes (ThürBG).
Sollen Bewerbungen per E-Mail zugelassen oder gar erwünscht sein, hat die verantwortliche Stelle geeignete Maßnahmen zu treffen, die unbefugte Kenntnisnahme der Bewerbungsunterlagen ausschließt und einen unversehrten Zugang zur zuständigen Personalverwaltung sicherstellt.
Das bedeutet, dass Bewerbern die in der Stellenausschreibung aufgefordert werden, sich per E-Mail zu bewerben, eine geeignete Verschlüsselungsmöglichkeit anzubieten ist, um die Vertraulichkeit der E-Mail und Sicherheit der übermittelten Daten zu gewährleisten. Weiterhin muss ein gesondertes Postfach zur Verfügung stehen, auf das nur befugte Personalverwalter der verantwortlichen Stelle zugreifen können.
Sollte ein Bewerbungsportal eingerichtet oder genutzt werden, muss der Verantwortliche die geschilderten notwendigen Maßnahmen auch gegebenenfalls im Rahmen der Auftragsverarbeitung vorgeben. Ein Beispiel dazu finden Sie im 11. Tätigkeitsbericht unter Punkt 6.16.

Bewerben sich Personen auf eine Stellenanzeige per E-Mail, ohne dass sie dazu aufgefordert und in der Stellenausschreibung auf das Risiko unbefugter Kenntnis hingewiesen wurden, weil z. B. eine Verschlüsselungstechnik nicht zur Verfügung steht, geht dieser Umgang mit personenbezogenen Daten nicht zu Lasten des Verantwortlichen. Aus Sicherheitsgründen sollte jedoch die empfangende Stelle die Eingänge und insbesondere Anhänge auf Viren und anderer Schadsoftware überprüfen, um die eigene IT-Sicherheit nicht zu gefährden.

6.28 Immer erreichbar auch in der Freizeit: Dürfen Arbeitgeber private Kontaktdaten verlangen?

Die zunehmende Entgrenzung der Arbeitswelt ist auch datenschutzrechtlich problematisch. Ändert eine verantwortliche Stelle die Festlegungen zur Rufbereitschaft derart, dass die Mitarbeiter verpflichtet werden, ihre privaten Kontaktdaten anzugeben, um somit auch außerhalb der Bereitschaftszeiten alarmiert werden zu können, stellt das einen unverhältnismäßigen Eingriff in die Privatsphäre der Betroffenen dar.

Noch vor Anwendbarkeit der EU Datenschutz-Grundverordnung (DS-GVO) erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) eine Anfrage, ob Beschäftigte in einem Gesundheitsamt ihre privaten Telefonnummern angeben müssten, damit diese mit weiteren privaten Kontaktdaten der Rettungsleitstelle für den Fall eines „Worst Case"-Szenarios weitergeleitet werden können. Hintergrund war, dass das Amt die Rufbereitschaft und das dafür vorgesehene Mobiltelefon einzelner Beschäftigter abgeschafft hatte. Fortan sollte im Notfall die Rettungsleitstelle die privaten Kontakte nach dem Zufallsprinzip abtelefonieren, um eine zuständige Person zu alarmieren. Da die Mitarbeiter nach dem Zufallsprinzip über den privaten Kontakt zu erreichen sein sollten, ließ dies den Schluss zu, dass die betroffenen Mitarbeiter keine Bereitschaft zum konkreten Zeitpunkt haben mussten.
Bei den Adressen und Telefonnummern von Bediensteten handelt es sich um Personaldaten, auf die nach § 33 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) die dienstrechtlichen Vorschriften anzuwenden sind. Nach § 79 Abs. 1 Thüringer Beamtengesetz gilt der Grund-

satz, dass Daten über Bedienstete nur verarbeitet werden dürfen, soweit dies zur Durchführung des Dienstverhältnisses erforderlich ist. Hierzu gehören auch die Kontaktdaten für Bereitschaften. Soweit ein Diensthandy für die Rufbereitschaft zur Verfügung steht, ist dieses im Fall eines Einsatzes ausschließlich zu nutzen. Private Kontaktdaten von Mitarbeitern sind nur dann erforderlich, wenn eine tatsächliche Erreichbarkeit über das Bereitschaftsdiensthandy im konkreten Fall nicht gegeben ist.
Das zur Stellungnahme aufgeforderte Landratsamt legte dar, dass man die Rufbereitschaft grundsätzlich neu geregelt habe. Rufbereitschaft bestehe nur noch an Wochenenden, gesetzlichen Feiertagen und Brückentage zwischen 7 Uhr und 19 Uhr. Außerhalb dieser Zeiten sollten die bei der Leitstelle hinterlegten privaten Kontaktdaten der Beschäftigten im Gesundheitsamt dazu dienen, die Mitarbeiter eines Sachgebiets in unaufschiebbaren Fällen kontaktieren zu können. Mitarbeiter seien schließlich arbeitsrechtlich aufgrund begründeter betrieblicher oder dienstlicher Notwendigkeiten auch in diesen Zeiten zur Wahrnehmung ihrer Dienstpflichten verpflichtet.
Wohnadressen habe man bei der Leitstelle deshalb hinterlegt, weil es denkbar sei, dass kein Mitarbeiter telefonisch erreichbar sei und deshalb der Nächstgelegene aufgesucht werden müsse, um festzustellen, ob derjenige doch zu Hause sei. Auch könne es sein, dass ein Mitarbeiter abgeholt werden müsse.
Das Landratsamt argumentierte weiter, dass die Mitarbeiter ihre Telefonnummern schließlich selbst angegeben hätten und diese Daten demnach auch genutzt werden dürften. Dass dies nicht ohne Zwang von statten gegangen war, ließ sich bereits aus der Anfrage an den TLfDI erkennen. Darin war ausgeführt, dass die Mitarbeiter teilweise mit Abmahnungen oder dienstrechtlichen Konsequenzen zur Abgabe der privaten Handynummern gedrängt wurden. Mit freiwilliger Angabe hatte dies sicher in einigen Fällen offenbar nichts zu tun.
Mit den bis dahin vorliegenden Stellungnahmen konnten die datenschutzrechtlichen Bedenken des TLfDI nicht ausgeräumt werden. Zwischenzeitlich hatte aber das Thüringer Landesarbeitsgericht eine Entscheidung zum Vorgehen des Landratsamts gefällt, nachdem Mitarbeiter gegen erhaltene Abmahnungen geklagt hatten, die gegen sie erlassen wurden, weil sie die Angabe ihrer privaten Kontaktdaten verweigert hatten. Das Gericht stellte in seiner Entscheidung vom 16. Mai 2018 (6 Sa 442/17 und 6 Sa 444/17) fest, die Pflicht zur Her-

ausgabe der privaten Mobilfunknummer stelle einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung dar, der durch ein berechtigtes Interesse des Arbeitgebers gerechtfertigt sein müsse. Eine Pflicht zur Bekanntgabe der privaten Mobilfunknummer greife besonders tief in die persönliche Sphäre des Arbeitnehmers ein. Aufgrund der ständigen Erreichbarkeit könne sich der Arbeitnehmer dem ständigen Rechtfertigungsdruck vor dem Arbeitgeber nicht mehr entziehen und somit nicht zur Ruhe kommen. Diese Problemlage habe der Arbeitgeber durch die Änderung der Rufbereitschaft herbeigeführt. Dem Arbeitgeber stünden jedoch andere Mittel zur Absicherung von Notfällen zur Verfügung.
Damit war das Verlangen zur Nennung insbesondere der privaten Handynummern als Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen – auch vom Landesarbeitsgericht festgestellt – unverhältnismäßig und damit datenschutzrechtlich unzulässig. Der TLfDI forderte das Landratsamt auf, die Erfassung insbesondere der privaten Handynummern einzustellen und die bereits erfassten Daten zu löschen. Das betreffende Landratsamt teilte daraufhin mit, dass man die Löschung der zwangsweise erhobenen Kontaktdaten bei der Leitstelle verlangt habe. Allerdings hätten sich doch noch Mitarbeiter dazu bereit erklärt, außerhalb ihrer Rufbereitschaft von der Leitstelle alarmiert werden zu können, was voraussichtlich sehr selten der Fall sein werde. Die freiwillig von diesen Mitarbeitern angegebenen Daten seien weiterhin zum Zweck der Alarmierung bereitgestellt. Soweit dies wirklich freiwillig erfolgte, wäre dies datenschutzrechtlich akzeptabel. Eine Einwilligung ist nämlich nur dann wirksam, wenn sie freiwillig erteilt wurde. Im Beschäftigungsverhältnis herrscht zwischen den Beschäftigten und der Beschäftigungsbehörde als Arbeitgeber aufgrund des Über-/Unterordnungsverhältnisses ein klares Ungleichgewicht, sodass beim Einholen von Einwilligungen regelmäßig nicht von einer Freiwilligkeit ausgegangen werden kann. Nur wenn sich die Beschäftigten frei entscheiden können, ob sie einwilligen oder eine Einwilligung ablehnen, kann die Einwilligung eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten darstellen (vergleiche auch die Ausführungen im Kurzpapier Nr. 14 der DSK unter

https://www.tlfdi.de/mam/tlfdi/themen/dsk_nr14_beschaftigtendaten-schutz.pdf). Nach § 27 Abs. 2 ThürDSG ist eine Einwilligung grundsätzlich in Schriftform einzuholen, wobei der Verantwortliche verpflichtet ist, den Betroffenen über den Zweck der Datenverarbeitung und das Widerspruchsrecht nach Art. 7 Abs. 3 DS-GVO aufzuklären.

6.29 Veröffentlichung von Personaldaten: Die Information der Bürger hat Grenzen

Anonyme Schreiben mit personenbezogenem Inhalt können von einer öffentlichen Stelle nicht einfach öffentlich bekanntgemacht werden. Sind darin Beschäftigtendaten enthalten, verstößt dies gegen die Regelungen im Beschäftigtendatenschutz. Auch wenn sich ein Bürgermeister gegen anonyme Vorwürfe verteidigen möchte, darf er den Bürgern keine Beschäftigtendaten zur Kenntnis geben.

Ein Bürgermeister sah sich veranlasst, eine anonym an die Kommunalaufsicht gerichtete Anzeige gegen ihn öffentlich in allen Schaukästen der Stadt auszuhängen. Damit rief er die Bürger zur Mithilfe bei der Ermittlung der Verfasser auf. Gegen die erhobenen Vorwürfe versuchte sich der Bürgermeister auf diese Weise dagegen zur Wehr zu setzen. In dieser anonymen Anzeige waren einige Bedienstete der Stadt mit Einzelheiten zu deren Beschäftigung in der Gemeinde, ihrer Befähigung und ihrer gesundheitlichen Verfassung enthalten. Ob dies zutraf oder nicht, war nicht maßgeblich. Für die geneigten Passanten war es sicherlich interessant, diese Einzelheiten zu den städtischen Bediensteten neben den Vorwürfen gegen den Bürgermeister zu erfahren.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) nahm dies zum Anlass, das Vorgehen des Bürgermeisters mit folgender Begründung gleich zu beanstanden:
Der Bürgermeister ist Dienstherr bei der Stadtverwaltung. Seinen Beschäftigten gegenüber hat er somit eine besondere Fürsorgepflicht. Durch den Aushang der Angaben zu den Beschäftigten wurden deren

Daten ohne Rechtsgrundlage und damit unzulässigerweise an eine Vielzahl von Empfängern übermittelt.
Für das Verarbeiten oder Nutzen von personenbezogenen Daten von Beschäftigten bei öffentlichen Stellen gelten nach § 33 des Thüringer Datenschutzgesetzes (ThürDSG) die §§ 79 bis 87 des Thüringer Beamtengesetzes (ThürBG) grundsätzlich entsprechender Weise. Nach diesen Vorschriften darf der Dienstherr personenbezogene Daten der Beschäftigten nur verarbeiten, soweit dies zur Begründung, Durchführung, Beendigung oder für weitere genannte Zwecke erforderlich ist oder eine Rechtsvorschrift dies erlaubt. Eine Vorschrift, die die Übermittlung der Beschäftigtendaten rechtfertigen könnte, findet sich in den dienstrechtlichen Vorschriften nicht. Auch die allgemeinen Vorschriften des Thüringer Datenschutzgesetzes rechtfertigten die Datenübermittlung nicht.
Die Datenübermittlung einer öffentlichen Stelle (eines Bürgermeisters) durch Aushang an Stellen außerhalb des öffentlichen Bereichs (Bürger der Stadt oder Passanten) wäre nach § 22 ThürDSG nur dann zulässig gewesen, wenn zum einen eine Erfüllung einer Aufgabe der öffentlichen Stelle vorlag und zum anderen die schutzwürdigen Interessen der Betroffenen beachtet wurden. Eine Aufgabe der Stadtverwaltung, die die Veröffentlichung der namentlich genannten Beschäftigten und die weiteren Angaben zu diesen rechtfertigte, war nicht ersichtlich. Bei Beschäftigtendaten besteht eine hohe Schutzwürdigkeit, sodass eine Abwägung mit den Interessen der Betroffenen in einem solchen Fall immer zugunsten der Betroffenen ausfällt. § 22 ThürDSG war daher ebenfalls keine Rechtsgrundlage für die Veröffentlichung.
Zur Behebung des Mangels forderte der TLfDI den Bürgermeister auf, die Aushänge unverzüglich zu entfernen und dies umgehend zu bestätigen. Gleichzeitig wurde auch die Kommunalaufsicht von der Beanstandung unterrichtet.
Obwohl der Bürgermeister überhaupt keine Einsicht zeigte, weil er ja das anonyme Schreiben nicht verfasst hatte und darüber hinaus im Aushang keine Veröffentlichung sah, ließ er die Schreiben aus den Aushängen entfernen und sah die Angelegenheit für erledigt an.
Dies verlangte geradezu weiteres Vorgehen des TLfDI, der nochmals eindringlich die Rechtslage darlegte und vor zukünftigen derartigen Aktionen eine eingehende interne Prüfung der datenschutzrechtlichen Vorschriften verlangte. Daraufhin bestätigte der Bürgermeister, dass zukünftig Aktionen, die nicht den datenschutzrechtlichen Vorschriften entsprechen, unterbleiben werden.

6.30 Darf die Landesärztekammer Einsicht in Arbeitsverträge von bei privaten Unternehmen angestellten Ärzten verlangen?

Die Thüringer Landesärztekammer (LÄK) ist gemäß § 24 Berufsordnung LÄK in Verbindung mit § 19 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) in der alten Fassung (§ 16 in der neuen Fassung) sowie § 20 Abs. 2 ThürDSG in der alten Fassung (§ 17 in der neuen Fassung) in Verbindung mit Art. 6 der Europäischen Datenschutz-Grundverordnung (DS-GVO) befugt, von privatwirtschaftlichen Unternehmen, die ärztliches Personal beschäftigen, die Vorlage von deren Arbeitsverträgen zu verlangen, um die korrekte Besoldung von Ärzten zu kontrollieren. Die LÄK ist zur Erhebung der Daten befugt; das Arbeitsschutzzentrum zur Übermittlung.

Im Februar 2018 wandte sich der Mitarbeiter eines Arbeitsschutzzentrums an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um Auskunft, ob das Arbeitsschutzzentrum einer Aufforderung der LÄK Folge leisten müsse. Die LÄK hatte das Arbeitsschutzzentrum darum gebeten, ihr die Arbeitsverträge der dort beschäftigten Ärzte zu übersenden. Als Rechtsgrundlage für die Übersendung benannte die LÄK § 24 ihrer Berufsordnung.
Der Mitarbeiter des Arbeitsschutzzentrums war sich nicht sicher, ob die Forderung der LÄK datenschutzrechtlich legitim sei. Hierzu teilte der TLfDI Folgendes mit:
Gemäß § 24 Berufsordnung der LÄK sollen Ärzte alle Verträge über ihre ärztliche Tätigkeit der Ärztekammer vorlegen, um die Wahrung ihrer beruflichen Belange prüfen zu lassen: „Auf Verlangen der Ärztekammer muss der Arzt/die Ärztin diese Verträge vorlegen, auch nach deren Abschluss.“
Die Ärztekammer durfte damit nach Art. 6 Abs. 1 Buchstabe e) DS-GVO die Daten beim Arbeitsschutzzentrum abfragen. Umgekehrt kam das Arbeitsschutzzentrum einer rechtlichen Verpflichtung nach (nämlich der Anfrage der Ärztekammer), sodass dieses die Daten nach Art. 6 Abs. 1 Satz 1 Buchstabe c) DS-GVO übermitteln durfte. Die Buchstaben c) und e) sind als Spiegelvorschriften anzusehen (Kühling; Kommentar zur DS-GVO, Art. 6 Rdnr. 78).

Aufgrund der oben genannten Rechtsvorschriften war die LÄK befugt, vom Arbeitsschutzzentrum Thüringen als privatrechtlich organisiertem Arbeitgeber von ärztlichem Personal, die Vorlage von personenbezogenen Daten in Form der Arbeitsverträge zu verlangen. Die Berufsordnung der LÄK sieht die Vorlage ärztlicher Arbeitsverträge an die LÄK vor.
Die Übermittlung war auch erforderlich, da von der LÄK zu prüfen war, ob die Weiterbildungen der Ärzte ordnungsgemäß erfolgten und ob die Besoldung den rechtlichen Vorgaben genüge. Insofern wurde auch die Verhältnismäßigkeit der Erhebung bejaht, da kein milderes Mittel zur Datenerhebung ersichtlich war.

6.31 Einführung neuer intelligenter Stromzähler

An intelligente Energienetze und -zähler sind hohe Datenschutz-/Datensicherheits-Anforderungen zu stellen. Die zentrale Komponente ist hierbei das Smart-Meter-Gateway. Diese Kommunikationseinheit mit einem eingebauten Sicherheitsmodul dient zur Übermittlung und Speicherung von Mess- und Netzzustandswerten sowie zur Steuerung und Wartung von intelligenten Geräten (z. B. intelligenten Hausgeräte, Solaranlagen) durch Marktteilnehmer (Messstellenbetreiber, Energielieferant und weitere). Zum Einsatz kommende Smart-Meter-Gateways bedürfen dabei eines Zertifikates vom Bundesamt für Sicherheit in der Informationstechnik (BSI), um einheitliche technische Sicherheitsstandards zu gewährleisten. Ein erstes Produkt wurde nun vom BSI zertifiziert, weitere befinden sich im Antragsverfahren. Der TLfDI wird das Thema auch 2019 datenschutzrechtlich im Blick behalten.

Im 10. Tätigkeitsbericht informierte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) unter Punkt 12.3, dass entsprechend der EU-Richtlinie über Energieeffizienz und Energiedienstleistungen (EDL 2006/32/EG) alle Mitgliedstaaten der Europäischen Union verpflichtet sind, intelligente Energienetze und -zähler einzuführen. Dabei sind hohe Anforderungen an den Datenschutz und die Datensicherheit zu stellen. Dies gilt insbesondere für die Smart-Meter-Gateways, die die Messdaten von Zählern empfangen, speichern und diese aufbereiten. Um einen einheitlichen technischen Sicherheitsstandard für alle Marktakteure in

Deutschland zu gewährleisten, hatte das Bundesamt für Sicherheit in der Informationstechnik (BSI) ein Sicherheitsprofil für die Smart-Meter-Gateways (BSI-CC-PP-0073) und eine entsprechende Technische Richtlinie (BSI TR-03109) erarbeitet. Die Rechtsgrundlage bildet dabei das Messstellenbetriebsgesetz (MsbG).

Gemäß § 24 Abs. 1 MsbG müssen Smart-Meter-Gateways im Rahmen des Zertifizierungsverfahrens durch das BSI zertifiziert sein. Ohne ein gültiges und gegenüber dem Smart-Meter-Gateway Administrator nachgewiesenes Zertifikat darf ein Smart-Meter-Gateway nicht als Bestandteil eines intelligenten Messsystems verwendet werden.

Eine Rückfrage bei der Thüringer Mess- und Zählerwesen GmbH & Co.KG im August 2018 ergab, dass bis dahin kein Smart-Meter-Gateway vom BSI zertifiziert wurde und somit die Aufnahme des Produktivbetriebs des intelligenten Messsystems erst in der ersten Jahreshälfte 2019 starten könne.

Nach Kenntnisstand des TLfDI wurde nun am 12. Dezember 2018 ein erstes Produkt vom BSI erfolgreich zertifiziert, weitere befinden sich beim BSI im Zertifizierung-Antragsverfahren:
https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/SmartMeterGateway/Zertifikate24Msbg/zertifikate24MsbG_node.html.

Der TLfDI wird 2019 die praktische Umsetzung prüfen.

7. Fälle nicht-öffentlicher Bereich

© alphaspirit – Female physician listening to her patient during consultation while sitting down in the office of a modern medical center

7.1 Umfrage des TLfDI zur Umsetzung der DS-GVO im nicht-öffentlichen Bereich

Im Berichtszeitraum führte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) eine Umfrage zu verschiedenen Bereichen der DS-GVO in Unternehmen durch. Ziel war es, einerseits die befragten Unternehmen für den Datenschutz und die daraus resultierenden Pflichten zu sensibilisieren sowie den Fortschritt bei der Umsetzung der DS-GVO im nicht-öffentlichen Bereich festzustellen und herauszufinden in welchen Bereichen Unternehmen noch besonders Unterstützung in datenrechtlichen Belangen benötigen.

In der vom TLfDI durchgeführten Umfrage wurden verschiedene Fragen zu unterschiedlichen Komplexen der DS-GVO gestellt. Im Einzelnen waren es Fragen zum Datenschutzbeauftragten, zum Verzeich-

nis von Verarbeitungstätigkeiten, zu Erlaubnistatbeständen, Umsetzung von Informationspflichten, Betroffenenrechten, der Datenschutz-Folgenabschätzung sowie der Auftragsverarbeitung.
Die Umfrage wurde anhand eines auszufüllenden PDFs durchgeführt, das die Unternehmen an den TLfDI per E-Mail zurück sendeten. Mit Rücksicht auf die Unternehmen wurde das Umfrageformular so gestaltet, dass sich der Zeitaufwand auf ein Minimum beschränkte. Das PDF Umfrageformular wurde aus diesem Grund ausschließlich mit Anklick-Feldern zum Beantworten der Fragen gestaltet. Zudem erleichtert diese Gestaltung des Umfrageformulars auch die Auswertung beim TLfDI.
Befragt wurden etwa 18.000 eingetrage Unternehmen Thüringens. Aus den Ergebnissen erhoffte der TLfDI zwei wesentliche Informationen:
Zum einen den derzeitigen Stand des Fortschritts bei der Umsetzung der DS-GVO in nicht-öffentlichen Unternehmen und zum anderen, in welchen Bereichen die Thüringer Wirtschaft noch besonders auf eine beratende Unterstützung angewiesen ist. In diesem Zusammenhang war es das Ziel des TLfDI, die befragten Unternehmen für den Datenschutz zu sensibilisieren und auch die eigene Beratungspraxis gegebenenfalls anzupassen.
In Bezug auf die Sensibilisierung der Unternehmen für ihre Pflichten als Verantwortlicher konnte der TLfDI bereits feststellen, dass die Meldung der Datenschutzbeauftragten an die Aufsichtsbehörden – u. a. eine Pflicht verantwortlicher Unternehmen– mit der durchgeführten Umfrage wieder deutlich zugenommen hat.

7.2 Die Kreishandwerkerschaft im Lichte der DS-GVO

Vor Umsetzung der Datenschutz-Grundverordnung (DS-GVO) erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Anfrage von einer Kreishandwerkerschaft. Diese wollte vom TLfDI wissen, ob sie nach der DS-GVO als öffentliche Stelle zu qualifizieren sei und ob man dann einen Datenschutzbeauftragten für die Innungen nach der DS-GVO bestellen müsse. Der TLfDI konnte der Stelle mitteilen, dass sie grundsätzlich als eine öffentliche Stelle anzusehen sei und einen Datenschutzbeauftragten bestellen müsse.

Vor dem Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Anfrage einer Thüringer Kreishandwerkerschaft. Diese wollte vom TLfDI wissen, ob die Kreishandwerkerschaften und Innungen ohne hoheitliche Aufgaben als öffentliche Stellen anzusehen seien. Darüber hinaus erkundigte sich die Kreishandwerkerschaft, ob für jede Innung ein Datenschutzbeauftragter bestellt werden müsse oder ob es ausreiche, wenn die Kreishandwerkerschaft selbst einen bestellen würde und dieser dann als gemeinsamer Datenschutzbeauftragter fungiere. Hintergrund der Anfrage war, dass die in Frage stehenden Innungen ohne Personal seien, da die Geschäftsführung der Kreishandwerkerschaft übertragen wurden. Der TLfDI nahm sich diesen Fragen an und konnte der Kreishandwerkerschaft mitteilen, dass Innungen und Kreishandwerkerschaften öffentliche Stellen darstellen und der Anwendungsbereich des damaligen Thüringer Datenschutzgesetz (ThürDSG) nach § 2 Abs. 1 ThürDSG (alte Fassung – a. F.) gelte. Die Bestellung eines Datenschutzbeauftragten richte sich daher nach den Vorschriften des ThürDSG (a. F.). Denn der damalige § 2 Abs. 1 ThürDSG (a. F.) sah vor, dass für die Verarbeitung und Nutzung personenbezogener Daten durch Behörden, Gerichte und sonstigen öffentlichen Stellen des Landes sowie für Gemeinden, Gemeindeverbände und sonstige der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts (öffentliche Stellen) die Bestimmungen dieses Gesetzes gelten. Auch nach der Auffassung von Gola/Schomerus (Gola/Schomerus, BDSG, Kommentar, § 2 Rdnr. 18, 11. Aufl.) handelt es sich bei einer Kreishandwerkerschaft um eine öffentliche Stelle des Landes, dies wird wie folgt begründet:

„Von Bedeutung ist, dass auch die juristischen Personen des öffentlichen Rechts, die der Aufsicht eines Landes unterstehen (z. B. kommunale Zweckverbände, Hochschulen, Industrie- und Handelskammer, Handwerkskammern, Kreishandwerkerschaften) zu den öffentlichen Stellen des Landes zählen. Diese Aussage gilt auch für Handwerksinnungen, auch wenn diese als Körperschaft des öffentlichen Rechts (§ 53 Handwerksordnung (HwO)) nicht der Aufsicht des jeweiligen Bundeslandes, sondern der Handwerkskammer (§ 73 HwO) unterstehen, wie dies auch bei dem Zusammenschluss der Handwerksinnungen eines Stadt- oder Landkreises (§ 89 Abs. 1 Nr. 5 HwO) der Fall ist. Aufgrund des öffentlichen-rechtlichen Charakters der Innungen

und Kreishandwerkerschaften und der zumindest mittelbar bestehenden Landesaufsicht ist es als sachgerecht anzusehen, sie auch den öffentlichen Stellen des Landes zuzuordnen. Vereinigungen der vorgenannten Stellen sind öffentliche Stellen der Länder, ungeachtet ihrer Rechtsform. Damit können sich die Stellen auch zu Vereinigungen des privaten Rechts zusammenschließen“. Der TLfDI schloss sich somit der herrschenden Meinung der Fachliteratur an.
Zudem teilte der TLfDI der Kreishandwerkerschaft noch mit, dass mit dem Inkrafttreten der Datenschutz-Grundverordnung diese Stellen weiterhin als öffentlichen Stellen zu qualifizieren seien und verwies auf den § 2 Abs. 2 des Entwurfs für ein angepasstes Thüringer Datenschutzgesetz (ThürDSG-E).
Hinsichtlich der Frage, ob solche Innungen einen Datenschutzbeauftragten bestellen müssen, konnte der TLfDI der Stelle mitteilen, dass es aus seiner Sicht grundsätzlich möglich sei, einen gemeinsamen Beauftragten zu bestellen, sofern kein Interessenkonflikt erkennbar sei. Der Entwurf für ein Thüringer Datenschutzgesetz sah zum damaligen Zeitpunkt im § 13 Abs. 4 ThürDSG-E vor, dass für mehrere öffentlichen Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter bestellt werden kann. Zudem können öffentliche Stelle gemäß § 13 Abs. 6 ThürDSG-E auch einen externen Datenschutzbeauftragten bestellen. Die beiden letztgenannten Regelungen sind dann ohne Änderung zusammen mit dem gesamten neuen Thüringer Datenschutzgesetz am 15. Juni 2018 in Kraft getreten.

7.3 Verstoß gegen den Erlaubnisvorbehalt: Sanktion gegen Mitglied eines Vereins

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat im Berichtszeitraum das Vorgehen im Rahmen einer Wahlwerbung mit einem vierstelligen Bußgeld sanktioniert. Das Verfahren ist mittlerweile rechtskräftig abgeschlossen.

Im Rahmen der letzten Landtagswahl hatte sich ein Bürger beim TLfDI beschwert, weil er durch einen zur Wahl stehenden Kandidaten, unter Bezugnahme auf eine bestimmte Vereinszugehörigkeit angeschrieben und um seine Stimme gebeten wurde. Bei diesem Anschreiben handelte es sich um einen unpersönlichen Massenbrief, der

offensichtlich an eine Vielzahl von Personen gerichtet war. Als Begrüßungsformel wurde „Liebes Vereinsmitglied“ gewählt. Der Bürger wurde stutzig, weil er neben der Vereinszugehörigkeit ansonsten keinerlei Bezug zum Werbenden hatte, dieser aber auf irgendeine Weise an die Information gekommen sein muss, wo der Betroffene wohnt, und dass er diesem bestimmten Verein angehört. Dass sich Kandidat und Bürger persönlich kennengelernt haben, konnte vom TLfDI ausgeschlossen werden.
Aufgrund der Beschwerde des Bürgers leitete der TLfDI zunächst ein Verwaltungsverfahren ein und befragte den zur Wahl stehenden Kandidaten zur Herkunft der zur eigenen Wahlwerbung genutzten Adressen und dem Zusammenhang der Vereinszugehörigkeit in dieser Angelegenheit. Hierauf antwortete der Wahlkandidat mit verschiedenen Begründungen, konnte aber nicht erklären, wie er an das personenbezogene Datum der Vereinszugehörigkeit der Personen kam.
Daraufhin wurde vom TLfDI ein Ordnungswidrigkeitenverfahren eingeleitet. Im Zuge des Verfahrens stieß er auf spürbare Widerstände und Widersprüche im Rahmen seiner Ermittlungsarbeiten. Aufgrund dessen entschied sich der TLfDI dafür, mehrere Zeugen anzuschreiben, um zu ermitteln, ob diese Personen ebenfalls einen entsprechenden Wahlbrief erhalten hatten. Dieser Verdacht konnte vom TLfDI tatsächlich erhärtet werden. Trotz des inzwischen erheblichen Zeitablaufs konnten sich noch ungefähr ein Dutzend Zeugen an einen entsprechenden Wahlbrief erinnern. Manche konnten ihn sogar beilegen und ebenfalls bestätigen, dass neben der Vereinszugehörigkeit keinerlei Bezug zum Wahlkandidaten bestand.
Für den TLfDI stand damit als erwiesen fest, was ohnehin bereits vermutet wurde. Der Kandidat hat in unzulässiger Art und Weise Mitgliedsdaten zu Zwecken der Wahlwerbung verwendet. Für diesen Datenschutzverstoß erließ der TLfDI einen Bußgeldbescheid in vierstelliger Höhe wegen unbefugten Verarbeitens personenbezogener Daten, die nicht allgemein zugänglich sind. Das Verfahren ist inzwischen rechtskräftig abgeschlossen.
Rechtlich war das Verfahren an dem inzwischen nicht mehr geltenden alten Datenschutzrecht zu messen, da der Verstoß zu einem Zeitpunkt stattfand, als dieses Recht noch in Kraft war. Damals wie heute gilt das Verbot mit Erlaubnisvorbehalt im Datenschutzrecht. Der Umgang mit personenbezogenen Daten ist demnach nur erlaubt, wenn es eine Norm gibt, die eben diesen Umgang erlaubt. Früher war dies in § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) -alt- geregelt.

Wann personenbezogene Daten zu Zwecken der (Wahl-)Werbung verwendet werden dürfen, war im damaligen BDSG speziell geregelt und zwar in § 28 Abs. 3 BDSG -alt-. Grundsätzlich durfte personenbezogene Werbung danach nur auf Grundlage einer wirksamen Einwilligung durchgeführt werden. Eine solche hatte der Wahlkandidat nicht eingeholt. Darüber hinaus räumte § 28 Abs. 3 Satz 2 BDSG die Möglichkeit ein, personenbezogene Daten in zulässiger Art und Weise für Werbezwecke zu verarbeiten oder zu nutzen. Diese Möglichkeit bestand jedoch nur, soweit es sich bei der Verarbeitung oder Nutzung der personenbezogenen Daten zum einen um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe (Namen, Anschrift) beschränken und zum anderen erforderlich für Eigenwerbung und Angebote der verantwortlichen Stelle ist.
Diese Möglichkeit ist allerdings an weitere Bedingungen geknüpft, die weder hier noch in allen anderen denkbaren Fällen von Wahlwerbung nicht vorlagen. Daher bleibt es auch im vorliegenden Fall mangels Erlaubnisnorm beim bereits erwähnten Verbot mit Erlaubnisvorbehalt, § 4 Abs. 1 BDSG (alt).

7.4 Datenschutz in der Praxis: Wann Ärzte einen Datenschutzbeauftragten bestellen müssen

Eines (betrieblichen) Datenschutzbeauftragten bedarf es in Anwendung des § 38 BDSG dann, wenn zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

Im Bereich logopädischer Praxen bestand Unklarheit, wann nach Art. 37 Datenschutz-Grundverordnung (DS-GVO) ein Datenschutzbeauftragter zu bestellen ist.
Die Unklarheit bezog sich insbesondere auf die Tatbestandsmerkmale
a) Kerntätigkeit des Verantwortlichen in der Datenverarbeitung und
b) Umfang der Datenverarbeitung (Art. 37 Abs. 1 Buchstabe b) DS-GVO).
Zunächst wurde zur Kerntätigkeit eines Arztes bzw. von Heilberufen die Auffassung vertreten, diese liege in der Heilung, nicht in der Datenverarbeitung. Diese Meinung wurde einhellig aufgegeben. Ziel der Tätigkeit von Ärzten ist es, Menschen gesund zu machen. Um aber

herauszufinden, wie das Leiden des Patienten zu bekämpfen ist oder ob, im Fall von Vorsorgeuntersuchungen, überhaupt ein Problem besteht, ist eine umfassende Untersuchung und Beobachtung des Patienten erforderlich, typischerweise auch regelmäßig über einen längeren Zeitraum. Die Kerntätigkeit von Ärzten liegt damit in der Verarbeitung sensibler Daten (Bergt, in Kühling/Buchner, Kommentar zur DS-GVO, Art. 37, Rdnr. 37).
§ 38 Bundesdatenschutzgesetz (BDSG) regelt, dass, wenn keine besonderen Umstände vorliegen, eine standardmäßige Arztpraxis bzw. die Praxis eines vergleichbaren Heilberufes, mit weniger als zehn Personen, die ständig mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt sind, keinen Datenschutzbeauftragten zu bestellen haben. Ab zehn Angestellten, die ständig mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt, sind gilt die Verarbeitung als umfangreich und es ist in jedem Fall ein Datenschutzbeauftragter zu bestellen, ebenso, wenn eine Datenschutz-Folgenabschätzung nach Art. 35 Abs. 1 DS-GVO durchzuführen ist § 38 Abs. 1 BDSG.

7.5 Reden ist Silber, Schweigen ist Gold: Was die ärztliche Schweigepflicht mit der Patienteneinwilligung für Heilpraktiker zu tun hat

Heilpraktiker benötigen für die Behandlung von Patienten eine Einwilligung, sie können sich nicht, wie Ärzte, auf Art. 9 Abs. 2 Buchstabe h) DS-GVO berufen.

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Anfrage des Verbandes des Osteopathen Deutschland e. V., die sich damit beschäftigte, ob Heilpraktiker für die Behandlung eine Einwilligung nach Art. 9 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) benötigen oder sich, wie Ärzte, auf Art. 9 Abs. 2 Buchstabe h) DS-GVO berufen können.
Personenbezogene Daten dürfen zu den in Art. 9 Abs. 2 Buchstabe h) DS-GVO genannten Zwecken verarbeitet werden, wenn diese Daten von Fachpersonal oder unter deren Verantwortung verarbeitet werden. Dieses Fachpersonal muss nach dem Unionsrecht, dem Recht eines

Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegen.
Für Ärzte ist dies der Fall. Sie unterliegen nach § 203 Strafgesetzbuch bzw. nach ärztlichem Standesrecht einer Schweigepflicht. Dies ist bei Heilpraktikern nicht der Fall. In der Anfrage der Osteopathen wurde angeführt, dass sich die Schweigepflicht für Heilpraktiker aus dem Behandlungsvertrag ergebe.
Berufsgeheimnisse können allerdings ihre Grundlage nur in Gesetzen sowie in anderen verbindlichen Vorschriften, also auch in berufsständischen Satzungen haben (Weichert, in Kühling/Buchner DS-GVO-Kommentar, 2. Auflage, Art. 9, Rdnr. 139). Einer einzelvertraglichen Regelung fehlt die Eigenschaft einer nationalen Stelle, die insoweit die Verantwortung vom Gesetzgeber übernimmt ein entsprechendes Regelungsregime zu errichten (Frenzel, in Paal-Pauly, DS-GVO, Art. 9 Rdnr. 47).
Daher ist eine Anwendbarkeit des Art. 9 Abs. 2 Buchstabe h) DS-GVO nicht gegeben. Es bleibt nur die Möglichkeit, mit einer Einwilligung nach Art. 9 Abs. 1 DS-GVO zu arbeiten.

7.6 Gängige Praxis im Wartezimmer: Die DS-GVO und das Aufrufen von Patienten-Namen

Aus Gründen des Datenschutzes und der Datenminimierung sollten Patienten bei der Registrierung/Anmeldung in einer Arztpraxis um Einwilligung zum Aufruf mit ihrem Namen gebeten werden. Patienten, die nicht mit ihrem Namen aufgerufen werden wollen, können von Praxismitarbeitern im Wartezimmer abgeholt werden.

Im Mai 2018 wandte sich ein Mitarbeiter einer Arztpraxis an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Frage, ob nach Umsetzung der Europäischen Datenschutz-Grundverordnung (DS-GVO) die Patienten im Wartezimmer weiterhin mit ihrem Nachnamen aufgerufen werden dürfen.
Das Aufrufen der Patienten mit Nachnamen ist datenschutzrechtlich problematisch, da deren Name Dritten, das heißt anderen Patienten, zugänglich gemacht werden. Diese Vorgehensweise wurde in deutschen Arztpraxen jedoch bisher weitgehend so gehandhabt.

Nicht gestützt werden kann diese Verfahrensweise auf Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO, da eine Interessensabwägung das überwiegende Interesse der Praxis am Aufruf des Patienten mit Namen nicht erkennen lässt und somit das Interesse des Patienten zum Schutz seiner personenbezogenen Informationen gegenüber Dritten überwiegt.
Der TLfDI empfahl, die Patienten bereits bei der Registrierung/Anmeldung um deren persönliche Einwilligung (Art. 6 Abs. 1 Satz 1 Buchstabe a) in Verbindung mit Art. 7 Abs. 1 DS-GVO) zu bitten oder sie darauf hinzuweisen, dass sie, ohne Nachteile zu haben, die Einwilligung für einen Aufruf mit Nachnamen verweigern können. Im Fall einer fehlenden Einwilligung können Mitarbeiter der Arztpraxis (Schwestern, Arzthelferinnen etc.) den jeweiligen Patienten im Wartezimmer abholen und zum Arzt begleiten ohne den Namen aufzurufen.
Als Alternative kann in den Arztpraxen auch ein Nummernsystem einschließlich eines zugehörigen Anzeigedisplays installiert werden, bei dem die Patienten nach Anmeldung in der Arztpraxis eine automatisch generierte Nummer ziehen. Die Nummer wird dann auf einem im Wartezimmer befindlichen Display angezeigt, wenn der betreffende Patient an der Reihe ist. Entsprechende Nummernsysteme werden bereits in verschiedenen Behörden seit mehreren Jahren angewandt.

7.7 Datenschutz beim Arzt: Vorgaben zum Informationsaustausch von Patientendaten zwischen Arztpraxen

Eine Übermittlung medizinischer Befunde wie Diagnosen oder Arztbriefe per Fax an weiterbehandelnde Ärzte ist zulässig (Art. 9 Abs. 2 Buchstabe h) in Verbindung mit Art. 9 Abs. 3 DS-GVO und § 22 Abs. 1 Nr. 1 Buchstabe b) Bundesdatenschutzgesetz (BDSG in der neuen Fassung). Die Übermittlung dieser Daten und Informationen unterliegt gemäß § 88 Telekommunikationsgesetz (TKG) dem Fernmeldegeheimnis und erfolgt insofern gesichert. Das Verschlüsseln eines Faxes ist technisch nicht möglich und aufgrund von § 88 TKG auch nicht erforderlich.

Im Mai 2018 wandte sich der Geschäftsführer eines Dienstleistungsunternehmens an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er gab an, bundesweit

zahlreiche Arztpraxen im Qualitätsmanagement und bei anderen gesetzlichen Anforderungen zu beraten und bat den TLfDI um Auskunft dazu, ob und unter welchen Bedingungen Arztpraxen ärztliche Dokumente per Fax versenden dürfen. Insbesondere wollte der Unternehmer wissen, ob hierbei eine Verschlüsselung auf dem Übermittlungsweg zwingend notwendig sei. Hierzu teilte der TLfDI dem Unternehmer Folgendes mit:
Mit Geltung der Europäischen Datenschutz-Grundverordnung (DS-GVO) ab 25. Mai 2018 traten zahlreiche neue Regelungen im Datenschutzrecht in Kraft. Für Arztpraxen ergeben sich aus der DS-GVO insbesondere erweiterte Informations- und Dokumentationspflichten gegenüber ihren Patienten.
In Art. 12 und Art. 13 DS-GVO sind die zwingend erforderlichen, datenschutzrechtlichen Informations- und Dokumentationspflichten der Ärzte gegenüber ihren Patienten festgelegt. Die Informationspflicht bezieht sich insbesondere auf folgende medizinische, technische und organisatorische Aspekte:

- auf die Person des Verantwortlichen
- den Zweck und die Rechtsgrundlage der Datenverarbeitung
- die Kategorien der Daten (Gesundheitsdaten)
- die Empfänger der Daten
- Zeitpunkt der Speicherung
- die Rechte des Betroffenen auf Auskunft, Berichtigung und Löschung oder Sperrung
- das Recht auf Beschwerde bei der Aufsichtsbehörde (Information ist nicht erforderlich wenn der Patient bereits über die Information verfügt (Art. 13 Abs. 4 Buchstabe a) und Art. 14 Abs. 5 Buchstabe a) DS-GVO).

Diese Informationen müssen gemäß Art. 13 Abs. 1 „zum Zeitpunkt der Erhebung“ der Daten erfolgen und somit vor Beginn der medizinischen Behandlung, da eine Behandlung erst nach der Diagnosestellung erfolgen kann, für die die Datenerhebung Voraussetzung ist. Das bedeutet, jeder Arzt ist gemäß Art. 12 Abs. 1 DS-GVO verpflichtet, seine Patienten „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ über alle Aspekte der Datenerhebung und Datenverarbeitung zu informieren. Gemäß Art. 13 Abs. 1 Buchstabe e) DS-GVO muss diese Information auch die Empfänger bzw. Kategorien von Empfängern der Daten enthalten. Dies sind beispielsweise andere Ärzte, die z. B. im Rahmen

einer medizinischen Weiterbehandlung personenbezogene, medizinische Daten übermittelt bekommen sowie Labore, denen der behandelnde Arzt medizinische Proben zur Analyse schickt. Falls der Arzt für Laboranalysen stets dieselbe Adresse nutzt, ist es zweckmäßig, die entsprechenden Kontaktdaten ebenfalls in der Patienteninformation anzugeben. Sofern sich im Verlauf der Behandlung weitere, bislang nicht genannte Datenempfänger ergeben, muss der Arzt den betroffenen Patienten hierüber ergänzend im Sinne Art. 13 informieren.
Sofern in der Patienteninformation gemäß Art. 13 Abs. 1 Buchstabe e) DS-GVO andere Ärzte und Labore als Empfänger der Daten benannt wurden, ist eine Einwilligung in die Datenweitergabe mit Blick auf Art. 9 Abs. 2 Buchstabe h) der DS-GVO in Verbindung mit Abs. 3 DS-GVO und § 22 Abs. 1 Nr. 1 Buchstabe b) Bundesdatenschutzgesetz –neu – (BDSG) entbehrlich.
Aus diesen Regelungen ergibt sich, dass die Übermittlung medizinischer Befunde per Fax an weiterbehandelnde Ärzte zulässig ist. Die entsprechende Datenübermittlung im Sinne einer gemeinsamen Mit- oder Weiterbhandlung erfolgt auf der Grundlage von Art. 9 Abs. 2 Buchstabe h) in Verbindung mit Art. 9 Abs. 3 DS-GVO, da nach der Rechtsprechung des Bundesgerichtshofes bei Inanspruchnahme eines anderen Facharztes (z. B. Laborarzt, Pathologe, Anästhesist) oder Hinzuziehung eines Konsiliararztes der Behandelnde als Vertreter des Patienten tätig wird und dadurch ein selbstständiger Vertrag zwischen dem zusätzlichen Arzt und dem Patienten zustande kommt (Weidenkaff, in Palandt; Kommentar zum BGB, § 630a, Rdnr. 3).
Art. 25 DS-GVO gibt die Parameter für den technischen Datenschutz vor. Gemäß Art. 25 Abs. 1 DS-GVO muss „der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verwendung geeignete technische und organisatorische Maßnahmen“ treffen, „die dafür ausgelegt sind, die Datenschutzgrundsätze […] wirksam umzusetzen“. Diese Forderung „zwingt den Verantwortlichen aber nicht, Maßnahmen zu treffen, die mit unverhältnismäßigen Belastungen einhergehen. Somit „muss der Verantwortliche weder Maßnahmen treffend, die über den Stand der Technik hinausgehen noch […] muss er solche Maßnahmen treffend, deren Implementierungskosten im Verhältnis zur Steigerung des Schutzniveaus für den Betroffenen unverhältnismäßig erscheinen.“ (vergleiche M. Martini in Paal/Pauly, Kommentar zur DS-GVO, Verlag Beck 2017, S. 302 Rdnr. 38) Die Übermittlung von Daten per

Fax ist in diesem Sinne als „Stand der Technik“ entsprechend anzusehen, es hat sich im Hinblick auf die „allgemein anerkannten Regeln der Technik“ als Übermittlungsmedium bewährt und ist in diesem Sinne auch von Fachleuten technisch wie rechtlich anerkannt. Der Begriff „Stand der Technik“ beschreibt dabei Maßnahmen, die dem aktuell Möglichen entsprechen. Dies trifft auf die Datenübermittlung per Fax zu. (vergleiche a. a. O., Rdnr. 39)
Um die datenschutzrechtlichen Bestimmungen bei einer Faxübersendung gemäß Art. 25 DS-GVO aus organisatorischer Sicht einzuhalten, rät der TLfDI, sich vom ärztlichen Empfänger des Faxes schriftlich bestätigen zu lassen, dass die übersandten Daten in seiner Arztpraxis bzw. seinem ärztlichen Verantwortungsbereich vor dem Zugriff Dritter (unbefugter Personen) geschützt sind und dass nur das medizinische Fachpersonal der jeweiligen Arztpraxis Zugriff auf diese Daten bzw. den per Fax übersandten Arztbrief hat.
Im Hinblick auf die durch die DS-GVO vorgegebenen technischen und organisatorischen Parameter garantiert § 88 Telekommunikationsgesetz (TKG), das die Datenübermittlung per Fax dem Fernmeldegeheimnis unterliegt. Ein Ausspähen der Daten ist gemäß Art. 10 Grundgesetz untersagt; eine Übermittlung erfolgt insofern gesichert. Eine Verschlüsselung des Faxversandes ist nicht möglich und aufgrund § 88 TKG auch nicht erforderlich. Anbieter von Telekommunikationsdiensten sind gemäß TKG verpflichtet, personenbezogene Daten über ihre Kunden geheim zu halten, beispielsweise Verbindungsdetails wie Nummer, Anschlusskennung und Zeitpunkt des Datenaustauschs sowie Nummer und Kennung der Anschlüsse. Dem Fernmeldegeheimnis unterliegen auch E-Mail, SMS und Telefon.

7.8 Informations- und Dokumentationspflichten im Gesundheitswesen: Was Arztpraxen im Umgang mit Patientendaten beachten sollten

Patienten, die bereits vor dem 25. Mai 2018 in der Arztpraxis behandelt wurden und dort weiterhin behandelt werden, sollten die Informationen gemäß Art. 13 und 14 der Datenschutz-Grundverordnung (DS-GVO) innerhalb von zwei Jahren nach Inkrafttreten der DS-GVO erhalten (Erwägungsgrund 171 DS-GVO).
Beim Abholen von Medikamenten durch fremde Personen sind Ärzte gesetzlich nicht verpflichtet, Vollmachten mit personenbezogenen

Angaben der dritten Personen (Abholer) aufzubewahren. Im Sinne von Art. 6 Abs. 1 Buchstabe b) DS-GVO ist eine Aufbewahrung aus Nachweisgründen allerdings empfehlenswert.

Im April 2018 wandte sich der Geschäftsführer eines Unternehmens für Qualitätsmanagement und Beratung aus Nordrhein-Westfalen an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Der Geschäftsführer gab an, Arztpraxen im gesamten Bundesgebiet zu beraten und bat um umfassende Auskünfte zur Auslegung von Regelungen der Datenschutz-Grundverordnung (DS-GVO) im Bereich des Gesundheitswesens. Folgende Fragen wurden aufgeworfen:

1) Reicht ein Aushang zum Thema Informationspflicht (Art. 13 und 14 DS-GVO) in der Arztpraxis, in dem das Labor, an das der Arzt Daten übermittelt, angegeben ist?
2) Muss die grundsätzliche Information nach Art. 13 und 14 DS-GVO jedem Patienten ausgehängt werden?
3) Wenn ja, müssen diese Informationen auch allen Patienten aus der Vergangenheit, gegebenenfalls mittels Briefsendung, übermittelt werden?
4) Muss bei notwendiger Aushändigung der Information eine Unterschrift zum Erhalt eingefordert werden?
5) Reicht es aus, wenn diese Informationen z. B. auf der Anmeldung ausliegen und jeder Patient bedient sich einfach?
6) Wie lange muss die Vollmacht eines Patienten für einen Abholer aufbewahrt werden, wenn der Patient Medikamente nicht selbst beim Arzt abholt, sondern hiermit eine andere Person beauftragt?

Da den Fragen 1 bis 6 der gemeinsame Aspekt Informationspflicht zugrunde lag beantwortete der TLfDI diese im Gesamtzusammenhang und teilte dem Fragesteller hierzu folgendes mit:
In Art. 12 und Art. 13 DS-GVO sind die zwingend erforderlichen datenschutzrechtlichen Informations- und Dokumentationspflichten festgelegt, die dementsprechend auch von Ärzten gegenüber ihren Patienten zu beachten sind. Diese Informationspflicht bezieht sich gemäß Art. 13 DS-GVO insbesondere auf folgende medizinischen, technischen und organisatorischen Aspekte:

- auf die Person des Verantwortlichen (Art. 13 Abs. 1 Buchstabe a) DS-GVO),

- auf den Zweck und die Rechtsgrundlage der Datenverarbeitung (Art. 13 Abs. 1 Buchstabe c) DS-GVO),
- auf die Empfänger und Kategorien von Empfängern der Daten (Art. 13 Abs. 1 Buchstabe e) DS-GVO),
- auf die Dauer der Speicherung (Art. 13 Abs. 2 Buchstabe a) DS-GVO),
- auf die Rechte des Betroffenen auf Auskunft, Berichtigung und Löschung (Art. 13 Abs. 2 Buchstabe b) DS-GVO) und
- auf das Recht zur Beschwerde bei der Aufsichtsbehörde (Art. 13 Abs. 2 Buchstabe d) DS-GVO).

Diese Informationen müssen vor Beginn der medizinischen Behandlung erfolgen. Das bedeutet, jeder Arzt ist gemäß Art. 12 Abs. 1 DS-GVO verpflichtet, seine Patienten „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ über alle Aspekte der Datenerhebung und Datenverarbeitung zu informieren.

Mit Bezug auf die Formulierungen in Art. 13 DS-GVO haben sich die Datenschutzbeauftragten des Bundes und der Länder in der Arbeitsgemeinschaft Gesundheit im März 2018 darauf verständigt, dass keine Differenzierung zwischen den Formulierungen in Art. 13 Abs. 1 DS-GVO („der Verantwortliche teilt mit“) und Art. 13 Abs. 2 DS-GVO („der Verantwortliche stellt zur Verfügung“) erforderlich ist. Grundsätzlich wird das Informieren der Patienten durch ein entsprechendes Faltblatt aus datenschutzrechtlicher Sicht und aus Nachweisgründen für den Verantwortlichen als eine sinnvolle Option angesehen. Ebenso wäre aber auch ein für alle Patienten gut sichtbarer Aushang in der Arztpraxis möglich. Entsprechende Musterformulare werden von verschiedenen Institutionen im medizinischen Bereich (Ärztekammern, Kassenärztliche Vereinigungen) erarbeitet. Eine Unterschrift der Patienten, die den Empfang der o. g. Informationen bestätigt, ist nach der DS-GVO nicht erforderlich (Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – Düsseldorf, 5. September 2018, siehe https://www.datenschutz-mv.de/datenschutz/publikationen/entschliessungen_2020_2011/?topiclist.expand=all).

Die o. g. Informationen müssen jedoch nicht an Patienten ausgegeben werden, die sich nicht (mehr) in der jeweiligen ärztlichen Behandlung befinden, deren Daten aber aufgrund ärztlicher Dokumentationspflichten noch im EDV-System vorhanden sind („Karteileichen"). Sofern Patienten bereits vor dem 25. Mai 2018 in der Arztpraxis behandelt wurden und dort weiterhin behandelt werden, sollten sie innerhalb von zwei Jahren nach Inkrafttreten der DS-GVO die entsprechenden Informationen erhalten (Erwägungsgrund 171 DS-GVO).
Zudem wollte der Fragesteller wissen, ob und wie lange die Vollmacht eines Patienten für einen Abholer aufbewahrt werden müsse, wenn der Patient Medikamente nicht selbst beim Arzt abholt, sondern hiermit eine andere Person beauftragt. Obliegt dem Arzt für den Fall, dass die Aufbewahrung der Vollmacht erforderlich ist, auch eine Informationspflicht (gemäß Art. 13/14 DS-GVO) gegenüber dem Abholer?
Der TLfDI beantwortete die Frage folgendermaßen: Bei der zur (Rezept-)Abholung bevollmächtigten Person handelt es sich um einen Vertreter im Sinne der §§ 163 ff. Bürgerliches Gesetzbuch. Der Vertreter handelt aufgrund der erteilten Vollmacht stellvertretend für den Patienten im Rahmen des Behandlungsvertrags.
Der Arzt ist gesetzlich nicht verpflichtet, die Vollmacht mit den personenbezogenen Angaben dieser dritten Person in irgendeiner Form aufzuheben oder zu speichern.
Zwar besteht für den Arzt keine gesetzliche Verpflichtung, die Vollmacht oder eine Kopie aufzubewahren, aus Nachweisgründen kann er dies zu seiner eigenen Sicherheit jedoch gemäß Art. 6 Abs. 1 Buchstabe b) DS-GVO tun. In diesem Falle muss der Arzt den Bevollmächtigten (Abholer des Rezepts) allerdings gemäß Art. 12 und 13 DS-GVO informieren, dass er dessen personenbezogene Angaben auf der Vollmacht als Verantwortlicher aufbewahrt und somit im Sinne von Art. 4 Nr. 2 DS-GVO verarbeitet.

7.9 Anfrage zum Verbleib der Patientenakte einer geschlossenen Arztpraxis in Gera

Ärztliche Aufzeichnungen müssen nach Abschluss der Behandlung grundsätzlich 10 Jahre aufbewahrt werden, § 630f Bürgerliches Gesetzbuch (BGB) sowie § 10 Abs. 4 Muster-Berufsordnung Ärzte (MBO-Ä). Die Weitergabe originaler Patientenakten, z. B. beim Arztwechsel, an einen weiterbehandelnden Arzt, bedarf grundsätzlich der

Einwilligung des Patienten. Der Patient hat gemäß § 13 Bundesdatenschutzgesetz (BDSG) in der alten Fassung (ebenso § 57 in der neuen Fassung) grundsätzlich ein Recht auf Auskunft über die zu seiner Person gespeicherten (Gesundheits-) Daten.

Im Januar 2018 wandte sich ein Bürger an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und legte dar, dass seine langjährige Arztpraxis, bei der er über 20 Jahre Patient war, Mitte 2017 geschlossen worden sei. Nach seiner Kenntnis gehörte diese Praxis zum Klinikum der Stadt. Zwischenzeitlich hatte der Beschwerdeführer eine neue Praxis gefunden. Um Missbrauch zu verhindern, hatte er im Dezember 2017 seine Krankenakte bei dem betreffenden Klinikum angefordert. Auf diese Anforderung hatte er jedoch weder eine Nachricht noch eine Information zum Verbleib seiner Akte erhalten oder über den Werdegang, wie mit entsprechenden Akten verfahren wird erhalten. Daher bat der Beschwerdeführer den TLfDI um Hilfe und Information, wie der Umgang mit solchen „hochsensiblen persönlichen Unterlagen“ gesetzlich geregelt ist. Der TLfDI informierte den Beschwerdeführer zunächst über die grundlegenden gesetzlichen Regelungen zum Umgang mit Patientenakten:
Die grundlegenden Rechtsgrundlagen sind Art. 6 Abs. 2 in Verbindung mit Art. 6 Abs. 3 Buchstabe b) und Art. 9 Abs. 2 Buchstabe h) Datenschutz-Grundverordnung (DS-GVO) zu finden. Diese Artikel enthalten eine Öffnungsklausel für den nationalen Gesetzgeber aufgrund derer er nationale Normen erlassen kann.
Gemäß § 10 Abs. 1 ff. der (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (MBO-Ä) ist der Arzt verpflichtet, über die in Ausübung seines Berufes gemachten Feststellungen und getroffenen Maßnahmen entsprechende Aufzeichnungen zu machen (Patientendokumentation, Patientenakte). Diese ärztlichen Aufzeichnungen müssen auch nach Abschluss der Behandlung grundsätzlich zehn Jahre aufbewahrt werden (§ 630f Bürgerliches Gesetzbuch (BGB) sowie § 10 Abs. 4 MBO-Ä).
Die Weitergabe des Originals der Patientenakte an einen anderen Arzt kann entweder so erfolgen, dass der „neue“ Arzt die Akte nach Art. 9 Abs. 2 Buchstabe h) DS-GVO wegen „Erforderlichkeit zur Behandlung“ oder nach Art. 9 Abs. 2 Buchstabe a) DS-GVO aufgrund der „Einwilligung des Patienten“ vom „alten“ Arzt anfordert. Selbstverständlich kann sich der Patient auch an den „alten“ Arzt wenden und

diesen um Weiterleitung der Akte bitten, wozu er diesem eine Einwilligung nach Art. 9 Abs. 2 Buchstabe a) DS-GVO für die Weiterleitung erteilt.
Im Falle des Beschwerdeführers war dieses Vorgehen jedoch nicht (mehr) möglich, da die langjährige Arztpraxis bereits dauerhaft geschlossen worden war, ohne dass der Beschwerdeführer von den oben genannten Möglichkeiten Gebrauch gemacht hatte bzw. machen konnte. Das heißt, der „alte“ Arzt stand als Ansprechpartner für den „neuen“ Arzt oder den Beschwerdeführer (ehemaliger Patient) nicht mehr zur Verfügung.
Daher wandte sich der TLfDI an das vom Beschwerdeführer angegebene Klinikum und bat aus datenschutzrechtlicher Sicht um Information zum Verbleib der Patientenakten aus der besagten geschlossenen Arztpraxis.
Das Klinikum teilte dem TLfDI mit, dass die betreffende Praxis nicht zum Klinikum, sondern zu einer anderen medizinischen Organisationseinheit gehörte. Somit befänden sich auch keine Patientenakten der genannten Praxis im Klinikum. Der Mitarbeiter des Klinikums nannte dem TLfDI die richtige medizinische Organisationseinheit, zu der die betreffende Arztpraxis gehörte; die Praxis stand in Trägerschaft einer privaten Poliklinik. Der Mitarbeiter des Poliklinikums teilte mit, dass im Archiv dieser Poliklinik die ehemaligen Patientenakten der geschlossenen Arztpraxis sicher verwahrt würden, getrennt von den „neuen“ Akten der Poliklinik. Der Zugriff auf die „alten“ Akten erfolge nur, wenn ein „alter“ Patient erscheine, der weiterbehandelt wird und in die Einsichtnahme in die alte Akte einwilligt (sogenannte 2 Schränke-Theorie).
Der TLfDI gab diese Information an den Beschwerdeführer weiter und empfahl ihm, sich direkt an die genannte Poliklinik zu wenden und teilte hierfür die Kontaktdaten der Einrichtung mit. Zudem wies der TLfDI den Beschwerdeführer auf sein Auskunftsrecht gemäß § 13 Abs. 1 BDSG in der alten Fassung (§ 57 BDSG in der neuen Fassung) hin und bot hierbei gegebenenfalls weitergehende Unterstützung an.

7.10 Team-Sitzungen in Krankenhäusern: Ein Fall für den Datenschutz?

Gesundheitsdaten zählen gemäß Art. 9 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) zu den besonders schützenswerten sensiblen Daten. Wenn unbefugte Personen im Krankenhaus an medizinischen Team-Sitzungen zur Planung der Weiterbehandlung von Patienten teilnehmen, obwohl sie an der Behandlung weder beteiligt waren noch beteiligt sein werden, würde dies eine Verletzung des Datenschutzes gemäß Art. 9 darstellen, da personenbezogene Daten unbefugten Dritten offengelegt würden, ohne dass eine Rechtfertigungsnorm des Art. 9 bestünde. Beschäftigte des Medizinischen Dienstes der Krankenversicherung Thüringen e. V. (MDK) sind nicht therapeutisch tätig und haben demnach auch nicht an medizinischen Team-Sitzungen zur Weiterbehandlung von Patienten im Krankenhaus teilzunehmen.

Im Juni 2018 erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) eine anonyme Beschwerde über den Medizinischen Dienst der Krankenversicherung Thüringen e. V. (MDK).
Der MDK habe die „Team-Sitzungen“, an denen nicht nur Ärzte und Pflegepersonal, sondern auch Therapeuten, beispielsweise Physio- und Ergotherapeuten oder Logopäden zur Festlegung der weiteren medizinischen Behandlungen teilnehmen, so gestaltet, dass das therapeutische Personal an der gesamten medizinischen Team-Sitzung teilnimmt, ohne Rücksicht auf die tatsächlichen Behandlungen, also auch dann, wenn die Patienten gar keine therapeutische Behandlung erhalten. Dadurch würden den Therapeuten unnötigerweise Patientendaten bekannt gegeben.
Aufgrund des Beschwerdevortrags bat der TLfDI den MDK um Stellungnahme zu den Vorwürfen über die Weitergabe sensibler Gesundheitsdaten an Dritte (Therapeuten, die nicht an der Behandlung von Patienten beteiligt sind) im Rahmen von medizinischen Teamsitzungen in Krankenhäusern. Der TLfDI fragte, ob der MDK bei den Beratungen zur weiteren Patientenbehandlung tatsächlich die Anwesenheit von Therapeuten fordert.
Der MDK antwortete, dass er von seinen Beschäftigten keine Teilnahme an medizinischen Teamsitzungen fordere. Der Vorwurf, dass ohne Erforderlichkeit Gesundheitsdaten verarbeitet würden (Art. 9

Abs. 2 Buchstabe h) DS-GVO „Behandlung“) konnte damit entkräftet werden.
Allerdings berate und begutachte der MDK im Auftrag der gesetzlichen Krankenversicherung gemäß §§ 275 ff. SGB V in gesetzlich bestimmten Fällen die Prüfung der ordnungsgemäßen Abrechnung von Leistungen. Der MDK legte dar, dass Beschäftigte des MDK keine, wie in der Beschwerde beschriebenen, medizinischen Team-Sitzungen im Krankenhaus durchführten und äußerte die Vermutung, dass durch den (anonymen) Beschwerdeführer Inhalte zur Abrechnungsmodalität des Entgeltsystems im Krankenhaus angesprochen wurden, die mit einer Dokumentation des Behandlungsverlaufs und dessen Besprechung in multiprofessionellen Teams verbunden sein können.
Eine Datenschutzverletzung konnte damit nicht festgestellt werden.

7.11 Umgang mit sensiblen Gesundheitsdaten: Arzt darf auf die Zusicherung der Behörde vertrauen, dass dieser eine Einwilligung zur Einsichtnahme in ärztliche Befunde vorliegt

Gemäß Art. 5 Abs. 2 bzw. Art. 7 Abs. 1 DS-GVO muss der Verantwortliche den Nachweis erbringen, dass Daten rechtmäßig, z. B. auf der Grundlage einer entsprechenden Einwilligungserklärung, erhoben und verarbeitet werden. Der Arzt darf der Zusicherung der Behörde vertrauen, wenn diese ihm gegenüber erklärt, dass eine Einwilligung zur Einsichtnahme in ärztliche Befunde vorliegt. Wenn er auf einer Übersendung der Einwilligung in Kopie besteht, wird dem die zuständige Behörde nachkommen.

Im Juli 2018 erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) unabhängig voneinander die Beschwerden von zwei Arztpraxen aus verschiedenen Thüringer Landkreisen. Die Beschwerden richteten sich jeweils gegen den Fachbereich Soziales/Schwerbehindertenrecht in den Landratsämtern. Die ärztlichen Beschwerdeführer legten dar, dass die betreffenden Behörden im Zusammenhang mit der Anforderung von ärztlichen Befundberichten im Rahmen des Feststellungsverfahrens für Schwerbehinderte den Ärzten mitteilten, dass eine ausdrückliche Einwilligungserklärung des Antragstellers aktenkundig in der Behörde vorliege und dass die Übersendung einer Kopie an den Arzt nicht erforderlich sei.

Die ärztlichen Beschwerdeführer vertraten hierzu jedoch die Auffassung, dass die Einwilligung der betroffenen Patienten/Antragsteller in die Erhebung und Übermittlung der Befunde an die Behörde auch dem Arzt vorliegen müsse. Das Thüringer Landesverwaltungsamt (TLVwA) berief sich auf die in Thüringen seit 2009 praktizierte Verfahrensweise: „Einholung der Einwilligungserklärung des Antragstellers mit Entbindung der Ärzte von der Schweigepflicht sowie Anschreiben der Ärzte mit Versicherung des Vorliegens und Zitieren der aktenkundigen Erklärung des Antragstellers im Wortlaut“. Diese wurde vereinbart zwischen der Landesärztekammer Thüringen, der Kassenärztlichen Vereinigung Thüringen, der Landeskrankenhausgesellschaft Thüringen, dem TLVwA sowie dem damaligen Thüringer Landesbeauftragten für den Datenschutz.
Das TLVwA vertrat die Auffassung, dass es nach dieser Vereinbarung dem Arzt, auch auf dessen Wunsch hin, nicht die Einwilligungserklärung übersenden müsse. Dies gelte auch für eine entsprechende Kopie. Der TLfDI antwortete dem TLVwA, dass das damalige Thüringer Ministerium für Soziales, Familie und Gesundheit im Nachgang zur Beratung 2009 mitgeteilt habe, dass Ärzten, die eine entsprechende Kopie verlangen würden, diese Kopie der Einwilligungserklärung auch übersandt werde.
Es wurde Übereinstimmung erzielt, an der bisherigen Praxis festzuhalten, einschließlich der (wohl in Vergessenheit geratenen) Möglichkeit für den Arzt, die Einwilligungserklärung in Kopie anzufordern. Für den TLfDI war lediglich zu prüfen, ob die neu in Kraft getretenen Regelungen der DS-GVO dem entgegenstehen könnten. Dies wurde im Ergebnis verneint.
Der Arzt muss gemäß Art. 5 Abs. 2 bzw. Art. 7 Abs. 1 DS-GVO den Nachweis erbringen, dass die Patientendaten rechtmäßig auf der Grundlage einer entsprechenden Einwilligungserklärung erhoben und verarbeitet werden. Nicht geregelt ist, wie der Nachweis zu erbringen ist, bzw. konkret formuliert, wo der Nachweis – d. h. die Einwilligungserklärung – gelagert wird. Wenn dies bei der Behörde erfolgt, ist der Nachweispflicht genüge getan. Wenn der Arzt/die Ärztin jedoch auf eine Übersendung der Kopie der Einwilligungserklärung besteht, wird die Behörde dem nachkommen.

7.12 Datenschutz im Gesundheitswesen: Kürzung von Pflegegeld bei festgestellten Mängeln

Gemäß § 11 Abs. 1 des Rahmenvertrags nach § 75 SGB XI zur ambulanten pflegerischen Versorgung im Freistaat Thüringen zwischen den Landesverbänden der Pflegekassen und der Arbeitsgemeinschaft der kommunalen Spitzenverbände und den Vereinigungen der Träger der ambulanten Pflegeeinrichtungen soll der Pflegedienst der Pflegekasse mittteilen, wenn nach seiner Einschätzung Maßnahmen der Prävention angezeigt erscheinen bzw. zu überprüfen sind.
Die Regelungen der Datenschutzgrundverordnung (DS-GVO) eröffnen die Möglichkeit, spezialgesetzliche Regelungen des nationalen Rechts, vorliegend des SGB, auch in Zukunft anzuwenden.

Im Juli 2018 beschwerte sich ein Bürger über einen privaten medizinischen Pflegedienst. Er gab an, dass er einen Pflegedienst mit Pflegeleistungen für seine Mutter beauftragt hatte und dass dieser Pflegevertrag im März 2018 endete. Der Pflegedienst habe im Zuge der Beendigung des Pflegvertrages neben der Tatsache der Auflösung des Vertragsverhältnisses unzulässigerweise weitere Informationen an die Krankenkasse übermittelt. Hierzu übersandte der Beschwerdeführer dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ein Schreiben der Krankenkasse, das die behauptete Datenschutzverletzung aus seiner Sicht bestätige.
Dem Schreiben der Krankenkasse war zu entnehmen, dass die pflegerische Versorgung der Mutter des Beschwerdeführers als kritisch anzusehen sei. Die Krankenkasse hatte den Beschwerdeführer gefragt, ob ein neuer Pflegedienst beauftragt worden sei und wie die Versorgung künftig erfolge. Der Beschwerdeführer gab an, den Pflegdienst nicht von der Schweigepflicht entbunden zu haben, so dass dieser gegen den Datenschutz verstoßen hätte, indem er die Daten an den medizinischen Dienst der Krankenkasse (MDK) übermittelte.
Gemäß § 75 Abs. 1 (Sozialgesetzbuch) SGB XI „sind Landesverbände der Pflegekassen unter Beteiligung des Medizinischen Dienstes der Krankenversicherung […] und die Vereinigungen Träger der ambulanten oder stationären Pflegeeinrichtungen im Land“ gehalten, „gemeinsam und einheitlich Rahmenverträge“ abzuschließen „mit dem Ziel, eine wirksame und wirtschaftliche pflegerische Versorgung der Versicherten sicherzustellen.“ Diese Rahmenverträge enthalten in der Regel auch gegenseitige Mitteilungspflichten, die u. a. auch die

Pflegesituation und/oder den Pflegezustand betreffen können. Gemäß § 11 Abs. 1 des Rahmenvertrags nach § 75 SGB XI zur ambulanten pflegerischen Versorgung im Freistaat Thüringen zwischen den Landesverbänden der Pflegekassen und der Arbeitsgemeinschaft der kommunalen Spitzenverbände und den Vereinigungen der Träger der ambulanten Pflegeeinrichtungen soll der Pflegedienst der Pflegekasse dem MDK mittteilen, wenn nach seiner Einschätzung Maßnahmen der Prävention angezeigt erscheinen bzw. zu überprüfen sind oder wenn sich der Pflegezustand oder die Pflegesituation des Pflegebedürftigen verändern (Wechsel der Pflegestufe).
Aus den vorgenannten gesetzlichen Regelungen des Sozialgesetzbuches sowie dem genannten Rahmenvertrag ergibt sich, dass Angaben über den tatsächlichen Pflegebedarf und den Pflegezustand rechtlich festgelegt sind. In diesem Sinne war auch die Übermittlung des Pflegedienstes an die Krankenkasse, dass die pflegerische Versorgung der Mutter des Beschwerdeführers als kritisch anzusehen sei, datenschutzrechtlich nicht zu beanstanden.
Die Regelungen des Sozialgesetzbuches, vorliegend SGB XI, stehen nicht im Widerspruch zu den datenschutzrechtlichen Regelungen der DS-GVO. Die DS-GVO enthält Öffnungsklauseln zur Anwendung nationaler gesetzlicher Regelungen, Art. 6 Abs. 2 und Abs. 3 Satz 1 Buchstabe b) DS-GVO, bezogen auf Gesundheitsdaten Art. 9 Abs. 2 Buchstabe i) (hier „Gewährleistungen hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsvorsorge“). Somit können auch in Zukunft spezialgesetzliche Regelungen des nationalen Rechts wie im SGB, im Rahmen der DS-GVO angewendet werden. Daher war der Pflegedienst gesetzlich gemäß Art. 75 Abs. 1 SGB XI verpflichtet, dem MDK Informationen (Daten) über den Pflegezustand der Mutter des Beschwerdeführers zu übermitteln.

7.13 Weiterleitung oder Auftragsdatenverarbeitung? Was Zahnärzte und Dentallabore im Umgang mit Patientendaten beachten sollten

Bei der Kooperation zwischen Zahnärzten und Dentallaboren muss es sich nicht in jedem Fall um eine Auftragsverarbeitung handeln. Hierbei kann es sich auch um eine Weiterleitung nach Art. 9 Abs. 2 Buchstabe h) Datenschutz-Grundverordnung (DS-GVO) handeln. Hierbei sind verschiedene Konstellationen zu unterscheiden. Dabei spielt der

Aspekt, ob das Dentallabor von einem Laborarzt oder einem Zahntechniker geleitet wird, eine entscheidende Rolle für die Frage, ob ein Vertrag zur Auftragsverarbeitung gemäß Art. 28 Abs. 2 DS-GVO erforderlich ist oder nicht.

Im Juni 2018 wandte sich die Zahntechniker-Innung Thüringen (ZIT) an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um Information, inwiefern und unter welchen Gesichtspunkten Verträge zur Auftragsverarbeitung (AVV) zwischen Zahnärzten und Dentallaboren erforderlich sind. Die Innung wies darauf hin, dass die Datenschutzbeauftragten der einzelnen Bundesländer hierzu eine unterschiedliche Auffassung verträten. So seien in Rheinland-Pfalz und Hessen nach erfolgter Prüfung keine Verträge mehr mit den Dentallaboren notwendig, wie eine Information des hessischen Datenschutzbeauftragten belege.
Die Innung legte dar, dass sie in Thüringen, nach Absprache mit der Landeszahnärztekammer Thüringen, folgende Empfehlung an die Mitgliedsbetriebe herausgegeben habe. Wenn das Dentallabor seine erbrachten Leistungen über den Zahnarzt abrechne, sei der Zahnarzt datenschutzrechtlich verpflichtet, die personenbezogenen Patientendaten zu pseudonymisieren. In diesem Fall sei keine AVV notwendig. Werden jedoch Patientennamen an das Dentallabor übermittelt, dann sei zwischen dem Zahnarzt und dem Dentallabor ein AVV erforderlich.
Die ZIT wollte wissen, ob sich der Thüringer Datenschutzbeauftragte der Rechtsauffassung des hessischen Datenschutzbeauftragten anschließen könne, nach der es sich bei der Einschaltung eines Dentallabors durch einen Zahnarzt im Regelfall nicht um eine Auftragsverarbeitung handele.
Der TLfDI teilte der ZIT mit, dass er die Auffassung seines hessischen Kollegen insoweit teile, dass es sich nicht in jedem Fall um eine Auftragsverarbeitung gemäß Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO) handeln muss, sondern dass es sich auch um eine Übermittlung nach Art. 9 Abs. 2 Buchstabe h) DS-GVO handeln könne und insofern verschiedene Konstellationen unterschieden werden müssen.
Der TLfDI legte dar, dass die Ausführungen des hessischen Kollegen eindeutig zuträfen, wenn die Rechtsprechung des Bundesgerichtshofes greife, dass der behandelnde Arzt in Vertretung für den Patienten

einen weiteren Behandlungsvertrag schließt. Im Ergebnis hat der Patient dann einen Vertrag mit dem behandelnden Arzt und dem weiterbehandelnden Arzt; es besteht allerdings kein Vertragsverhältnis zwischen den beiden Ärzten (vergleiche hierzu Palandt, Kommentar zum BGB, 77. Auflage, § 630a, Rdnr. 3) wodurch auch eine Auftragsdatenverarbeitung zwischen beiden nicht in Betracht kommt, da dazu nach Art 28 Abs. 3 DS-GVO ein Vertrag zwischen Auftraggeber und -nehmer geschlossen werden müsste.
Schwieriger ist die Antwort allerdings, wenn das Labor nicht durch einen Laborarzt, sondern durch einen Zahntechniker geführt wird. Zahntechniker gehören nicht zu den Behandelnden im Sinne des § 630a Bürgerliches Gesetzbuch (BGB) (vergleiche Palandt, a. a. O., Vor. § 630a, Rdnr. 3). Die besondere Vertretungsbefugnis ist Ärzten vorbehalten, da diese umfassend für das Wohl des Patienten verantwortlich sind, und damit von einer stillschweigenden Bevollmächtigung des Arztes zum Abschuss notwendiger weiterer Verträge mit anderen Behandelnden auszugehen ist (Rechtsprechung des Bundesgerichtshofes, siehe Nachweise in Palandt, Kommentar zum BGB, 77. Auflage, § 172, Rdnr. 19). Wenn Zahntechniker beispielsweise durch Vermittlung des Arztes einen direkten Werkvertrag mit dem Patienten abschließen, sodass ebenfalls kein Vertrag zwischen Arzt und Dentallabor besteht, dann erübrigt sich die Frage nach einer Weiterleitung/Auftragsverarbeitung, da es zu keiner Datenübermittlung zwischen Arzt und Dentallabor kommt, sondern die Daten nur zwischen Patient und Zahntechniker ausgetauscht werden.
Für den Fall, dass keinerlei Vertrag zwischen Patient und Dentallabor (geleitet durch einen Zahntechniker) besteht, sondern ausschließlich zwischen Arzt und Dentallabor ein Vertrag existiert, ist keine (einfache) Weiterleitung nach Art. 9 Abs. 2 Buchstabe h) DS-GVO möglich, da § 22 Abs. 1 Nr. 1 Buchstabe b) Bundesdatenschutzgesetz in Verbindung mit Art. 9 Abs. 3 DS-GVO eine solche Übermittlung nur erlaubt, wenn die beteiligten Personen Angehörige eines Gesundheitsberufes sind, die einer entsprechenden Geheimhaltungspflicht unterliegen. Zahntechniker unterliegen keiner gesetzlichen Geheimhaltungspflicht, sodass daran die Möglichkeit einer Weiterleitung nach Art. 9 Abs. 2 Buchstabe h) DS-GVO scheitert. In diesem Fall bedarf es eines Vertrags zur Auftragsverarbeitung nach Art. 28 und 29 DS-GVO. Eine solche Konstellation ist für den Patienten daran zu erkennen, dass der jeweilige Arzt dem Patienten die erbrachten Laborleistungen direkt in Rechnung stellt.

7.14 Namensschilder am Arbeitsplatz: Müssen Beschäftigte ihren Namen dafür hergeben?

Will ein Unternehmen die namentliche Ansprechbarkeit der Mitarbeiter für Kunden und Besucher anbieten, müssen dabei auch die Belange und Interessen der Mitarbeiter berücksichtigt werden.

Offenbar sensibilisiert durch die Anwendbarkeit der Europäischen Datenschutz-Grundverordnung (DS-GVO) seit 25. Mai 2018 erreichten den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) Anfragen von Beschäftigten verschiedener Unternehmen, ob sie denn Namensschilder tragen müssten.
Die Thematik ist auch nach der Änderung der datenschutzrechtlichen Vorschriften daher immer wieder aktuell. Bereits im 2. Tätigkeitsbericht des TLfDI im nicht-öffentlichen Bereich aus den Jahren 2014/2015 wurde die Rechtslage unter 5.13 zu Namensschildern im Krankenhaus dargestellt. Daran hat sich in der Sache grundsätzlich nichts geändert. Da das Tragen von Namensschildern nicht für die Durchführung des Beschäftigungsverhältnisses erforderlich ist, sondern nur die namentliche Ansprechbarkeit gewährleisten soll, kommt § 26 des Bundesdatenschutzgesetzes -neu- (BDSG) als Vorschrift für die besondere Verarbeitungssituation im Beschäftigungsverhältnis nicht zur Anwendung.
Nach wie vor gilt daher, dass die Verarbeitung personenbezogener Daten (hier der Name) nur dann zulässig ist, wenn die betroffene Person eingewilligt hat oder die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordert, überwiegen (Art. 6 Abs. 1 Buchstabe a) und Buchstabe f) der DS-GVO). Dieser Grundsatz fand sich auch in § 28 Abs. 1 Nr. 2 des Bundesdatenschutzgesetzes -alt-.
Eine Einwilligung im Beschäftigungsverhältnis ist aber mangels Freiwilligkeit der Entscheidung nur in wenigen Fällen wirksam. Eine freie Entscheidung in diesem Zusammenhang ist aufgrund des Über- und Unterordnungsverhältnisses kaum denkbar.
Insoweit muss der Arbeitgeber die berechtigten Interessen der Beschäftigten abwägen. Tragende Gründe für das Unternehmen sind zumeist Kundennähe und namentliche Ansprechbarkeit der Mitarbeiter.

Sollen die Beschäftigten Namensschilder tragen, muss der Arbeitgeber einschätzen, inwieweit die Beschäftigten durch das Tragen ihrer (vollständigen) Namen beeinträchtigt werden können. Für den einzelnen Beschäftigten, der sich mit vollem Namen auszuweisen hat, besteht die Gefahr, dass seine personenbezogenen Daten mit weiteren Daten (Adresse, Telefonnummer, Angaben in sozialen Netzwerken) zusammengeführt werden können, sodass unerwünscht möglicherweise außerhalb des Beschäftigungsverhältnisses Kontakte gesucht werden. Um diese Gefahr zu minimieren würde es ausreichen, entweder den Vor- oder den Nachnamen auf dem Namensschild anzubringen. Der TLfDI vertritt nach wie vor die Auffassung, dass es den Beschäftigten freigestellt werden sollte, ob sie lediglich den Nachnamen auf dem Namensschild zu lesen wünschen oder gegebenenfalls auch nur den Vornamen.
Dienen Namensschilder auf der Berufskleidung in einem Unternehmen lediglich intern der erforderlichen Zuordnung zur Person, ohne dass unternehmensfremde Personen wie z. B. Kunden diese zur Kenntnis nehmen können, kann es sich grundsätzlich um einen zulässigen Zweck handeln, können etwaige entgegenstehende Interessen der Betroffenen zurücktreten.

7.15 GPS-Ortung: Das Auge des Chefs

GPS (Global Positioning Systems) garantiert, dass sekundenschnell und nahezu ohne Ausnahme festgestellt werden kann, wo sich ein bestimmtes Fahrzeug zu einem präzisen Zeitpunkt befindet. Selbst das Fahrverhalten des Autos kann damit kontrolliert werden. Ein solches System darf aber nicht dazu genutzt werden, Beschäftigte anlasslos auf „Schritt und Tritt“ zu überwachen. Bevor GPS-Dienste zur Kontrolle eingesetzt werden, muss daher von der verantwortlichen Stelle genau geprüft werden, welche Daten zu welchem Zweck verarbeitet werden dürfen.

Global Positioning Systems (GPS) werden zunehmend in Unternehmens- und Dienstfahrzeugen eingesetzt und bieten Vorteile primär zur Positionsbestimmung im Zusammenhang mit Diebstählen. Zumindest ist das immer das erste Argument, das von Arbeitgeberseite ins Feld geführt wird. Da GPS aber vor allem auch dazu geeignet ist, die Be-

wegung der Mitarbeiter mit dem damit ausgestatteten Fahrzeug minutiös zu überwachen, erreichten den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) sowohl Beschwerden von Mitarbeitern, die sich vom Arbeitgeber kontrolliert sahen als auch Beratungsanfragen von verantwortlichen Stellen, die den Einsatz von GPS rechtskonform gestalten wollten.

Bei GPS als (noch) neuer Technologie handelt es sich grundsätzlich um Verfahren, für die nach Art. 35 Abs. 1 Satz 1 Datenschutz-Grundverordnung (DS-GVO) eine Datenschutzfolgenabschätzung durchzuführen ist. In einer Vorabprüfung ist vom Verantwortlichen einzuschätzen, ob die Verarbeitung aufgrund ihrer Art, ihrer Umstände und ihrer Zwecke voraussichtlich ein hohes Risiko für Rechte und Freiheiten natürlicher Personen aufweist. Will ein Unternehmen Bewegungsprofile von Beschäftigten zur Sicherung des Personals (z. B. Wachpersonal), zum Schutz von wertvollem Eigentum des Arbeitgebers oder eines Dritten (z. B. LKW-, Geldtransport oder mitgeführte Spezialgeräte) oder zur Koordinierung von Arbeitseinsätzen im Außendienst, eine „Geolokalisierung“ einsetzen, muss es zunächst vor dem Einsatz der Systeme prüfen, welche konkreten Daten erfasst und verarbeitet werden sollen. Verarbeitet werden dürfen nur die Daten, die für den konkreten Zweck erforderlich sind. Die Risiken für die Betroffenen sind zu minimieren oder zu kompensieren. Daher sind reine Fahrzeugbewegungsdaten und Fahrzeugpositionsbestimmungen zunächst nicht risikobehaftet, wenn sie nicht mit einem Fahrzeugführer verknüpft sind oder werden.

Sollte das System in eigener Regie oder in Auftragsverarbeitung unter Beteiligung eines Dienstleisters betrieben werden, müssen die konkreten Daten für den zulässigen Zweck festgelegt werden. Im Falle der Auftragsverarbeitung ist eine entsprechende Vereinbarung abzuschließen.

Es muss weiterhin bestimmt werden, für welchen konkreten Zweck welche Personen Zugriff haben dürfen, wie lange die Daten aufbewahrt bzw. gespeichert werden dürfen – was wiederum am konkreten Zweck und der Erforderlichkeit auszurichten ist – und gegebenenfalls, für welche Zwecke die Daten genutzt werden dürfen. Im Falle der Auftragsverarbeitung ist die Grundlage eine entsprechende Vereinbarung mit der damit beauftragten Firma.

Eine besondere Bedeutung kommt der Transparenz für die Betroffenen nach Art. 12 DS-GVO zu. Mitarbeiter müssen demnach entweder durch eine Dienst- bzw. Betriebsvereinbarung oder eine Dienst- bzw.

Betriebsanweisung umfassend darüber informiert werden, welche personenbezogenen Daten erhoben und wie lange diese Daten verarbeitet werden sowie für welche Zwecke sie genutzt werden. Bewegungsprofile, die mithilfe von GPS erstellt werden können, dürfen nicht für eine unzulässige Leistungs- und Verhaltenskontrolle genutzt werden. Dies muss eindeutig als unzulässig erklärt werden.
Der Einsatz eines GPS-Ortungssystem kann auch regelmäßig nicht auf die Einwilligung der beschäftigten Betroffenen gestützt werden, denn bei flächendeckender Überwachung kann nicht von einer Freiwilligkeit der Einwilligung ausgegangen werden.
In folgenden Fällen kann der Einsatz einer GPS-Überwachung zulässig sein:

I. Winterdienst

Die Dokumentation zur Einhaltung der Räumungs- und Streutouren von Winterdiensten stellt einen zulässigen Zweck dar, der die Erfassung von Bewegungsdaten der jeweiligen Fahrzeuge rechtfertigt. Dabei ist darauf zu achten, dass die Zusammenführung dieser Daten mit den für diese Aufgaben eingeteilten Mitarbeitern grundsätzlich ausgeschlossen wird. Zum Nachweis, dass die Arbeiten erledigt wurden und bei eventuellen Regressansprüchen gegen die Kommune, reicht es aus nachzuweisen, dass ein Fahrzeug die Tour zu einem bestimmten Zeitpunkt erledigt hat. Sind weitere Ansprüche nicht mehr zu erwarten oder auszuschließen, müssen die Daten der gelöscht werde, sofern mit Einsatzlisten festgestellt werden könnte, welche Mitarbeiter das Fahrzeug bedient haben, damit eine Leistungs-und Verhaltenskontrolle ausgeschlossen werden kann.

II. Motorisierte Straßenaufsicht

Auch das Abfahren von Straßen und Wegen zur Dokumentation und somit auch zur Erfassung möglicher Schäden sind zulässige Zwecke, die mithilfe von GPS erfolgen können. Auch hier gilt, dass eine Verknüpfung mit personenbezogenen Daten der Mitarbeiter auszuschließen ist. Werden die Fahrzeuge nur von wenigen Mitarbeitern bedient, ist eine personenbezogene Auswertung dieser Daten zur Verhaltens- und Leistungskontrolle der Angestellten unzulässig.

III. Notdienste

Kommt es darauf an, schnellstmöglich aufgrund eines Notfalls oder einer Havarie vor Ort zu sein, kann mit der Einsicht in die Positionsdaten schnell festgestellt werden, welches Fahrzeug sich in nächster Nähe befindet. In diesen Fällen muss auch mit dem Fahrer Kontakt aufgenommen werden können, um ihn über die bevorstehende Aufgabe zu informieren. Aus diesem Grund darf in einem solchen Fall ein Personenbezug mit erhobenen GPS-Daten hergestellt werden.

IV. Nutzung als Fahrtenbuch

Ist einem Beschäftigten auch die private Nutzung eines mit GPS ausgestatteten Fahrzeugs gestattet, muss es möglich sein, das GPS für private Fahrten zu deaktivieren. Die Führung eines Fahrtenbuchs mithilfe von GPS-Daten ist nur mit einer ausdrücklichen und freiwilligen Einwilligung des Beschäftigten zulässig. Diese richtet sich nach § 26 Abs. 2 BDSG bzw. § 27 Abs. 2 ThürDSG.

7.16 Einwilligungen am Arbeitsplatz: Was bei der Übermittlung von Beschäftigtendaten zu beachten ist

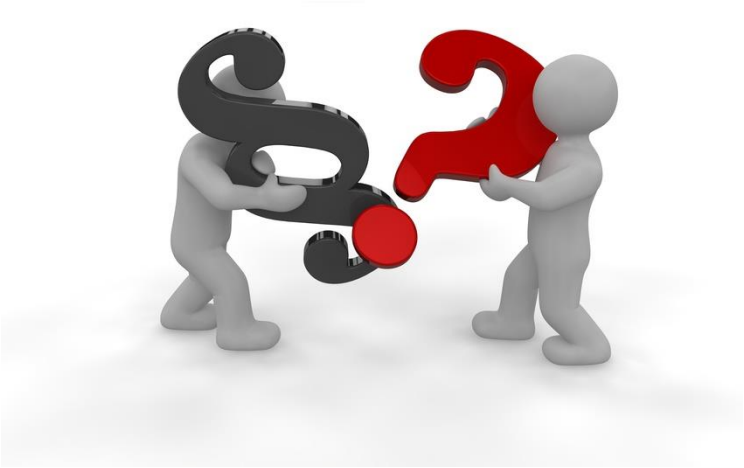
Die Verarbeitung von Beschäftigtendaten auf der Grundlage der Einwilligung der Betroffenen ist regelmäßig mangels Freiwilligkeit im Hinblick auf das Ober-/ Unterordnungsverhältnis unwirksam, es sei denn, es liegen Ausnahmen in den in § 26 Abs. 2 Bundesdatenschutzes (BDSG) genannten Fällen vor.

Fälle, in denen Beschäftigtendaten auf Basis einer Einwilligung der betroffenen Personen verarbeitet werden dürfen, sind selten. Im Kurzpapier Nr. 14 der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder „Beschäftigtendatenschutz“ (https://www.tlfdi.de/mam/tlfdi/themen/dsk_nr14_beschaftigtendatenschutz.pdf) ist dazu unter II) ausgeführt, dass die Einwilligung aufgrund der hohen Anforderungen an die Freiwilligkeit in der

Praxis überwiegend in Konstellationen möglich sein wird, die nicht das Arbeitsverhältnis als solches, sondern Zusatzleistungen des Arbeitgebers betreffen. § 26 Abs. 2 BDSG regelt restriktiv, dass Beschäftigte dann in eine Datenverarbeitung freiwillig einwilligen, wenn für die Beschäftigten ein rechtlicher oder wirtschaftlicher Erfolg erreicht wird.
Auch wenn es ein Unternehmen mit seinen Beschäftigten nur gut meint, müssen die Mitarbeiter umfassend informiert werden und deren freiwillige Einwilligungen schriftlich vorliegen (§ 26 Abs. 2 BDSG), damit Datenverarbeitungen auf der Basis von Einwilligen zulässig sind.
Ein Beschäftigter eines Unternehmens, der kurz zuvor aus Altersgründen ausgeschieden war, wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil er von einer privaten Krankenkasse angeschrieben wurde und über die Verarbeitung seiner personenbezogenen Daten nach Art. 13 und Art. 14 Datenschutz-Grundverordnung informiert wurde. Wieso und weshalb, konnte er sich nicht erklären und befürchtete, es kämen auf ihn Zahlungsverpflichtungen zu. Nach seinem Dafürhalten konnte das Versicherungsunternehmen seine Daten nur von seinem ehemaligen Arbeitgeber erhalten haben.
Der vom TLfDI angeschriebene ehemalige Arbeitgeber teilte mit, er habe kostenfrei für alle Mitarbeiter ein privates Zusatzpaket zur Krankenversicherung mit vielen Vorteilen abgeschlossen. Dies sei auch nicht hinter dem Rücken der Beschäftigten gemacht worden, man habe sie in einer Betriebsversammlung informiert und zudem Informationen zum Vorhaben als Newsletter bereitgestellt. Da keine Widersprüche der Beschäftigten bekannt wurden, war man davon ausgegangen, dass alles im Sinne der Betroffenen sei. Damit die Beschäftigten die Vorteile dieser Zusatzversicherung auch in Anspruch nehmen konnten, habe dem Versicherungsunternehmen die Kontaktdaten der Beschäftigten mitgeteilt. Leider habe man versäumt, von jedem Einzelnen eine Einwilligung zur Datenübermittlung einzuholen.
Der TLfDI führte aus, er halte aus Gründen der Transparenz eine weitergehende Information aller Mitarbeiter zur erfolgten Datenübermittlung und die schriftliche Einwilligung hierzu für erforderlich, auch wenn die Versicherung über die Kontaktdaten bereits verfüge. Sollte ein Mitarbeiter damit im Nachhinein nicht einverstanden sein, müssten die Löschung der Daten beim Versicherungsunternehmen veranlasst werden.

Dem kam das Unternehmen unverzüglich nach. Es teilte mit, man habe nachträglich den Beschäftigten die erforderlichen Informationen und ein Formular zur schriftlichen Einwilligung ausgehändigt. Sollte eine Einwilligung nicht erteilt werden, werde auf eine unverzügliche Löschung der Daten hingewirkt.
Damit wurde den datenschutzrechtlichen Anforderungen Rechnung getragen.

8. Entschließungen und Beschlüsse



© ilro - Paragraph und Fragezeichen - fotolia.com.jpg

8.1 Zuverlässigkeitsüberprüfungen bei öffentlichen und privaten Veranstaltungen nur im erforderlichen Maß und nach einem rechtsstaatlichen und transparenten Verfahren

Entschließung
der 95. Konferenz der unabhängigen Datenschutzbehörden
des Bundes und der Länder
am 24. – 26. April 2018 in Düsseldorf

Zunehmend werden im Rahmen von öffentlichen und privaten Veranstaltungen Personen, die in unterschiedlichen Funktionen auf einem Veranstaltungsgelände tätig werden wollen oder sonst Zutritt zu Sicherheitszonen begehren (beispielsweise Anwohner), durch Sicherheitsbehörden auf ihre Zuverlässigkeit überprüft. Auch bei privaten Veranstaltungen fordern die Polizeien die Veranstalter bisweilen dazu auf, dafür zu sorgen, dass alle im Rahmen der Veranstaltung Tätigen einer solchen Prüfung unterzogen werden. In den meisten Fällen ist alleinige Grundlage für diese Maßnahmen immer noch die Einwilligung der Betroffenen.

Bereits vor mehr als zehn Jahren haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 25./26. Oktober 2007 darauf hingewiesen, dass allein die Einwilligung der Betroffenen in eine Zuverlässigkeitsüberprüfung keine legitimierende Grundlage für solche tiefen Eingriffe in das Recht auf informationelle Selbstbestimmung darstellen kann. Die wiederholten Forderungen nach Schaffung gesetzlicher Grundlagen haben seitdem die Gesetzgeber nur weniger Bundesländer aufgegriffen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) fordert die Gesetzgeber und die Verantwortlichen deshalb erneut nachdrücklich auf, für ein rechtsstaatliches und transparentes Verfahren solcher Zuverlässigkeitsüberprüfungen zu sorgen, das auf das absolut erforderliche Maß beschränkt bleibt, sowohl was den Umfang der Überprüfung als auch den betroffenen Personenkreis betrifft. Dabei sind insbesondere folgende Rahmenbedingungen zu beachten:

Zuverlässigkeitsüberprüfungen nur aufgrund einer spezifischen Rechtsgrundlage

Die Gesetzgeber werden aufgefordert, bereichsspezifische Rechtsgrundlagen zu schaffen, die den Grundsatz der Verhältnismäßigkeit beachten und aus denen sich die Voraussetzungen und der Umfang der Überprüfungen klar und für die Bürgerinnen und Bürger erkennbar ergeben.

Zuverlässigkeitsüberprüfungen nur im erforderlichen Maß

Anwendung, Umfang, Kreis der betroffenen Personen und die Datenverarbeitung sind auf das Erforderliche zu beschränken. Generell dürfen Zuverlässigkeitsüberprüfungen nur bei solchen Veranstaltungen eingesetzt werden, die aufgrund ihrer spezifischen Ausprägung infolge einer belastbaren Gefahrenprognose als besonders gefährdet bewertet werden. Korrespondierend müssen die personenbezogenen Daten, die in den zum Abgleich herangezogenen Dateien und Informationssystemen gespeichert sind, nicht nur eine ausreichende Qualität haben, es dürfen auch nur hinreichend gewichtige Delikte in die Über-

prüfung einbezogen werden. Zudem müssen die Kriterien, die zur Annahme von Sicherheitsbedenken führen, einen konkreten Bezug zu den abzuwehrenden Gefahren haben.

Zuverlässigkeitsüberprüfungen nur in einem transparenten Verfahren

Die Rechte und Freiheiten der betroffenen Personen müssen durch ein transparentes Verfahren gewährleistet werden. Dazu müssen insbesondere Anhörungsrechte der betroffenen Personen rechtlich verankert werden. Im praktischen Verfahren kann im Einzelfall auch die Einrichtung einer Clearingstelle sinnvoll sein. Zudem sollten zumindest die Datenschutzbeauftragten der Verantwortlichen frühzeitig vorab beteiligt werden, damit eine datenschutzrechtliche Beratung für eine datensparsame Ausgestaltung und Beschränkung des konkreten Verfahrens stattfinden kann.

8.2 Facebook Privacy Scandal – Enforcing the New Data Protection Law within Social Network Services

Entschließung
der 95. Konferenz der unabhängigen Datenschutzbehörden
des Bundes und der Länder
am 24. – 26. April 2018 in Düsseldorf

In March 2018, it became public that – according to the company – personal data of 87 million users worldwide, of which 2.7 million were Europeans and around 310,000 Germans, were collected through an app which was connected with Facebook from November 2013 until May 2015 and transferred to the analysis company Cambridge Analytica. Apparently, they have been also used for profiling for political purposes there.

On this occasion, the competent authority in Germany, the Hamburg Commissioner for Data Protection and Freedom of Information (HmbBfDI), initiated fine proceedings against Facebook. He is in close exchange with his European colleagues, with the Information Commissioner's Office in Great Britain and the Article 29 Working Party in particular. The privacy scandal concerning Facebook and Cambridge Analytica highlights the handling of millions of users' data. The occurrences regarding Cambridge Analytica are further documenting that Facebook allowed developers of apps access to personal data of individuals who are friends with Facebook users who use this app on a huge scale over years. It happened without consent of the data subjects. In fact, the currently discussed case of a single app is just the tip of the iceberg. Tens of thousands of apps employ the Facebook login system. The number of the persons concerned unlawfully is likely to go dramatically beyond the dimension of the Cambridge Analytica case and, basically, affect all Facebook users. This incident shows, moreover, the risks of profiling when using social media and subsequent microtargeting which, obviously, was utilized for the manipulation of a democratic process of developing an informed opinion.

Germany's Conference of Independent Federal and Länder Data Protection Authorities, commonly referred to as the DSK or "Datenschutzkonferenz" (Data Protection Conference) urges to draw the

following conclusions from the infringement of data protection rights of individuals in, obviously, huge numbers:

- Social network services have to adjust their business models to the new European data protection law and have to meet their responsibilities. Among these are: making reasonable arrangements against abuse of personal data.
- In the future, Facebook has to make sure that the rules of the General Data Protection Regulation (GDPR) are being implemented: the introduction of the automatic facial recognition by Facebook in Europe raised significant doubts if the procedure of approval is compatible with the legal requirements, with regards to consent in particular. It is an illegitimate manipulation of users if Facebook forces them and makes it much easier for them to give their consent in the processing of biometric data than to refrain from it.
- The reactions to the infringement of data protection law are not restricted to the execution of data protection law but are concerning also competition and anti-trust law. The call for demerging the Facebook enterprise will increase to the same extent asit tries to obtain anti-competitive advantages on the market of digital services by systematically bypassing data protection law. There is a demand of European initiatives to limit monopoly-like structures in the area of social networks and to create transparency about algorithms.

Since the processing of data is becoming more and more complex and intransparent for data subjects, the data protection authority is playing a crucial role. Its professional expertise is in demand. They have to have the organizational and personnel means to be able to advise and shape. A strong data protection law and effective supervisory authorities reduce the risks for citizens in a digital society. If Facebook and other social network services are not ready to comply with the European law that protects users, all measures available to the supervisory authorities have to be exploited consistently on the national and on the European level.

8.3 Facebook-Datenskandal – Neues Europäisches Datenschutzrecht bei Sozialen Netzwerken durchsetzen!

Entschließung
der 95. Konferenz der unabhängigen Datenschutzbehörden
des Bundes und der Länder
am 24. – 26. April 2018 in Düsseldorf

Im März 2018 wurde in der Öffentlichkeit bekannt, dass über eine von November 2013 bis Mai 2015 mit Facebook verbundene App nach Angaben des Unternehmens Daten von 87 Millionen Nutzern weltweit, davon 2,7 Millionen Europäern und etwa 310.000 Deutschen erhoben und an das Analyseunternehmen Cambridge Analytica weitergegeben wurden. Dort wurden sie offenbar auch zur Profilbildung für politische Zwecke verwendet.

Aus diesem Anlass hat der national zuständige Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ein Bußgeldverfahren gegen Facebook eingeleitet. Er steht dabei in engem Austausch mit seinen europäischen Kollegen, insbesondere mit dem Information Commissioner's Office in Großbritannien sowie der Artikel-29-Gruppe. Der Datenskandal um Facebook und Cambridge Analytica wirft ein Schlaglicht auf den Umgang mit Millionen Nutzerdaten. Zudem dokumentieren die Vorgänge um Cambridge Analytica, dass Facebook über Jahre hinweg den Entwicklern von Apps den massenhaften Zugriff auf Daten von mit den Verwendern der Apps befreundeten Facebook-Nutzenden ermöglicht hat. Das geschah ohne eine Einwilligung der Betroffenen. Tatsächlich ist der aktuell diskutierte Fall einer einzelnen App nur die Spitze des Eisbergs. So geht die Zahl der Apps, die das Facebook-Login-System nutzen, in die Zehntausende. Die Zahl der davon rechtswidrig betroffenen Personen dürfte die Dimension des Cambridge-Analytica-Falls in dramatischer Weise sprengen und dem Grunde nach alle Facebook-Nutzenden betreffen. Das Vorkommnis zeigt zudem die Risiken für Profilbildung bei der Nutzung sozialer Medien und anschließendes Mikrotargeting, das offenbar zur Manipulation von demokratischen Willensbildungsprozessen eingesetzt wurde.

Die Datenschutzkonferenz fordert aus diesen offenbar massenhaften Verletzungen von Datenschutzrechten Betroffener folgende Konsequenzen zu ziehen:

- Facebook muss den wahren Umfang der Öffnung der Plattform für App-Anbieter in den Jahren bis 2015 offenlegen und belastbare Zahlen der eingestellten Apps sowie der von dem Facebook-Login-System betroffenen Personen nennen. Ferner gilt es Betroffene über die Rechtsverletzungen zu informieren.
- In Zukunft muss Facebook sicherstellen, dass die Vorgaben der Datenschutz-Grundverordnung (DS-GVO) rechtskonform umgesetzt werden: Die Vorstellung von Facebook zur Einführung der automatischen Gesichtserkennung in Europa lässt erhebliche Zweifel aufkommen, ob das Zustimmungsverfahren mit den gesetzlichen Vorgaben insbesondere zur Einwilligung vereinbar ist. Wenn Facebook die Nutzenden dazu drängt und es ihnen wesentlich leichter macht, der biometrischen Datenverarbeitung zuzustimmen, als sich ihr zu entziehen, führt dies zu einer unzulässigen Beeinflussung des Nutzers.
- Die Reaktionen auf datenschutzwidriges Verhalten sind dabei nicht allein auf den des Datenschutzrechts beschränkt, sondern betreffen auch das Wettbewerbs- und Kartellrecht. Die Forderung nach einer Entflechtung des Facebook-Konzerns wird in dem Maße zunehmen, wie sich dieser durch die systematische Umgehung des Datenschutzes wettbewerbswidrige Vorteile auf dem Markt digitaler Dienstleistungen zu verschaffen versucht. Es bedarf europäischer Initiativen, um monopolartige Strukturen im Bereich der sozialen Netzwerke zu begrenzen und Transparenz von Algorithmen herzustellen.

Weil Datenverarbeitungsprozesse zunehmend komplexer und für Betroffene intransparenter werden, kommt der Datenschutzaufsicht eine elementare Rolle zu. Ihre fachliche Expertise ist gefragt, sie muss organisatorisch und personell in der Lage sein, beratend und gestaltend tätig zu sein. Ein starkes Datenschutzrecht und effektive Aufsichtsbehörden vermindern gemeinsam die Risiken für die Bürgerinnen und

Bürger in der digitalen Gesellschaft. Sollten Facebook und andere soziale Netzwerke nicht bereit sein, den europäischen Rechtsvorschriften zum Schutz der Nutzenden nachzukommen, muss dies konsequent durch Ausschöpfung aller vorhandenen aufsichtsbehördlichen Instrumente auf nationaler und europäischer Ebene geahndet werden.

8.4 Die Zeit der Verantwortungslosigkeit ist vorbei: EuGH bestätigt gemeinsame Verantwortung von Facebook und Fanpage-Betreibern

Entschließung
der 2. Sonderkonferenz der unabhängigen Datenschutzbehörden
des Bundes und der Länder
am 6. Juni 2018 in Düsseldorf

Die unabhängigen Datenschutzbehörden des Bundes und der Länder begrüßen das Urteil des Europäischen Gerichtshofs (EuGH) vom 5. Juni 2018, das ihre langjährige Rechtsauffassung bestätigt.

Das Urteil des EuGH zur gemeinsamen Verantwortung von Facebook und den Betreibern einer Fanpage hat unmittelbare Auswirkungen auf die Seitenbetreiber. Diese können nicht mehr allein auf die datenschutzrechtliche Verantwortung von Facebook verweisen, sondern sind selbst mitverantwortlich für die Einhaltung des Datenschutzes gegenüber den Nutzenden ihrer Fanpage.

Dabei müssen sie die Verpflichtungen aus den aktuell geltenden Regelungen der Datenschutz-Grundverordnung (DS-GVO) beachten. Zwar nimmt das Urteil Bezug auf die frühere Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr, doch die vom EuGH festgestellte Mitverantwortung der Seitenbetreiber erstreckt sich auf das jeweils geltende Recht, insbesondere auf die in der DS-GVO festgeschriebenen Rechte der Betroffenen und Pflichten der Verarbeiter.

Im Einzelnen ist Folgendes zu beachten:

- 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 trackt, 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 DS-GVO erfüllt.

- Für die Bereiche der gemeinsamen Verantwortung von Facebook und Fanpage-Betreibern ist in einer Vereinbarung festzulegen, wer von ihnen welche Verpflichtung der DS-GVO erfüllt. Diese Vereinbarung muss in wesentlichen Punkten den Betroffenen zur Verfügung gestellt werden, damit diese ihre Betroffenenrechte wahrnehmen können.

Für die Durchsetzung der Datenschutzvorgaben bei einer Fanpage ist die Aufsichtsbehörde zuständig, die für das jeweilige Unternehmen oder die Behörde zuständig ist, die die Fanpage betreibt. Die Durchsetzung der Datenschutzvorgaben im Verantwortungsbereich von Facebook selbst obliegt primär der irischen Datenschutzaufsicht im Rahmen der europäischen Zusammenarbeit.

Die deutschen Aufsichtsbehörden weisen darauf hin, dass nach dem Urteil des EuGH dringender Handlungsbedarf für die Betreiber von Fanpages besteht. Dabei ist nicht zu verkennen, dass die Fanpage-Betreiber ihre datenschutzrechtliche Verantwortung nur erfüllen können, wenn Facebook selbst an der Lösung mitwirkt und ein datenschutzkonformes Produkt anbietet, das die Rechte der Betroffenen wahrt und einen ordnungsgemäßen Betrieb in Europa ermöglicht.

8.5 Der Vorschlag der EU-Kommission für eine E-Evidence-Verordnung führt zum Verlust von Betroffenenrechten und verschärft die Problematik der sog. Vorratsdatenspeicherung

Entschließung
der 96. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
am 7. November 2018

Mit ihrem Vorschlag für eine E-Evidence-Verordnung (Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (COM (2018) 225 final)) möchte die EU-Kommission eine Alternative zum förmlichen Rechtshilfeverfahren schaffen und den Ermittlungsbehörden einen schnelleren Zugang zu Kommunikationsdaten ermöglichen. Die Strafverfolgungsbehörden der EU-Mitgliedstaaten sollen die Befugnis erhalten, Anbieter von Telekommunikations-und Internetdienstleistungen in anderen Mitgliedstaaten der EU und auch in Staaten außerhalb der EU (Drittstaaten) unmittelbar zur Herausgabe von Bestands-, Zugangs-, Transaktions-und Inhaltsdaten zu verpflichten.
Die DSK weist hierzu auf die kritische Stellungnahme des Europäischen Datenschutzausschusses hin (https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-commission-proposals-european-production-and_de). Diese stellt bereits das Vorliegen einer Rechtsgrundlage in Frage. Mit Besorgnis sieht die DSK vor allem auch die vorgeschlagene Abkehr vom Grundsatz der doppelten bzw. beiderseitigen Strafbarkeit.
Erstmals im Bereich der internationalen Zusammenarbeit in Strafsachen soll die Herausgabe von Daten nicht mehr davon abhängig sein, ob die verfolgte Tat dort, wo die Daten ersucht werden, überhaupt strafbar ist. Im Ergebnis könnten Unternehmen mit Sitz in Deutschland also zur Herausgabe von Daten an Ermittlungsbehörden in anderen EU-Mitgliedstaaten verpflichtet werden, obwohl die verfolgte Tat in Deutschland überhaupt keine Straftat ist. Das könnte zum Beispiel ein in Deutschland erlaubter Schwangerschaftsabbruch sein oder eine politische Meinungsäußerung, wenn diese im ersuchenden Staat strafbewehrt ist.
Zu befürchten ist hierbei auch, dass Drittstaaten die Regelung der EU als Blaupause für eigene Regelungen heranziehen werden. Provider in

EU-Mitgliedstaaten würden sich dann vermehrt Herausgabeanordnungen von Drittstaaten ausgesetzt sehen, mit denen möglicherweise Straftaten aus einer völlig anderen Rechtstradition verfolgt werden.
Kritisch sieht die DSK auch, dass im Regelfall jegliche Information und Beteiligung der Justizbehörden des Staates, in dem der Provider seinen Sitz hat, unterbleibt und damit ein wichtiges verfahrensrechtliches Korrektiv fehlt. Ob die Rechtmäßigkeit eines Ersuchens überprüft wird, hängt im vorgeschlagenen Verfahren ausschließlich vom Verhalten der Provider ab. Nur wenn sich das Unternehmen weigert, Daten zu übermitteln, muss der ersuchende Staat bei den Behörden vor Ort um Vollstreckungshilfe bitten. Nur dann können diese noch in das Verfahren eingreifen. Werden Daten herausgegeben, erlangen die zuständigen Justizbehörden hiervon jedoch keine Kenntnis. Der Vorschlag sieht keine Informationspflicht gegenüber den Behörden am Sitz des Unternehmens vor. Provider verfolgen aber in der Regel wirtschaftliche Interessen und unterliegen in ihren Entscheidungen anderen Verpflichtungen als die Justizbehörden Hierdurch werden Betroffene deutlich schlechter gestellt.
Provider als Adressaten eines Ersuchens sehen sich künftig nicht mehr den Justizbehörden des eigenen Staates gegenüber, sondern müssen sich mit den Behörden des anordnenden Staates auseinandersetzen. Den Betroffenen wiederum steht, wenn überhaupt, nur ein Rechtsbehelf im ersuchenden Mitgliedsstaat zu, dessen Rechtsordnung ihnen in der Regel aber fremd ist.
Ein besonderes Verfahren ist vorgesehen, wenn sich Provider mit Sitz in Drittstaaten darauf berufen, dass die angeordnete Übermittlung gegen das dortige Recht verstößt. Für diesen Fall sieht der Vorschlag eine gerichtliche Überprüfung im anordnenden Staat vor. Wenn das Gericht zu der Auffassung gelangt, dass tatsächlich ein Rechtskonflikt vorliegt, muss es die zuständigen Behörden im Zielstaat der Anordnung beteiligen. Das Ergebnis der Konsultation ist für das Gericht verbindlich. Diese Regelung ist ausdrücklich zu begrüßen. Denn auch hier wird eine Blaupause geschaffen für die Frage, welche Rechte europäische Unternehmen in der umgekehrten Situation haben sollten, wenn sie aus Drittstaaten auf der Grundlage von deren Gesetzen (wie z. B. US-Cloud-Act) zu einer Übermittlung verpflichtet werden und welche Verbindlichkeit eine Konsultation der zuständigen Behörden in Europa für Gerichte in Drittstaaten haben sollte.
Besonders kritisch ist jedoch, dass in Deutschland Telekommunikationsdienstleister verpflichtet sind, u. a. sämtliche Verkehrsdaten für

zehn Wochen zu speichern. Aus diesen Daten lassen sich genaue Schlüsse auf das Privatleben der Betroffenen, insbesondere deren Kontakt- und Interessenprofil ziehen. Die Problematik dieser sog. Vorratsdatenspeicherung verschärft sich deutlich, wenn ausländische Strafverfolgungsbehörden einen direkten Zugriff auf derartige Informationen erhalten.
Die DSK appelliert daher an alle im Gesetzgebungsverfahren Beteiligten, den Vorschlag für eine E-Evidence-Verordnung zu stoppen!

8.6 Übermittlung von E-Mail-Adressen durch Onlineversandhändler an Postdienstleister

Beschluss
der Datenschutzkonferenz vom 23. März 2018

Die Übermittlung von E-Mail-Adressen durch Onlinehändler an Postdienstleister ist nur bei Vorliegen einer Einwilligung der Kunden in eben diese Übermittlung rechtmäßig. Die Praxis hat gezeigt, dass es vielen Onlinehändlern möglich ist, die Zustellinformationen selbst an den Kunden weiterzugeben bzw. einen Link zur Sendungsverfolgung in die eigene Bestellbestätigung einzubinden. Dies stellt jedenfalls eine objektiv zumutbare Alternative dar. Aus dem gleichen Grund wird auch die Erforderlichkeit im Rahmen des§ 28 Abs. 1 Satz 1 Nr. 2 Bundesdatenschutzgesetz bzw. Art. 6 Abs. 1 Satz 1 lit. f Datenschutz-Grundverordnung verneint.

8.7 Mahnung durch Computeranruf

Beschluss
der Datenschutzkonferenz am 23. März 2018

Eine telefonische Mahnung durch Computeranruf ist wegen der hohen Gefahr, dass eine andere als die betroffene Person die Nachricht erhält und so personenbezogene Daten unbefugt offenbart werden, unzulässig.

8.8 Kontaktloses Bezahlen

Beschluss
der Datenschutzkonferenz am 23. März 2018

Kontaktloses Bezahlen ist derzeit in vielen Varianten möglich. Der zugrunde liegende Übertragungsstandard Near Field Communication (NFC) wird für Geld- und Kreditkarten sowie für mobiles Bezahlen z. B. mit dem Smartphone genutzt. Die Datenschutzaufsichtsbehörden begleiten die Entwicklung aus datenschutzrechtlicher und -technischer Sicht. So wurde bereits im Beschluss des Düsseldorfer Kreises vom 19. September 2012 zu „Near Field Communication (NFC) bei Geldkarten“ auf die datenschutzrechtlichen Grundanforderungen hingewiesen. Mittlerweile sind die Verantwortlichen vielen dieser Forderungen nachgekommen bzw. mit deren Umsetzung befasst.

Die grundsätzlichen Forderungen bezüglich kontaktloser Bezahlverfahren lassen sich wie folgt zusammenfassen:

Notwendigkeit einer Datenschutz-Folgenabschätzung ist nach Art. 35 DS-GVO zu prüfen.

Die Karten ausgebenden Institute sind verpflichtet, umfassende und verständliche Informationen für Nutzerinnen und Nutzer über Datenhaltung und -verarbeitung bereitzustellen. Bei Bezahlverfahren, die ein Smartphone voraussetzen, ist weiterhin über die damit einhergehenden besonderen Risiken zu informieren. Zudem sind Hinweise zur Risikominimierung zu geben.

Die Kundinnen und Kunden sind darüber zu unterrichten, dass eine kostenlose Schutzhülle in der Standardversion zur Verfügung steht.

Es muss sichergestellt sein, dass durch Voreinstellung die NFC-Funktion zunächst deaktiviert ist. Den Kundinnen und Kunden muss ermöglicht werden, die NFC-Funktion jederzeit abschalten zu können. Alternativ können auch Karten ohne NFC-Funktion angeboten werden, ohne dass für Kundinnen und Kunden Mehrkosten entstehen.

Um das unberechtigte Auslesen etwaiger personenbeziehbarer Daten zu verhindern, ist die drahtlose Kommunikation zwischen (virtueller)

Karte und Terminal zu verschlüsseln. Die (Kredit-)Wirtschaft wird aufgefordert, die zurzeit laufenden Arbeiten an einer internationalen Spezifikation der Verschlüsselung weiterhin zu forcieren. Auch bleiben weitere Maßnahmen zur technisch-organisatorischen Absicherung von NFC-basierten Konzepten – wie z. B. die Randomisierung der Kartennummer – fortgesetzt aktuell.

Es sollte grundsätzlich keine Möglichkeit des kontaktlosen Auslesens einer wiederkehrenden Kennziffer (z. B. Kartennummer) möglich sein, die unter Umständen zu Zwecken der Profilbildung herangezogen werden kann.

Bei Bezahlverfahren, die ein Smartphone voraussetzen, ist die Bezahl-App von den ausgebenden Kreditinstituten aktuell zu halten. Die Kundinnen und Kunden sind dazu anzuhalten, nur die aktuellen Software- und Betriebssystemversionen einzusetzen. Bei nicht aktualisierten Software- und Betriebssystemversionen ist mindestens kontinuierlich und unübersehbar darauf hinzuweisen, wenn die Anwendungen zu Sicherheitsrisiken führen.

Die Karten ausgebenden Institute werden darauf hingewiesen, dass etwaige auf der Karte vorhandene Drittanwendungen, die geeignet sind, das Pseudonymisierungskonzept des Bezahlsystems zu unterlaufen, eine neue datenschutzrechtliche Bewertung erforderlich machen. Zudem sind die Drittanbieter darauf hinzuweisen, dass und wie eine mögliche Depseudonymisierung infolge unsachgemäßer Belegung von Datenfeldern zu vermeiden ist.

8.9 Einmeldung offener und unbestrittener Forderungen in eine Wirtschaftsauskunftei unter Geltung der DS-GVO

Beschluss
der Datenschutzkonferenz am 23. März 2018

Die Zulässigkeit einer Einmeldung beurteilt sich künftig nach Art. 6 Abs. 1 S. 1 lit. f Datenschutz-Grundverordnung (DS-GVO).

Hierzu ist es notwendig, dass die Einmeldung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Zudem dürfen die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen. Das bedeutet, dass eine Abwägung unter Berücksichtigung dieser Kriterien im Einzelfall vorzunehmen ist.

Im Rahmen dieser Einzelfallprüfung entfalten die nachfolgenden Fallgruppen eine Indizwirkung für eine zulässige Einmeldung:

1. Die Forderung ist durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden oder es liegt ein Schuldtitel nach § 794 der Zivilprozessordnung vor.
2. Die Forderung ist nach § 178 der Insolvenzordnung festgestellt und nicht vom Schuldner im Prüfungstermin bestritten worden.
3. Der Betroffene hat die Forderung ausdrücklich anerkannt.
4. Der Betroffene ist nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden, die erste Mahnung liegt mindestens vier Wochen zurück, der Betroffene ist zuvor, jedoch frühestens bei der ersten Mahnung, über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet worden und der Betroffene hat die Forderung nicht bestritten.
5. Das der Forderung zugrunde liegende Vertragsverhältnis kann aufgrund von Zahlungsrückständen fristlos gekündigt werden und der Betroffene ist zuvor über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet worden.

Zusätzliche Anhaltspunkte oder Hinweise können ggf. zu einer anderen Abwägung führen.

Darüber hinaus muss eine Kompatibilitätsprüfung nach Art. 6 Abs. 4 DS-GVO erfolgen, weil die personenbezogenen Daten zunächst für einen anderen Zweck – zur Durchführung eines Rechtsgeschäfts und nicht zur Einmeldung bei einer Auskunftei – verarbeitet wurden. Der Betroffene muss also zuvor durch die Auskunftei-Vertragspartner über die Möglichkeit der Einmeldung unterrichtet worden sein, denn es darf nur das eingemeldet werden, womit der Betroffene vernünftigerweise rechnen muss (Erwägungsgrund 47 der DS-GVO).

8.10 Keine fortlaufenden Bonitätsauskünfte an den Versandhandel

Beschluss
der Datenschutzkonferenz vom 23. März 2018

Auskunfteien dürfen Bonitätsauskünfte gemäß Art. 6 Abs. 1 S. 1 lit. f Datenschutz-Grundverordnung (DS-GVO) grundsätzlich nur erteilen, wenn es zur Wahrung eines berechtigten Interesses eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.
Besteht zwischen diesem Dritten (also dem anfragenden Unternehmen) und dem Betroffenen ein Dauerschuldverhältnis, aufgrund dessen das anfragende Unternehmen während der gesamten Dauer des Bestehens ein finanzielles Ausfallrisiko trägt (z. B. Ratenzahlungskredit, Girokonto, Energielieferungs-, Telekommunikationsvertrag), so dürfen Bonitätsauskünfte nicht nur zu dem Zeitpunkt erteilt werden, zu dem der Betroffene ein solches Vertragsverhältnis beantragt hat, sondern während der gesamten Laufzeit des Vertragsverhältnisses und bis zur Erfüllung sämtlicher Pflichten des Betroffenen. Bei jeder dieser weiteren Auskünfte sind jedoch im Einzelfall die Voraussetzungen des Art. 6 Abs. 1 S. 1 lit. f DS-GVO strikt zu beachten. Das heißt vor jeder Übermittlung sind die konkreten berechtigten Interessen des Dritten gegen die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person abzuwägen.
Ein Versandhandelsgeschäft stellt als solches kein Dauerschuldverhältnis dar. Die aufgrund der bisherigen Erfahrungen mit den Kunden möglicherweise bestehende Wahrscheinlichkeit und darauf gegründete Erwartung, dass der Kunde nach der ersten Bestellung wiederholt bestellen wird, und die zur Erleichterung der Bestellvorgänge möglicherweise erfolgte Einrichtung eines „Kundenkontos“ rechtfertigten es nicht, ein Versandhandelsgeschäft mit einem Dauerschuldverhältnis gleichzusetzen.
Ein berechtigtes Interesse seitens des Versandhandels gemäß Art. 6 Abs. 1 S. 1 lit. f DS-GVO ist demnach nur gegeben, wenn aufgrund eines konkreten Bestellvorgangs ein finanzielles Ausfallrisiko vorliegt.
Nach Vertragsschluss sind Bonitätsauskünfte an Versandhändler dann nicht zu beanstanden, wenn ein Ratenzahlungskredit vereinbart wurde

oder noch ein offener Saldo besteht. In allen anderen Fällen ist das Rechtsgeschäft nach Abwicklung des einzelnen Kaufgeschäftes für den Versandhandel abgeschlossen, ein berechtigtes Interesse an Bonitätsauskünften ist dann nicht mehr zu belegen. Damit sind Nachmeldungen oder sonstige Beauskunftungen in dieser Konstellation rechtlich unzulässig.

8.11 Aufzeichnung von Telefongesprächen

Beschluss
der Datenschutzkonferenz vom 23. März 2018

Die Aufzeichnung von Telefongesprächen ist datenschutzrechtlich in aller Regel nur mit Einwilligung auch des externen Gesprächspartners zulässig. Eine datenschutzrechtlich wirksame Einwilligung im Sinne von Art. 4 Nr. 11 Datenschutz-Grundverordnung (DS-GVO) setzt voraus, dass der externe Gesprächspartner vor Beginn der beabsichtigten Aufzeichnung gefragt wird, ob er mit der Aufzeichnung einverstanden ist, und falls er einverstanden ist, gebeten wird, sein Einverständnis beispielsweise durch Aussprechen eines „Ja“ oder durch eine aktive bestätigende Handlung (etwa durch das Betätigen einer Telefontaste) eindeutig zum Ausdruck zu bringen. Diese Einwilligung umfasst nicht eine biometrische Auswertung. Die bloße Einräumung einer Widerspruchsmöglichkeit und das anschließende Fortsetzen des Telefonats stellen keine datenschutzrechtlich wirksame Einwilligung im Sinne der DS-GVO dar. Da der datenschutzrechtlich Verantwortliche nachweisen können muss, dass die betroffene Person eine wirksame Einwilligung erteilt hat (Art. 7 Abs. 1 DS-GVO), muss er auch nachweisen können, dass die betroffene Person die Einwilligung „in informierter Weise“ abgegeben hat (vgl. Art. 4 Nr. 11 DS-GVO).

Die Aufzeichnung betrifft regelmäßig auch Beschäftigte. Insoweit gelten besondere Anforderungen. Sie sind nicht Gegenstand dieses Beschlusses.

8.12 Datenschutzbeauftragten-Bestellpflicht nach Artikel 37 Abs. 1 lit. C Datenschutz-Grundverordnung bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs

Beschluss
der Datenschutzkonferenz vom 26. April 2018

1. Betreibt ein einzelner Arzt, Apotheker oder sonstiger Angehöriger eines Gesundheitsberufs eine Praxis, Apotheke oder ein Gesundheitsberufsunternehmen und sind dort einschließlich seiner Person in der Regel mindestens 10 Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt, besteht eine gesetzliche Verpflichtung zur Benennung eines Datenschutzbeauftragten (DSB).

2. Bei Ärzten, Apothekern oder sonstigen Angehörigen eines Gesundheitsberufs, die zu mehreren in einer Berufsausübungsgemeinschaft (Praxisgemeinschaft) bzw. Gemeinschaftspraxis zusammengeschlossen sind oder die ihrerseits weitere Ärzte, Apotheker bzw. sonstige Angehörige eines Gesundheitsberufs beschäftigt haben, ist in der Regel nicht von einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten im Sinne von Art. 37 Abs. 1 lit. c Datenschutz-Grundverordnung (DS-GVO) auszugehen – in diesen Fällen ist unter Berücksichtigung von Punkt 3 dann kein DSB zu benennen, wenn weniger als 10 Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind.

3. Bei Ärzten, Apothekern oder sonstigen Angehörigen eines Gesundheitsberufs, die zu mehreren in einer Berufsausübungsgemeinschaft (Praxisgemeinschaft) bzw. zusammengeschlossen sind oder die ihrerseits weitere Ärzte, Apotheker bzw. sonstige Angehörige eines Gesundheitsberufs beschäftigt haben, bei denen ein hohes Risiko für die Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten zu erwarten ist, ist eine Datenschutzfolgenabschätzung vorgeschrieben und damit zwingend ein Datenschutzbeauftragter

zu benennen. Dies kann neben einer umfangreichen Verarbeitung (z. B. große Praxisgemeinschaften), die ohnehin nach Art. 37 Abs. 1 lit. c DS-GVO zu einer Benennungspflicht führt, beispielsweise beim Einsatz von neuen Technologien, die ein hohes Risiko mit sich bringen, der Fall sein. Der Datenschutzbeauftragte ist damit auch dann zu benennen, wenn weniger als 10 Personen ständig mit der Verarbeitung personenbezogener Daten zu tun haben.

4. Der Begriff „Gesundheitsberuf“ ist im Sinne der Aufzählung nach § 203 Abs. 1 Strafgesetzbuch (StGB) auszulegen und umfasst die in § 203 Abs. 1 Nr. 1, 2, 4 und 5 StGB aufgezählten Berufsbilder.

8.13 Verarbeitung von Positivdaten zu Privatpersonen durch Auskunfteien

Beschluss
der Datenschutzkonferenz vom 11. Juni 2018

Handels- und Wirtschaftsauskunfteien können sog. Positivdaten zu Privatpersonen grundsätzlich nicht auf Grundlage des Art. 6 Abs. 1 lit. f Datenschutz-Grundverordnung (DS-GVO) erheben. Denn bei Positivdaten – das sind Informationen, die keine negativen Zahlungserfahrungen oder sonstiges nicht vertragsgemäßes Verhalten zum Inhalt haben – überwiegt regelmäßig das schutzwürdige Interesse der betroffenen Personen, selbst über die Verwendung ihrer Daten zu bestimmen. Werden die Daten von einem Verantwortlichen an eine Auskunftei übermittelt, ist insoweit bereits die Übermittlung dieser Datennach Art. 6 Abs. 1 S. 1 lit. f DS-GVO regelmäßig unzulässig.

Will eine Auskunftei Positivdaten zu Privatpersonen erheben, bedarf es dafür im Regelfall einer wirksamen Einwilligung der betroffenen Personen im Sinne des Art. 7 DS-GVO. Auf die hohen Anforderungen an die Freiwilligkeit nach Art. 7 Abs. 4 DS-GVO wird hingewiesen. Sofern die Auskunftei oder ihre Vertragspartner zu diesem Zweck eine für eine Vielzahl von Fällen vorformulierte Einwilligungsklausel verwenden, die als Allgemeine Geschäftsbedingung im Sinne des § 305 Bürgerliches Gesetzbuch (BGB) zu werten ist, muss eine entsprechende Einwilligung darüber hinaus den Anforderungen des § 307 BGB genügen.

Besonderheiten für Kreditinstitute:

Es wird für zulässig angesehen, wenn Kreditinstitute aufgrund von Art. 6 Abs. 1 S. 1 lit. f DS-GVO – wie bisher durch § 28a Abs. 2 Bundesdatenschutzgesetz gesetzlich erlaubt – personenbezogene Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung von Kredit- und Giroverträgen sowie Garantiegeschäften (insbesondere Bürgschaften) an Auskunfteien übermitteln, es sei denn, dass im Einzelfall das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Übermittlung gegenüber den Interessen der Auskunftei an der Kenntnis der Daten offensichtlich überwiegt.

Diese Besonderheit für Kreditinstitute begründet sich mit den speziellen Bonitätsprüfungsverpflichtungen der Kreditinstitute nach dem Kreditwesengesetz sowie gesamtgesellschaftlichen Gesichtspunkten des Schutzes der betroffenen Personen vor Überschuldung. Die betroffene Person ist vor Abschluss des Vertrages über die damit verbundene Datenübermittlung an Auskunfteien zu unterrichten.

Dies gilt nicht für Giroverträge, die die Einrichtung eines Kontos ohne Überziehungsmöglichkeit zum Gegenstand haben.

Ebenso ist die Übermittlung von Daten zu allgemeinen Konditionenanfragen, die der Herstellung von Markttransparenz dienen, an Auskunfteien unzulässig; hierzu kann auch keine rechtswirksame Einwilligung der betroffenen Person eingeholt werden.

Die Übermittlung von Daten an Auskunfteien für Bonitätsabfragen ist nach Art. 6 Abs. 1 S. 1 lit. b DS-GVO zulässig, wenn dies zur Durchführung eines Beratungsvertrages oder einer vorvertraglichen Maßnahme, die auf Anfrage der betroffenen Person erfolgt, erforderlich ist mit dem Ziel, Konditionen, die auf eine bestimmte Person zugeschnittenen werden, zu überprüfen.

Nachträgliche Änderungen von Tatsachen hat das Kreditinstitut gemäß Art. 19 DS-GVO der Auskunftei unverzüglich nach Kenntniserlangung mitzuteilen, solange die ursprünglich übermittelten Daten bei der Auskunftei gespeichert sind. Die Auskunftei hat das betreffende Kreditinstitut über die Löschung der ursprünglich übermittelten Daten zu unterrichten.

Zur Einmeldung von Dauerschuldverhältnissen außerhalb des KWG werden im AK Auskunfteien noch weitere Abstimmungen erfolgen.

8.14 Geschäftsordnung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz)

Beschluss
der Datenschutzkonferenz vom 5. September 2018[3]

A. Zweck, Aufgaben und Arbeitsweise der Datenschutzkonferenz

I. Zusammensetzung der Datenschutzkonferenz

Die Datenschutzkonferenz (DSK) ist der Zusammenschluss der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder und besteht aus der oder dem Bundesbeauftragten für den Datenschutz, den Landesbeauftragten für den Datenschutz und der Präsidentin oder dem Präsidenten des Bayerischen Landesamtes für Datenschutzaufsicht (Mitglieder der DSK).
Die Mitglieder der DSK können sich in den Sitzungen der DSK durch eine Mitarbeiterin oder einen Mitarbeiter ihrer Dienststelle vertreten lassen. Ein anderes Mitglied kann durch Stimmrechtsübertragung zur Vertreterin oder zum Vertreter bestellt werden.

II. Zweck der Datenschutzkonferenz

Die DSK hat das Ziel, die Datenschutzgrundrechte zu wahren und zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten.

III. Aufgaben der Datenschutzkonferenz

Die DSK fördert den Datenschutz und verständigt sich auf gemeinsame Positionen der Datenschutzaufsichtsbehörden des Bundes und der Länder.

[3] Beschluss zu TOP 9 der 4. Sonderkonferenz am 5.September 2018 in Düsseldorf.

Dies geschieht namentlich durch Entschließungen, Beschlüsse, Orientierungshilfen, Standardisierungen, Stellungnahmen, Pressemitteilungen und Festlegungen.

- Entschließungen sind öffentliche Stellungnahmen zu datenschutzpolitischen Fragen.
- Beschlüsse sind Positionen, die die Auslegung datenschutzrechtlicher Regelungen bzw. entsprechende Empfehlungen betreffen.
- Orientierungshilfen und Standardisierungen sind fachliche Anwendungshilfen für Verantwortliche, Auftragsverarbeiter, Herstellerinnen und Hersteller und die Öffentlichkeit.
- Stellungnahmen sind Positionen, die u. a. in gerichtlichen Verfahren oder Gesetzgebungsverfahren abgegeben werden.
- Pressemitteilungen sind Verlautbarungen für die Medien und die Öffentlichkeit.
- Festlegungen sind Positionen zu internen inhaltlichen, technischen oder organisatorischen Fragen einschließlich der Gremienarbeit.

IV. Arbeitsweise der Datenschutzkonferenz

1. Vorsitz der Datenschutzkonferenz

Ein Mitglied der Konferenz führt den Vorsitz. Der Vorsitz wechselt in alphabetischer Reihenfolge der Länder. Der Bund steht am Beginn der Reihenfolge. Die Konferenz kann jederzeit Abweichungen von der Reihenfolge beschließen. Die Amtszeit des Vorsitzes beginnt am 1. Januar und endet am 31. Dezember eines Jahres.
Der Vorsitz richtet die Sitzungen der DSK aus und stellt hierfür die Tagesordnung auf. Er leitet die Sitzungen, veranlasst

die Umsetzung der Arbeitsergebnisse und vertritt die Konferenz nach außen.

2. Sitzungen der Datenschutzkonferenz

Die DSK tagt regulär zweimal im Jahr. Weitere ordentliche Sitzungen sind möglich.
Aus konkretem Anlass können ferner Sonderkonferenzen einberufen werden.
Eine Sitzung ist einzuberufen, wenn dies mehr als die Hälfte der Mitglieder verlangt.
Die DSK ist in einer Sitzung beschlussfähig, wenn mehr als die Hälfte der Stimmberechtigten vertreten ist.
Die Sitzungen der DSK sind nicht öffentlich, soweit die DSK nichts anderes beschließt. Soweit kein Mitglied der DSK Einwände erhebt, können zu einzelnen Tagesordnungspunkten Dritte eingeladen werden.
Zur Vorbereitung und Vorbesprechung der ordentlichen Sitzungen kann vorher die Vorkonferenz der Stellvertreterinnen und Stellvertreter bzw. der oder des mit der Vertretung beauftragten Mitarbeiterin oder Mitarbeiters stattfinden. Die Leitung der Vorkonferenz obliegt dem jeweiligen Vorsitzland.
Aufgabe der Vorkonferenz ist es, zu den jeweiligen Tagesordnungspunkten der ordentlichen Sitzung vorbereitend Einvernehmen zu erzielen, hilfsweise alternative Fassungen zu erarbeiten. Tagesordnungspunkte, über die auf der Vorkonferenz Einvernehmen erzielt wurde, werden in der Sitzung der DSK in einem verkürzten Verfahren, d. h. in der Regel ohne Aussprache, zur Abstimmung gebracht.
Der Vorsitz lädt die Mitglieder der DSK spätestens zwei Monate vor der ordentlichen Sitzung ein. Zugleich wird der Termin der Vorkonferenz mitgeteilt. Die Mitglieder können bis vier Wochen vor der Sitzung Tagesordnungspunkte anmelden. Spätestens drei Wochen vor der Sitzung ist den Mitgliedern die endgültige Tagesordnung für die Sitzung der DSK zuzuleiten. Nicht fristgerecht angemeldete Tagesordnungspunkte werden nur dann behandelt, wenn eine besondere Dringlichkeit gegeben ist. Die Dringlichkeit ist zu begrün-

den. Die Entscheidung über die Aufnahme eines nicht fristgerecht angemeldeten Tagesordnungspunktes trifft die Konferenz. Wird die Verspätung der Anmeldung nicht begründet, gilt diese als nicht erfolgt. Für Sonderkonferenzen kann der Vorsitz abweichende Fristen festsetzen.
Die Anmeldung eines Tagesordnungspunktes muss eine Darstellung des Beratungsgegenstandes, ein Beratungsziel bzw. einen Entscheidungsvorschlag und ggfs. einzuladende Dritte enthalten.
An den Sitzungen der DSK nimmt eine Vertreterin bzw. ein Vertreter der ZASt regelmäßig teil.

3. Abstimmungen der Datenschutzkonferenz

Zur Erreichung gemeinsamer Positionen strebt die Konferenz Einvernehmen an.
Bei Abstimmungen gilt die einfache Mehrheit der abgegebenen Stimmen, sofern nicht gesetzlich oder in dieser Geschäftsordnung etwas anderes geregelt ist. Enthaltungen werden nicht mitgezählt.
Entschließungen verabschiedet die Konferenz grundsätzlich mit einer Mehrheit von mindestens 12 Stimmen (2/3). Entschließungen, die sich auf einen Gegenstand beziehen, bei dem eine individuell-konkrete Betroffenheit eines Mitglieds besteht, dürfen nicht gegen die Stimme dieses Mitglieds verabschiedet werden.
Abstimmungen mit finanziellen Auswirkungen auf die Haushalte der Aufsichtsbehörden haben keine Bindungswirkung gegenüber den Mitgliedern der DSK, die gegen den Sachverhalt gestimmt haben.
Bei Abstimmungen haben jedes Land sowie der Bund jeweils eine Stimme.
Bei Mehrheitsentscheidungen zu gemeinsamen Positionen werden auf Wunsch abweichende Voten durch die Bezeichnung des jeweiligen Mitglieds der Konferenz in dem zur Veröffentlichung bestimmten Dokument kenntlich gemacht.

4. Protokoll

Von jeder Sitzung der Konferenz ist ein Ergebnisprotokoll zu fertigen.
Bei Mehrheitsentscheidungen werden Abstimmungsergebnisse im Protokoll durch die Bezeichnung des jeweiligen Mitglieds der Konferenz dargestellt, es sei denn, ein Mitglied widerspricht. Der Entwurf dieses Protokoll ist innerhalb von drei Wochen allen Mitgliedern zuzuleiten. Einwendungen gegen den Entwurf sind innerhalb von drei Wochen nach Zuleitung des Entwurfs geltend zu machen. Nach Ablauf dieser Frist wird über den endgültigen Entwurf in einem schriftlichen Umlaufverfahren abgestimmt.
Diese Protokolle werden nach erfolgtem Umlaufverfahren grundsätzlich veröffentlicht. Über Ausnahmen beschließt die DSK mit einfacher Mehrheit.

5. Umlaufverfahren

Zwischen den Sitzungen der DSK können gemeinsame Positionen nach Abschnitt A.III. im Umlaufverfahren herbeigeführt werden. Das Verfahren wird durch den Vorsitz eingeleitet.
Ein Umlaufverfahren ist einzuleiten, wenn ein Mitglied der DSK dies beantragt und einen entsprechenden Beschlussvorschlag vorlegt. Für die Kommentierung der Entwürfe im Umlaufverfahren sind angemessene Fristen zu setzen. Im Abstimmungsverfahren gilt die Nichtäußerung (Schweigen) auf einen Entwurf als Enthaltung. Der Vorsitz stellt das Ergebnis der Abstimmung fest und teilt dieses den Mitgliedern der DSK mit.
Es gelten im Übrigen die Abstimmungsmodalitäten der Konferenz.

6. Veröffentlichungen der Datenschutzkonferenz

Entschließungen, Orientierungshilfen, Standardisierungen, Pressemitteilungen und für die Öffentlichkeit bestimmte Beschlüsse und Stellungnahmen sowie Protokolle von Sitzun-

gen der DSK werden auf der Homepage der DSK veröffentlicht und können zusätzlich auf den Webseiten der Mitglieder veröffentlicht werden.

B. Arbeitskreise der Datenschutzkonferenz

I. Errichtung und Besetzung von Arbeitskreisen

Die DSK richtet zur Unterstützung ihrer Arbeit Arbeitskreise ein. Alle Datenschutzaufsichtsbehörden sind zur Mitarbeit in den Arbeitskreisen eingeladen.
Die inhaltliche Ausrichtung der Arbeitskreise orientiert sich an den Expertengruppen des Europäischen Datenschutzausschusses. Die Einrichtung weiterer Arbeitskreise ist möglich.
Die DSK entscheidet über den Arbeitskreisvorsitz. Die Beauftragung mit dem Vorsitz erfolgt für die Dauer von vier Jahren und kann verlängert werden. Bei der Beauftragung werden möglichst alle Aufsichtsbehörden gleichmäßig einbezogen.
Die DSK kann für einzelne Arbeitsthemen temporäre Arbeitskreise einrichten.
Der Vorsitz der DSK pflegt eine Übersicht über die Arbeitskreise der DSK und deren Vorsitz.

II. Aufgaben und Arbeitsweise der Arbeitskreise

Die Arbeitskreise arbeiten der DSK zu. Sie bereiten deren Entscheidungen vor. Die DSK kann die Arbeitskreise mit der Vorbereitung von Positionsbestimmungen beauftragen.
Die Arbeitskreise tagen in der Regel so rechtzeitig vor der ordentlichen Sitzung, dass die Ergebnisse ihrer Beratungen fristgerecht in die DSK eingebracht werden können. Ihre Sitzungen sind nicht öffentlich. Über die Teilnahme Dritter an den Sitzungen entscheidet der jeweilige Arbeitskreis.
Bei Abstimmungen gilt die einfache Mehrheit der abgegebenen Stimmen. Enthaltungen werden nicht mitgezählt.
Jeder Arbeitskreis soll innerhalb von zwei Wochen ein Ergebnisprotokoll erstellen, das die wesentlichen Aspekte der Diskussion enthält. Die Protokolle werden nicht veröffentlicht. Der Entwurf des Protokolls ist allen Mitgliedern des

Arbeitskreises zuzuleiten. Einwendungen können von den teilnehmenden Mitgliedern innerhalb von einer Woche geltend gemacht werden. Die Protokolle werden anschließend allen Mitgliedern der DSK zur Verfügung gestellt.
Die Arbeitskreise können für einzelne Themen Unterarbeitskreise einrichten.

C. Mitwirkung in Europäischen Gremien

I. Arbeitsgruppen des Europäischen Datenschutzausschusses (Expertengruppen)

In den Expertengruppen repräsentieren die Vertreterinnen und Vertreter des Bundes und der Länder gemeinsam die deutsche Position und wirken darauf hin, dass Themen von grundsätzlicher Bedeutung auf europäischer Ebene eingebracht werden.

II. Besetzung der Expertengruppen

Die Aufsichtsbehörden des Bundes und der Länder werden in den Expertengruppen jeweils durch eine Vertreterin oder einen Vertreter der oder des Bundesbeauftragten und eine Vertreterin oder einen Vertreter der Aufsichtsbehörden der Länder (Ländervertreter) repräsentiert. Eine weitere Vertreterin oder ein weiterer Vertreter der Aufsichtsbehörden der Länder wird jeweils als Stellvertreterin oder Stellvertreter des Ländervertreters bestimmt. Die Stellvertreterin oder der Stellvertreter beteiligt sich ständig an den Arbeiten der Expertengruppe und nimmt regelmäßig an ihren Sitzungen teil. Bei Bedarf können die Aufsichtsbehörden in Absprache mit den Vertreterinnen und Vertretern weitere Teilnehmerinnen und Teilnehmer fallweise zu den Sitzungen der Expertengruppen entsenden.
Die Aufsichtsbehörden der Länder bestimmen in entsprechender Anwendung des in Abschnitt A. IV. 3 geregelten Verfahrens, welche Aufsichtsbehörden der Länder den Ländervertreter und dessen Stellvertreterin oder Stellvertreter in die jeweiligen Expertengruppen entsenden. Abschnitt B. I., 3. Absatz gilt entsprechend

III. Aufgaben & Arbeitsweise

Die Vertreterinnen und Vertreter informieren über die inhaltlichen Entwicklungen in den Expertengruppen, insbesondere erstellen sie über die Sitzungen einen gemeinsamen Bericht und teilen Themen und Eckpunkte frühzeitig mit. Beiträge, Rückmeldungen oder Einwände werden den Vertreterinnen und Vertretern sowie allen Aufsichtsbehörden unverzüglich zugeleitet.
Darüber hinaus soll mindestens eine Vertreterin oder ein Vertreter bei den Sitzungen des jeweilig fachlich zugeordneten Arbeitskreises der DSK bei Bedarf anwesend sein und dort über die Arbeit der Expertengruppe berichten. Die vorgenannten Arbeitskreise unterstützen die Vertreterinnen oder Vertreter und informieren sie über relevante Positionen der Aufsichtsbehörden des Bundes und der Länder zu den jeweiligen Sachthemen. Die Vertreterinnen und Vertreter wirken auf ein einheitliches Meinungsbild hin.
Unbeschadet der Voraussetzungen nach § 18 BDSG kann eine Aufsichtsbehörde die Einholung eines gemeinsamen Standpunktes bei der zentralen Anlaufstelle initiieren, wenn sie dies für geboten hält.
In der Expertengruppe sind die Vertreterinnen und Vertreter an gemeinsame Standpunkte nach § 18 BDSG gebunden. Gemeinsame Positionen nach Abschnitt A. III. sind zu beachten. Gibt es keinen gemeinsamen Standpunkt nach § 18 BDSG und keine gemeinsame Position nach Abschnitt A. III. bilden die von den Aufsichtsbehörden mitgeteilten Positionen nach Abschnitt C. III., Absätze 1 und 2 die Grundlage für die Meinungsäußerungen in der Expertengruppe. Dabei werden neben der Mehrheitsmeinung auch abweichende Auffassungen aufgenommen und als solche dargestellt.
In der Sitzung selbst stimmen sich die anwesenden Vertreterinnen und Vertreter erforderlichenfalls ad-hoc ab. Kann auf diesem Wege kein Einvernehmen hergestellt werden, verhalten sich die deutschen Vertreterinnen und Vertreter zunächst neutral und leiten eine Klärung der Frage in die Wege.

Für sonstige Gremien des Europäischen Datenschutzausschusses gelten die Regularien unter Abschnitt C. II. und III. entsprechend.

D. Änderung der Geschäftsordnung

Die Regelungen in den Abschnitten

- A.IV.2, letzter Satz,
- A.IV.3,
- A.IV.5,
- C.I und
- C.II.1. Absatz

dieser Geschäftsordnung können nur durch einstimmigen Beschluss der Konferenz geändert werden. Im Übrigen bedarf es für die Änderung dieser Geschäftsordnung einer Mehrheit von 2/3 der Stimmberechtigten.

8.15 Ablehnung der Behandlung durch Ärztinnen und Ärzte bei Weigerung der Patientin oder des Patienten, die Kenntnisnahme der Informationen nach Art. 13 DS-GVO durch Unterschrift zu bestätigen

Beschluss
der Datenschutzkonferenz vom 5. September 2018

Die Datenschutzaufsichtsbehörden des Bundes und der Länder sprechen sich dagegen aus, dass Ärztinnen und Ärzte oder andere Angehörige von Gesundheitsberufen die Behandlung ablehnen oder die Verweigerung der Behandlung androhen, wenn die Patientin oder der Patient die Informationen nach Art. 13 Datenschutz-Grundverordnung (DS-GVO) nicht mit ihrer oder seiner Unterschrift versieht. Eine solche Praxis ist nicht mit der DS-GVO vereinbar.

Die Informationspflicht nach Art. 13 DS-GVO bezweckt lediglich, dass der Patientin bzw. dem Patienten die Gelegenheit gegeben wird, die entsprechenden Informationen einfach und ohne Umwege zu erhalten. Sie oder er muss diese jedoch nicht zur Kenntnis nehmen, wenn sie oder er dies nicht möchte.
Um seinen Nachweispflichten gegenüber der Aufsichtsbehörde nachzukommen, kann der Verantwortliche das Aushändigen der Information vermerken oder einen konkreten Verfahrensablauf betreffend die Umsetzung der Informationspflicht dokumentieren, aus dem hervorgeht, wie die Patientin oder der Patient die Informationen im Regelfall erhält.

8.16 Beschluss der DSK zu Facebook Fanpages

Beschluss
der Datenschutzkonferenz vom 5. September 2018

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-Betreiberinnen und Betreibern und Facebook besteht. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat in ihrer Entschließung vom 6. Juni 2018 deutlich gemacht, welche Konsequenzen sich aus dem Urteil für die gemeinsam Verantwortlichen – insbesondere für die Betreiberinnen und Betreiber einer Fanpage – ergeben.
Bei einer gemeinsamen Verantwortlichkeit fordert die Datenschutz-Grundverordnung (DS-GVO) unter anderem eine Vereinbarung zwischen den Beteiligten, die klarstellt, wie die Pflichten aus der DS-GVO erfüllt werden.
Seit dem Urteil des EuGH sind drei Monate vergangen. Zwar hat Facebook einige Änderungen in seinem Angebot – zum Beispiel bezüglich der Cookies – vorgenommen, doch weiterhin werden auch bei Personen, die keine Facebook-Nutzerinnen und Nutzer sind, Cookies mit Identifikatoren gesetzt, jedenfalls wenn sie über die bloße Startseite einer Fanpage hinaus dort einen Inhalt aufrufen.
Auch werden nach wie vor die Fanpage-Besuche von Betroffenen nach bestimmten, teilweise voreingestellten Kriterien im Rahmen einer sogenannten Insights-Funktion von Facebook ausgewertet und den Betreiberinnen und Betreibern zur Verfügung gestellt.
Der EuGH hat unter anderem hervorgehoben, dass „die bei Facebook unterhaltenen Fanpages auch von Personen besucht werden können, die keine Facebook-Nutzer sind und somit nicht über ein Benutzerkonto bei diesem sozialen Netzwerk verfügen. In diesem Fall erscheint die Verantwortlichkeit des Betreibers der Fanpage hinsichtlich der Verarbeitung der personenbezogenen Daten dieser Personen noch höher, da das bloße Aufrufen der Fanpage durch Besucher automatisch die Verarbeitung ihrer personenbezogenen Daten auslöst.“
Offizielle Verlautbarungen vonseiten Facebooks, ob und welche Schritte unternommen werden, um einen rechtskonformen Betrieb von Facebook-Fanpages zu ermöglichen, sind bisher ausgeblieben. Eine von Facebook noch im Juni 2018 angekündigte Vereinbarung

nach Art. 26 DS-GVO (Gemeinsam für die Verarbeitung Verantwortliche) wurde bislang nicht zur Verfügung gestellt. Die deutschen Datenschutzaufsichtsbehörden wirken daher auf europäischer Ebene auf ein abgestimmtes Vorgehen gegenüber Facebook hin.
Auch Fanpage-Betreiberinnen und Betreiber müssen sich ihrer datenschutzrechtlichen Verantwortung stellen. Ohne Vereinbarung nach Art. 26 DS-GVO ist der Betrieb einer Fanpage, wie sie derzeit von Facebook angeboten wird, rechtswidrig.
Daher fordert die DSK, dass nun die Anforderungen des Datenschutzrechts beim Betrieb von Fanpages erfüllt werden. Dazu gehört insbesondere, dass die gemeinsam Verantwortlichen Klarheit über die derzeitige Sachlage schaffen und die erforderlichen Informationen den betroffenen Personen (= Besucherinnen und Besucher der Fanpage) bereitstellen.
Eine gemeinsame Verantwortlichkeit bedeutet allerdings auch, dass Fanpage-Betreiberinnen und Betreiber (unabhängig davon, ob es sich um öffentliche oder nicht-öffentliche Verantwortliche handelt) die Rechtmäßigkeit der gemeinsam zu verantwortenden Datenverarbeitung gewährleisten und dies nachweisen können. Zudem können Betroffene ihre Rechte aus der DS-GVO bei und gegenüber jedem Verantwortlichen geltend machen (Art. 26 Abs. 3 DS-GVO).
Insbesondere die im Anhang aufgeführten Fragen müssen deshalb sowohl von Facebook als auch und von Fanpage-Betreiberinnen und Betreibern beantwortet werden können.

Anhang: Fragenkatalog

1. In welcher Art und Weise wird zwischen Ihnen und anderen gemeinsam Verantwortlichen festgelegt, wer von Ihnen welche Verpflichtung gemäß der DS-GVO erfüllt? (Art. 26 Abs. 1 DS-GVO)
2. Auf Grundlage welcher Vereinbarung haben Sie untereinander festgelegt, wer welchen Informationspflichten nach Art. 13 und 14 DS-GVO nachkommt?
3. Auf welche Weise werden die wesentlichen Aspekte dieser Vereinbarung den betroffenen Personen zur Verfügung gestellt?
4. Wie stellen Sie sicher, dass die Betroffenenrechte (Art. 12 ff. DS-GVO) erfüllt werden können, insbesondere die Rechte auf Löschung nach Art. 17 DS-GVO, auf Einschränkung der

Verarbeitung nach Art. 18 DSGVO, auf Widerspruch nach Art. 21 DS-GVO und auf Auskunft nach Art. 15 DS-GVO?

5. Zu welchen Zwecken und auf welcher Rechtsgrundlage verarbeiten Sie die personenbezogenen Daten der Besucherinnen und Besucher von Fanpages? Welche personenbezogenen Daten werden gespeichert? Inwieweit werden aufgrund der Besuche von Facebook-Fanpages Profile erstellt oder angereichert? Werden auch personenbezogene Daten von Nicht-Facebook-Mitgliedern zur Erstellung von Profilen verwendet? Welche Löschfristen sind vorgesehen?
6. Zu welchen Zwecken und auf welcher Rechtsgrundlage werden beim Erstaufruf einer Fanpage auch bei Nicht-Mitgliedern Einträge im sogenannten Local Storage erzeugt?
7. Zu welchen Zwecken und auf welcher Rechtsgrundlage werden nach Aufruf einer Unterseite innerhalb des Fanpage-Angebots ein Session-Cookie und drei Cookies mit Lebenszeiten zwischen vier Monaten und zwei Jahren gespeichert?
8. Welche Maßnahmen haben Sie ergriffen, um Ihren Verpflichtungen aus Art. 26 DS-GVO als gemeinsam für die Verarbeitung Verantwortlicher gerecht zu werden und eine entsprechende Vereinbarung abzuschließen?

8.17 Anwendung der DS-GVO im Bereich von Parlamenten, Fraktionen, Abgeordneten und politischen Parteien

Beschluss
der Datenschutzkonferenz vom 5. September 2018

Die Konferenz nimmt das Ergebnis der Beratungen des Arbeitskreises Grundsatzfragen des Datenschutzes zur Kenntnis und empfiehlt für die weitere Rechtspraxis, die im Folgenden aufgeführten Positionierungen bei der Tätigkeit als Aufsichtsbehörde zu Grunde zu legen:

1. Soweit Datenverarbeitungen von Parlamenten (auch deren Organe einschließlich der Abgeordneten) den parlamentarischen Kerntätigkeiten zuzuordnen sind, findet die Datenschutz-Grundverordnung (DS-GVO) keine Anwendung.
2. Parlamente (auch deren Organe einschließlich der Abgeordneten) unterliegen bei der Ausübung originär parlamentarischer Kerntätigkeiten nur dann datenschutzrechtlichen Vorgaben und der Aufsicht der Aufsichtsbehörde, wenn sich dies aus einer klaren gesetzlichen Regelung ergibt.
3. Die Einordnung von Tätigkeiten der Parlamente (auch deren Organe einschließlich der Abgeordneten) als verwaltende und fiskalische in Abgrenzung zur parlamentarischen Kerntätigkeit bedarf jeweils einer Bewertung im Einzelfall.
4. Soweit gesetzlichen Grundlagen für die parlamentarische Kerntätigkeit bestehen, wäre eine Datenschutzordnung des Parlaments zu empfehlen, die sich an der DS-GVO orientieren sollte. Eine Beratung durch die Aufsichtsbehörde sollte in jedem Fall unbenommen bleiben.
5. Parteien als nicht-öffentliche Stellen sind grundsätzlich Normadressaten der DS-GVO und unterliegen damit der Aufsicht der Aufsichtsbehörden. Eine mögliche Berücksichtigung ihres besonderen Status im Rahmen der Gesetzesanwendung bleibt unberührt.

9. Vorträge

9.1 Der TLfDI informiert!: Hohe Nachfrage nach Vorträgen und Veranstaltungen zum Datenschutz

Zwei Großveranstaltungen und fast 200 Vorträge zur Umsetzung der DS-GVO, das ist die arbeitsreiche Bilanz 2018 des TLfDI.

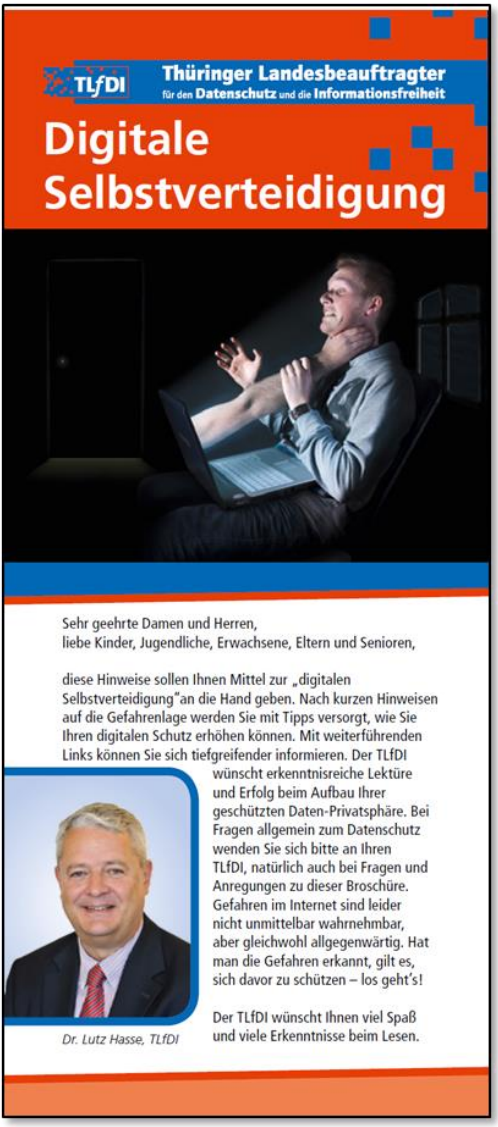
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte im Jahr 2018 zwei Großveranstaltungen im Freistaat Thüringen ins Leben gerufen. Am 18. Januar 2018 fand die gemeinsame Veranstaltung „Trojaner, Body-Cams und Co. – Polizeiarbeit zwischen Sicherheit und Schutz der informationellen Selbstbestimmung“ mit dem Bund Deutscher Kriminalbeamter, der Deutschen Polizei Gewerkschaft, und der Gewerkschaft der Polizei Thüringen im Augustinerkloster zu Erfurt statt. Mehr als 300 Teilnehmer hatten sich angemeldet. 150 Gäste, vorwiegend Bedienstete der Thüringer Polizei, konnten die Veranstaltung besuchen. Hierbei wurden die technischen Mittel und Möglichkeiten der Polizeiarbeit von verschiedenen Akteuren kritisch beleuchtet. Gefährden oder schützen Polizei und Verfassungsschutz die Grundrechte der informationellen Selbstbestimmung? Diese und viele andere Fragen galt es zu beantworten.
Die nächste Veranstaltung war dem Thema „Arbeit 4.0 etc.: Menschenwürde auf Digi-Tal-Fahrt?“ gewidmet. Dabei wurden die voranschreitende Digitalisierung und die Zukunft der Arbeitsgesellschaft ins Visier genommen. Fortschritt und Grundrechtsschutz, passt das noch zusammen? Wir versuchten die Antwort darauf im Dialog zu finden. Dieses Event fand unter der Federführung des TLfDI am 14. August 2018 im Augustinerkloster in Erfurt statt gemeinsam mit der Arbeitsgemeinschaft für Arbeitnehmerfragen, der Thüringer Jusos und ver.di. Die nächste Veranstaltung, diesmal zur Künstlichen Intelligenz (KI): Am 1. Juli 2019 im Augustinerkloster.
Eines hat das Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) am 25. Mai 2018 auf jeden Fall in Bewegung gesetzt, nämlich die Anfragen von Schulungen durch den TLfDI. Fast 200 Vorträge, an Universitäten, in Pflegeeinrichtungen oder im Ortsverband der Vereine, die Neuerungen der DS-GVO betreffend, wurden von Mitarbeitern des TLfDI umgesetzt. Um so viele Unternehmerinnen und Unter-

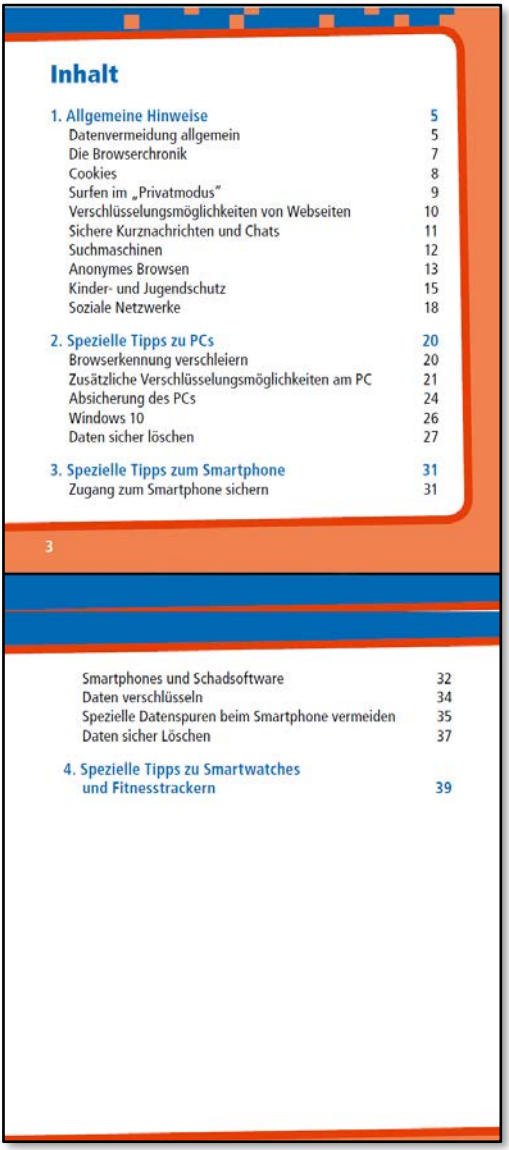
nehmer, Schulleiterinnen und Schulleiter, Vereinsvorsitzende und andere Datenschutzbeauftragte wie nur möglich zu erreichen, gab es die Möglichkeit an sieben Sammelvorträgen in der Industrie- und Handelskammer Erfurt und in den fünf Schulämtern Thüringens teilzunehmen. Somit wurden insgesamt einige Tausende Interessierte in die Neuheiten der DS-GVO eingeführt. Schön, dass die Nachfrage und das Interesse so groß war und immer noch ist!

Auch bei Veranstaltungen in der ganzen Bundesrepublik war der TLfDI ein gefragter Redner, von „A“, wie „Autorecht“ über „D“, wie „didacta“ bis „Z“, wie“ Zukunftsthemen“. Hier standen vor allem die Fragen im Vordergrund, wie die Aufsichtsbehörde die DS-GVO umsetzt und was den TLfDI sonst noch so umtreibt.

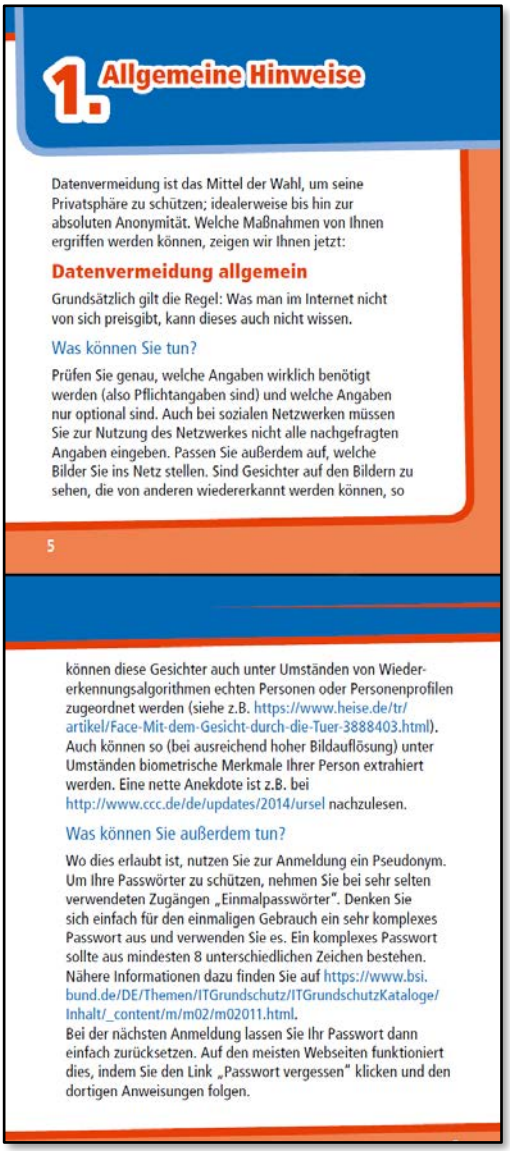
Fortsetzung folgt!

10. Anhang – Broschüre digitale Selbstverteidigung





Inhalt



1. Allgemeine Hinweise

Datenvermeidung ist das Mittel der Wahl, um seine Privatsphäre zu schützen; idealerweise bis hin zur absoluten Anonymität. Welche Maßnahmen von Ihnen ergriffen werden können, zeigen wir Ihnen jetzt:

Datenvermeidung allgemein

Grundsätzlich gilt die Regel: Was man im Internet nicht von sich preisgibt, kann dieses auch nicht wissen.

Was können Sie tun?

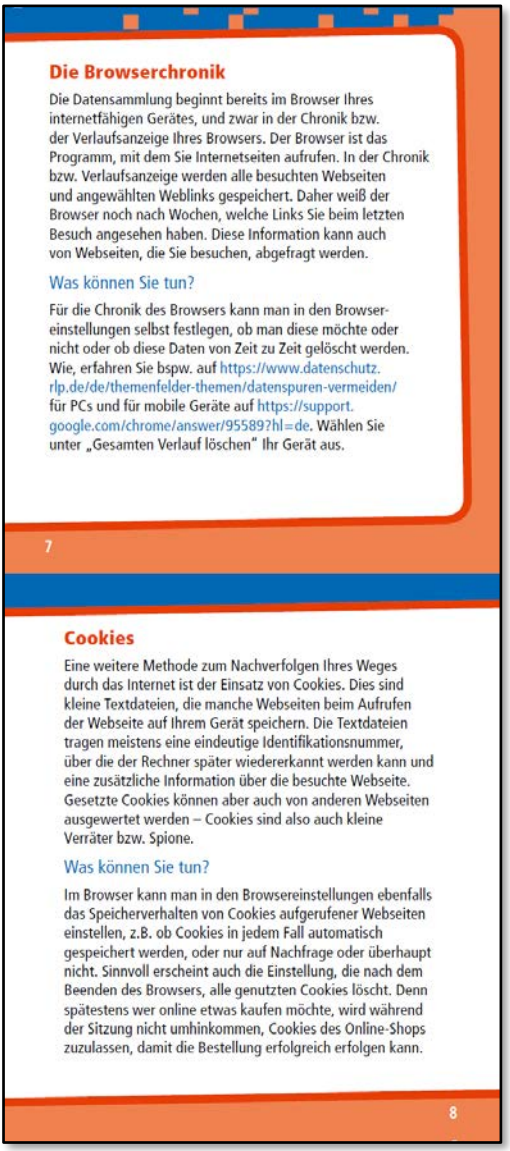
Prüfen Sie genau, welche Angaben wirklich benötigt werden (also Pflichtangaben sind) und welche Angaben nur optional sind. Auch bei sozialen Netzwerken müssen Sie zur Nutzung des Netzwerkes nicht alle nachgefragten Angaben eingeben. Passen Sie außerdem auf, welche Bilder Sie ins Netz stellen. Sind Gesichter auf den Bildern zu sehen, die von anderen wiedererkannt werden können, so

5

können diese Gesichter auch unter Umständen von Wiedererkennungsalgorithmen echten Personen oder Personenprofilen zugeordnet werden (siehe z.B. https://www.heise.de/tr/artikel/Face-Mit-dem-Gesicht-durch-die-Tuer-3888403.html). Auch können so (bei ausreichend hoher Bildauflösung) unter Umständen biometrische Merkmale Ihrer Person extrahiert werden. Eine nette Anekdote ist z.B. bei http://www.ccc.de/de/updates/2014/ursel nachzulesen.

Was können Sie außerdem tun?

Wo dies erlaubt ist, nutzen Sie zur Anmeldung ein Pseudonym. Um Ihre Passwörter zu schützen, nehmen Sie bei sehr selten verwendeten Zugängen „Einmalpasswörter". Denken Sie sich einfach für den einmaligen Gebrauch ein sehr komplexes Passwort aus und verwenden Sie es. Ein komplexes Passwort sollte aus mindesten 8 unterschiedlichen Zeichen bestehen. Nähere Informationen dazu finden Sie auf https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html.
Bei der nächsten Anmeldung lassen Sie Ihr Passwort dann einfach zurücksetzen. Auf den meisten Webseiten funktioniert dies, indem Sie den Link „Passwort vergessen" klicken und den dortigen Anweisungen folgen.



Die Browserchronik

Die Datensammlung beginnt bereits im Browser Ihres internetfähigen Gerätes, und zwar in der Chronik bzw. der Verlaufsanzeige Ihres Browsers. Der Browser ist das Programm, mit dem Sie Internetseiten aufrufen. In der Chronik bzw. Verlaufsanzeige werden alle besuchten Webseiten und angewählten Weblinks gespeichert. Daher weiß der Browser noch nach Wochen, welche Links Sie beim letzten Besuch angesehen haben. Diese Information kann auch von Webseiten, die Sie besuchen, abgefragt werden.

Was können Sie tun?

Für die Chronik des Browsers kann man in den Browsereinstellungen selbst festlegen, ob man diese möchte oder nicht oder ob diese Daten von Zeit zu Zeit gelöscht werden. Wie, erfahren Sie bspw. auf https://www.datenschutz.rlp.de/de/themenfelder-themen/datenspuren-vermeiden/ für PCs und für mobile Geräte auf https://support.google.com/chrome/answer/95589?hl=de. Wählen Sie unter „Gesamten Verlauf löschen" Ihr Gerät aus.

7

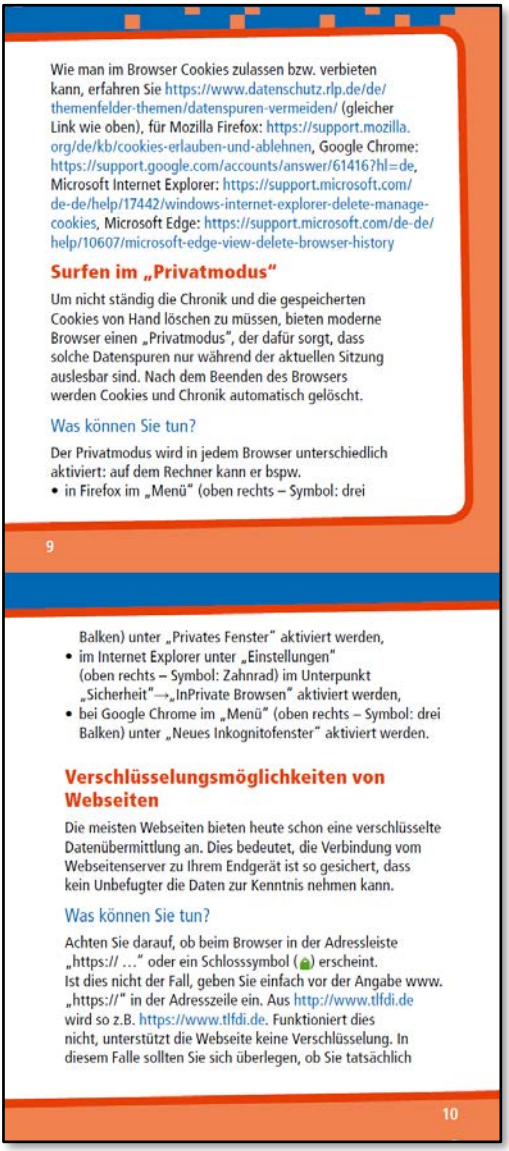
Cookies

Eine weitere Methode zum Nachverfolgen Ihres Weges durch das Internet ist der Einsatz von Cookies. Dies sind kleine Textdateien, die manche Webseiten beim Aufrufen der Webseite auf Ihrem Gerät speichern. Die Textdateien tragen meistens eine eindeutige Identifikationsnummer, über die der Rechner später wiedererkannt werden kann und eine zusätzliche Information über die besuchte Webseite. Gesetzte Cookies können aber auch von anderen Webseiten ausgewertet werden – Cookies sind also auch kleine Verräter bzw. Spione.

Was können Sie tun?

Im Browser kann man in den Browsereinstellungen ebenfalls das Speicherverhalten von Cookies aufgerufener Webseiten einstellen, z.B. ob Cookies in jedem Fall automatisch gespeichert werden, oder nur auf Nachfrage oder überhaupt nicht. Sinnvoll erscheint auch die Einstellung, die nach dem Beenden des Browsers, alle genutzten Cookies löscht. Denn spätestens wer online etwas kaufen möchte, wird während der Sitzung nicht umhinkommen, Cookies des Online-Shops zuzulassen, damit die Bestellung erfolgreich erfolgen kann.

8



Wie man im Browser Cookies zulassen bzw. verbieten kann, erfahren Sie https://www.datenschutz.rlp.de/de/themenfelder-themen/datenspuren-vermeiden/ (gleicher Link wie oben), für Mozilla Firefox: https://support.mozilla.org/de/kb/cookies-erlauben-und-ablehnen, Google Chrome: https://support.google.com/accounts/answer/61416?hl=de, Microsoft Internet Explorer: https://support.microsoft.com/de-de/help/17442/windows-internet-explorer-delete-manage-cookies, Microsoft Edge: https://support.microsoft.com/de-de/help/10607/microsoft-edge-view-delete-browser-history

Surfen im „Privatmodus"

Um nicht ständig die Chronik und die gespeicherten Cookies von Hand löschen zu müssen, bieten moderne Browser einen „Privatmodus", der dafür sorgt, dass solche Datenspuren nur während der aktuellen Sitzung auslesbar sind. Nach dem Beenden des Browsers werden Cookies und Chronik automatisch gelöscht.

Was können Sie tun?

Der Privatmodus wird in jedem Browser unterschiedlich aktiviert: auf dem Rechner kann er bspw.

- in Firefox im „Menü" (oben rechts – Symbol: drei

9

Balken) unter „Privates Fenster" aktiviert werden,
- im Internet Explorer unter „Einstellungen" (oben rechts – Symbol: Zahnrad) im Unterpunkt „Sicherheit"→„InPrivate Browsen" aktiviert werden,
- bei Google Chrome im „Menü" (oben rechts – Symbol: drei Balken) unter „Neues Inkognitofenster" aktiviert werden.

Verschlüsselungsmöglichkeiten von Webseiten

Die meisten Webseiten bieten heute schon eine verschlüsselte Datenübermittlung an. Dies bedeutet, die Verbindung vom Webseitenserver zu Ihrem Endgerät ist so gesichert, dass kein Unbefugter die Daten zur Kenntnis nehmen kann.

Was können Sie tun?

Achten Sie darauf, ob beim Browser in der Adressleiste „https:// …" oder ein Schlosssymbol (🔒) erscheint. Ist dies nicht der Fall, geben Sie einfach vor der Angabe www. „https://" in der Adresszeile ein. Aus http://www.tlfdi.de wird so z.B. https://www.tlfdi.de. Funktioniert dies nicht, unterstützt die Webseite keine Verschlüsselung. In diesem Falle sollten Sie sich überlegen, ob Sie tatsächlich

10

personenbezogene Daten auf der Webseite eingeben wollen, da die Datenübermittlung ansonsten unverschlüsselt erfolgt.

Sichere Kurznachrichten und Chats

Kurznachrichtendienste und Chats werden heute häufig schon verschlüsselt übertragen. Dadurch können z.B. Angreifer oder „Mithörer" die Daten auf dem Datenweg nicht einfach mitlesen. Ist eine Schadsoftware, wie z.B. ein Trojaner, auf Ihrem Gerät installiert, welche z.B. die Tastatureingabe oder die Bildschirmanzeige ausliest, nützt allerdings Verschlüsselung gar nichts. Auch Betreiber der Kurznachrichtendienste könnten die Inhalte evtl. mitlesen und daraus wieder Informationen für Profile extrahieren.

Was können Sie tun?

Verwenden Sie verschlüsselte Kurznachrichten mit einer sogenannten Ende-zu-Ende Verschlüsselung. Ein einfaches Browser-Plugin oder eine entsprechende App kann dann zur verschlüsselten Unterhaltung mit Ende-zu-Ende Verschlüsselung

© gena96 – Fotolia

11

genutzt werden und der Betreiber oder Personen mit krimineller Energie können nicht mehr mitlesen. Den Link beispielsweise zum Programm CryptoCat finden Sie hier: https://de.wikipedia.org/wiki/Cryptocat. Cpypto-Cat ist eine Browsererweiterung oder eine App für Smartphones, die eine Ende-zu-Ende verschlüsselte Kommunikation ermöglicht.

Aber wie gesagt, wenn Sie die Schadsoftware auf Ihrem Gerät haben, welche die Tastatureingaben und Bildschirminhalte mitliest, hilft auch dies nicht. Deshalb ist es wichtig, dass Sie neben der Ende-zu-Ende-Verschlüsselung stets die Sicherheitsupdates des Antivirenprogramms, des Betriebssystems und anderer Programme installiert haben (siehe hierzu Absicherung des PCs).

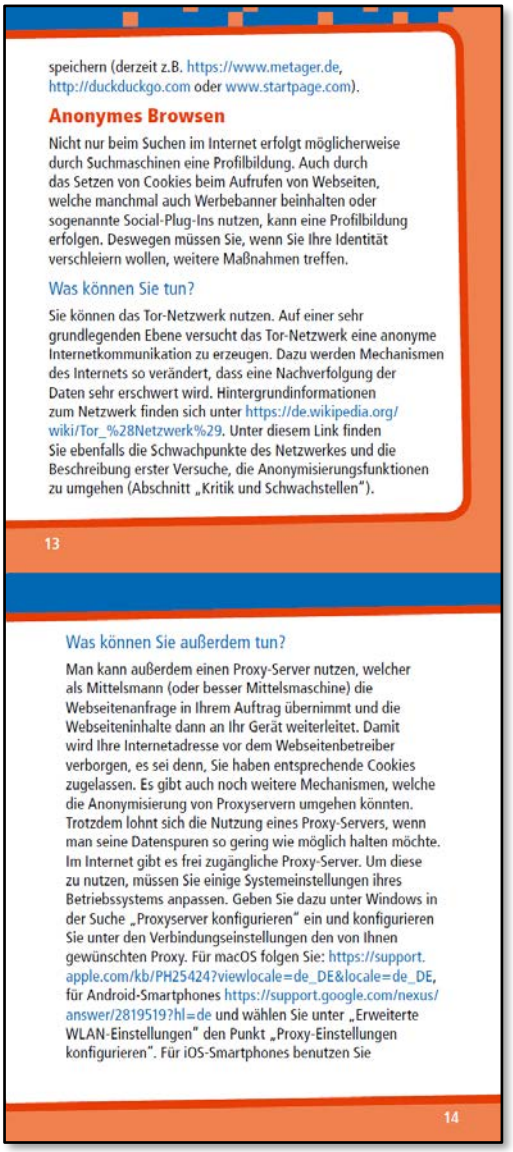
Suchmaschinen

Die Betreiber von Suchmaschinen versuchen, möglichst viele Informationen über ihre Nutzer zu erfahren. Auch durch die Auswertung der von Ihnen eingegebenen Suchbegriffe kann viel über Sie herausgefunden werden.

Was können Sie tun?

Es gibt datenschutzfreundliche Suchmaschinen, welche die IP-Adressen der Nutzer anonymisieren oder gar nicht erst

12



speichern (derzeit z.B. https://www.metager.de, http://duckduckgo.com oder www.startpage.com).

Anonymes Browsen

Nicht nur beim Suchen im Internet erfolgt möglicherweise durch Suchmaschinen eine Profilbildung. Auch durch das Setzen von Cookies beim Aufrufen von Webseiten, welche manchmal auch Werbebanner beinhalten oder sogenannte Social-Plug-Ins nutzen, kann eine Profilbildung erfolgen. Deswegen müssen Sie, wenn Sie Ihre Identität verschleiern wollen, weitere Maßnahmen treffen.

Was können Sie tun?

Sie können das Tor-Netzwerk nutzen. Auf einer sehr grundlegenden Ebene versucht das Tor-Netzwerk eine anonyme Internetkommunikation zu erzeugen. Dazu werden Mechanismen des Internets so verändert, dass eine Nachverfolgung der Daten sehr erschwert wird. Hintergrundinformationen zum Netzwerk finden sich unter https://de.wikipedia.org/wiki/Tor_%28Netzwerk%29. Unter diesem Link finden Sie ebenfalls die Schwachpunkte des Netzwerkes und die Beschreibung erster Versuche, die Anonymisierungsfunktionen zu umgehen (Abschnitt „Kritik und Schwachstellen").

13

Was können Sie außerdem tun?

Man kann außerdem einen Proxy-Server nutzen, welcher als Mittelsmann (oder besser Mittelsmaschine) die Webseitenanfrage in Ihrem Auftrag übernimmt und die Webseiteninhalte dann an Ihr Gerät weiterleitet. Damit wird Ihre Internetadresse vor dem Webseitenbetreiber verborgen, es sei denn, Sie haben entsprechende Cookies zugelassen. Es gibt auch noch weitere Mechanismen, welche die Anonymisierung von Proxyservern umgehen könnten. Trotzdem lohnt sich die Nutzung eines Proxy-Servers, wenn man seine Datenspuren so gering wie möglich halten möchte. Im Internet gibt es frei zugängliche Proxy-Server. Um diese zu nutzen, müssen Sie einige Systemeinstellungen ihres Betriebssystems anpassen. Geben Sie dazu unter Windows in der Suche „Proxyserver konfigurieren" ein und konfigurieren Sie unter den Verbindungseinstellungen den von Ihnen gewünschten Proxy. Für macOS folgen Sie: https://support.apple.com/kb/PH25424?viewlocale=de_DE&locale=de_DE, für Android-Smartphones https://support.google.com/nexus/answer/2819519?hl=de und wählen Sie unter „Erweiterte WLAN-Einstellungen" den Punkt „Proxy-Einstellungen konfigurieren". Für iOS-Smartphones benutzen Sie

14

https://support.apple.com/de-de/HT202693. Die Anonymität von Proxy-Servern kann allerdings durch Cookies oder JavaScript recht einfach umgangen werden. Nähere Informationen dazu finden Sie auf der Webseite der TU-Dresden: https://anon.inf.tu-dresden.de/help/jap_help/de/help/otherServices.html. Noch weitergehende Werkzeuge zum anonymen Surfen werden ebenfalls von der TU-Dresden zur Verfügung gestellt – https://anon.inf.tu-dresden.de/help/jap_help/de/help/about.html.

Kinder- und Jugendschutz

Auch im Internet muss der Kinder- und Jugendschutz eingehalten werden. Deshalb sollten auch Eltern sich regelmäßig über die Gefahren informieren, denen ihre Kinder im Internet evtl. ausgesetzt sein können. Diese Gefahren können sich zum einen aus

© Maxim Ruzaikow – Fotolia

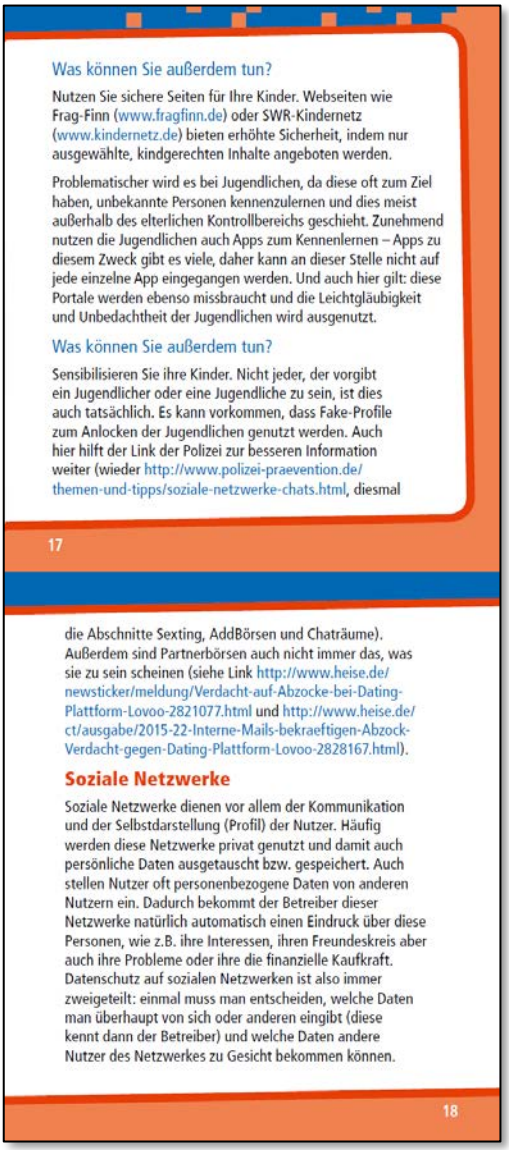
15

dem Besuch von z.B. nicht jugendfreien Webseiten ergeben oder, indem die Kinder oder Jugendlichen aktiv von Fremden kontaktiert werden – z.B. über Chats und Nachrichten-Apps. Neben den bekannten Kommunikationsdiensten wie Facebook-Messenger, WhatsApp oder Threema gibt es auch zahlreiche Onlinespiele, die eine Chatfunktion beinhalten. Auch gibt es – speziell für Kinder – Nachrichten und Apps, welche kindgerecht gestaltet sind. Diese kindgerechten Apps mit Chatfunktion ziehen leider auch Pädophile an. Diese versuchen dann, mit falscher Identität über Geschenke oder Versprechungen, die Kinder / Jugendlichen zu sexuellen Handlungen zu überreden.

Was können Sie tun?

Sensibilisieren Sie ihre Kinder. Wenn jemand Kontakt sucht oder Dinge wie Spiele-Gegenstände oder Spiele-Währung gegen Fotos oder Videos eintauschen will, so sollte das Kind vorsichtig sein. Kennt ihr Kind das digitale Gegenüber als echte Person, so ist die Gefahr des Missbrauchs geringer. Weitere Informationen finden Sie auf den Seiten der Polizei (z.B. http://www.polizei-praevention.de/themen-und-tipps/soziale-netzwerke-chats.html in den Abschnitten Addbörsen und Chaträume).

16



Was können Sie außerdem tun?

Nutzen Sie sichere Seiten für Ihre Kinder. Webseiten wie Frag-Finn (www.fragfinn.de) oder SWR-Kindernetz (www.kindernetz.de) bieten erhöhte Sicherheit, indem nur ausgewählte, kindgerechten Inhalte angeboten werden.

Problematischer wird es bei Jugendlichen, da diese oft zum Ziel haben, unbekannte Personen kennenzulernen und dies meist außerhalb des elterlichen Kontrollbereichs geschieht. Zunehmend nutzen die Jugendlichen auch Apps zum Kennenlernen – Apps zu diesem Zweck gibt es viele, daher kann an dieser Stelle nicht auf jede einzelne App eingegangen werden. Und auch hier gilt: diese Portale werden ebenso missbraucht und die Leichtgläubigkeit und Unbedachtheit der Jugendlichen wird ausgenutzt.

Was können Sie außerdem tun?

Sensibilisieren Sie ihre Kinder. Nicht jeder, der vorgibt ein Jugendlicher oder eine Jugendliche zu sein, ist dies auch tatsächlich. Es kann vorkommen, dass Fake-Profile zum Anlocken der Jugendlichen genutzt werden. Auch hier hilft der Link der Polizei zur besseren Information weiter (wieder http://www.polizei-praevention.de/themen-und-tipps/soziale-netzwerke-chats.html, diesmal

17

die Abschnitte Sexting, AddBörsen und Chaträume). Außerdem sind Partnerbörsen auch nicht immer das, was sie zu sein scheinen (siehe Link http://www.heise.de/newsticker/meldung/Verdacht-auf-Abzocke-bei-Dating-Plattform-Lovoo-2821077.html und http://www.heise.de/ct/ausgabe/2015-22-Interne-Mails-bekraeftigen-Abzock-Verdacht-gegen-Dating-Plattform-Lovoo-2828167.html).

Soziale Netzwerke

Soziale Netzwerke dienen vor allem der Kommunikation und der Selbstdarstellung (Profil) der Nutzer. Häufig werden diese Netzwerke privat genutzt und damit auch persönliche Daten ausgetauscht bzw. gespeichert. Auch stellen Nutzer oft personenbezogene Daten von anderen Nutzern ein. Dadurch bekommt der Betreiber dieser Netzwerke natürlich automatisch einen Eindruck über diese Personen, wie z.B. ihre Interessen, ihren Freundeskreis aber auch ihre Probleme oder ihre die finanzielle Kaufkraft. Datenschutz auf sozialen Netzwerken ist also immer zweigeteilt: einmal muss man entscheiden, welche Daten man überhaupt von sich oder anderen eingibt (diese kennt dann der Betreiber) und welche Daten andere Nutzer des Netzwerkes zu Gesicht bekommen können.

18

Was können Sie tun?

Für den ersten Fall, überlegen Sie genau, welche Daten Sie ihrem Profil anvertrauen da dies dann auch der Betreiber kennt. Und prüfen Sie, ob diese Daten für den Zweck, für welches das Profil genutzt werden soll auch wirklich notwendig sind. Der zweite Fall, die Sichtbarkeit nach außen, ist meist eine Frage der Einstellungen. Hierzu gibt es im Internet für jeden Dienst gute Anleitungen (suchen Sie einfach nach dem Stichpunkt „Privatsphäre"). Für Facebook finden Sie z.B. die Anleitungen https://www.facebook.com/about/basics, für Twitter https://support.twitter.com/articles/334631, für Instagram https://help.instagram.com/116024195217477/ und für WhatsApp https://www.whatsapp.com/faq/de/android/23225461.

© Matthias Enter - Fotolia

19

2. Spezielle Tipps zu PCs

Zusätzlich zu den genannten Tipps, kann man auf dem PC bzw. dem Laptop noch ein paar weitere Maßnahmen zur Datenvermeidung treffen:

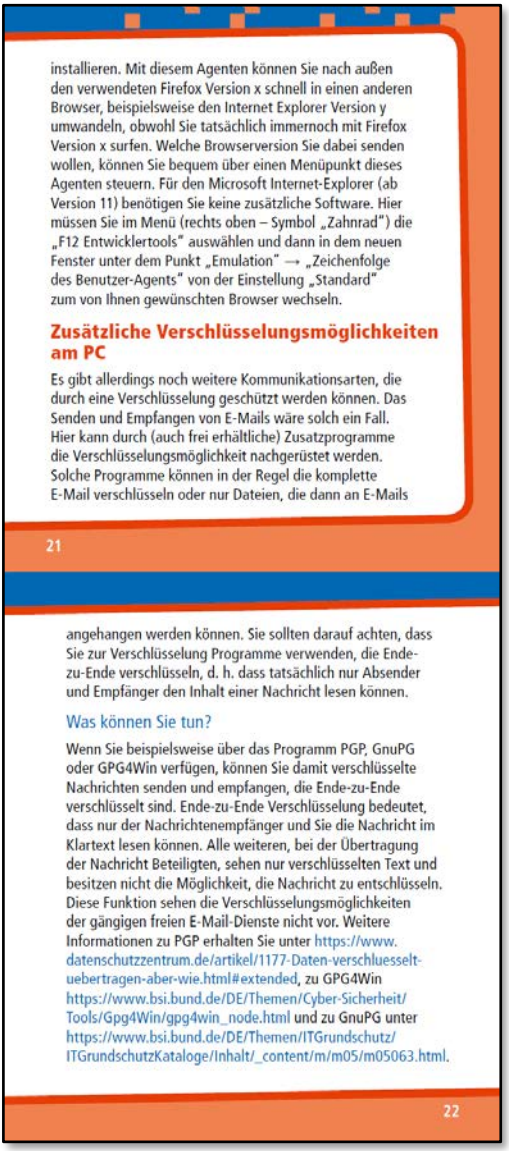
Browserkennung verschleiern

Beim Aufruf sendet der verwendete Browser neben der Adressangabe (URL) auch seine Browserkennung. Dies ist teilweise notwendig, um speziell auf diesen Browser angepasste Versionen der Webseiten anzuzeigen. Außerdem werden Informationen, wie z.B. das genutzte Betriebssystem, übertragen. Angreifer könnten wegen dieser Information gezielt Schwachstellen in Browsern und Betriebssystemen ausnutzen.

Was können Sie tun?

Um diese Information etwas zu verschleiern, können Sie bspw. den User Agent Switcher (https://addons.mozilla.org/de/firefox/addon/user-agent-switcher/) für Firefox

20



installieren. Mit diesem Agenten können Sie nach außen den verwendeten Firefox Version x schnell in einen anderen Browser, beispielsweise den Internet Explorer Version y umwandeln, obwohl Sie tatsächlich immernoch mit Firefox Version x surfen. Welche Browserversion Sie dabei senden wollen, können Sie bequem über einen Menüpunkt dieses Agenten steuern. Für den Microsoft Internet-Explorer (ab Version 11) benötigen Sie keine zusätzliche Software. Hier müssen Sie im Menü (rechts oben – Symbol „Zahnrad") die „F12 Entwicklertools" auswählen und dann in dem neuen Fenster unter dem Punkt „Emulation" → „Zeichenfolge des Benutzer-Agents" von der Einstellung „Standard" zum von Ihnen gewünschten Browser wechseln.

Zusätzliche Verschlüsselungsmöglichkeiten am PC

Es gibt allerdings noch weitere Kommunikationsarten, die durch eine Verschlüsselung geschützt werden können. Das Senden und Empfangen von E-Mails wäre solch ein Fall. Hier kann durch (auch frei erhältliche) Zusatzprogramme die Verschlüsselungsmöglichkeit nachgerüstet werden. Solche Programme können in der Regel die komplette E-Mail verschlüsseln oder nur Dateien, die dann an E-Mails

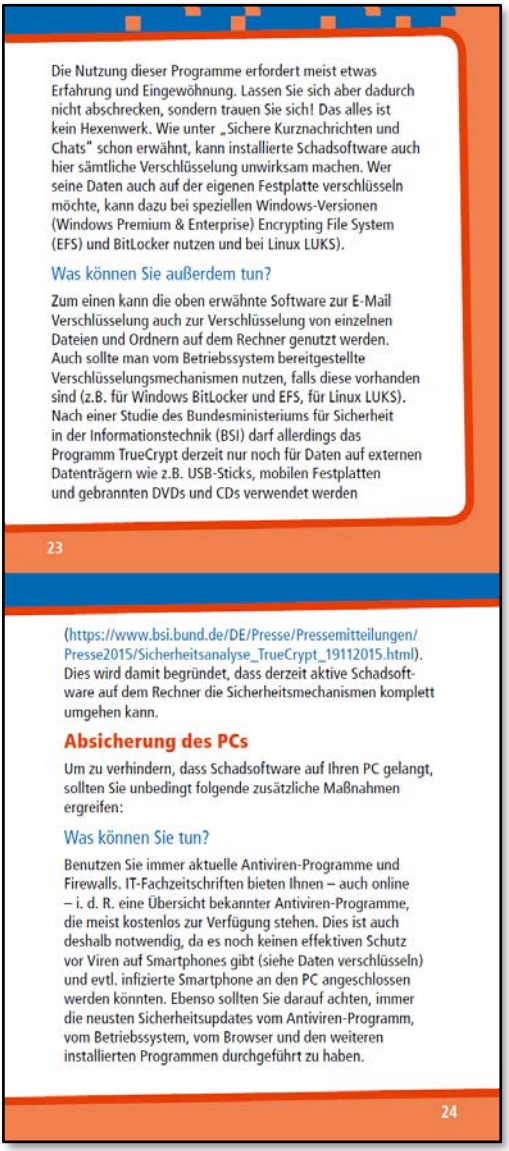
21

angehangen werden können. Sie sollten darauf achten, dass Sie zur Verschlüsselung Programme verwenden, die Ende-zu-Ende verschlüsseln, d. h. dass tatsächlich nur Absender und Empfänger den Inhalt einer Nachricht lesen können.

Was können Sie tun?

Wenn Sie beispielsweise über das Programm PGP, GnuPG oder GPG4Win verfügen, können Sie damit verschlüsselte Nachrichten senden und empfangen, die Ende-zu-Ende verschlüsselt sind. Ende-zu-Ende Verschlüsselung bedeutet, dass nur der Nachrichtenempfänger und Sie die Nachricht im Klartext lesen können. Alle weiteren, bei der Übertragung der Nachricht Beteiligten, sehen nur verschlüsselten Text und besitzen nicht die Möglichkeit, die Nachricht zu entschlüsseln. Diese Funktion sehen die Verschlüsselungsmöglichkeiten der gängigen freien E-Mail-Dienste nicht vor. Weitere Informationen zu PGP erhalten Sie unter https://www.datenschutzzentrum.de/artikel/1177-Daten-verschluesselt-uebertragen-aber-wie.html#extended, zu GPG4Win https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Tools/Gpg4Win/gpg4win_node.html und zu GnuPG unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05063.html.

22



Die Nutzung dieser Programme erfordert meist etwas Erfahrung und Eingewöhnung. Lassen Sie sich aber dadurch nicht abschrecken, sondern trauen Sie sich! Das alles ist kein Hexenwerk. Wie unter „Sichere Kurznachrichten und Chats" schon erwähnt, kann installierte Schadsoftware auch hier sämtliche Verschlüsselung unwirksam machen. Wer seine Daten auch auf der eigenen Festplatte verschlüsseln möchte, kann dazu bei speziellen Windows-Versionen (Windows Premium & Enterprise) Encrypting File System (EFS) und BitLocker nutzen und bei Linux LUKS).

Was können Sie außerdem tun?

Zum einen kann die oben erwähnte Software zur E-Mail Verschlüsselung auch zur Verschlüsselung von einzelnen Dateien und Ordnern auf dem Rechner genutzt werden. Auch sollte man vom Betriebssystem bereitgestellte Verschlüsselungsmechanismen nutzen, falls diese vorhanden sind (z.B. für Windows BitLocker und EFS, für Linux LUKS). Nach einer Studie des Bundesministeriums für Sicherheit in der Informationstechnik (BSI) darf allerdings das Programm TrueCrypt derzeit nur noch für Daten auf externen Datenträgern wie z.B. USB-Sticks, mobilen Festplatten und gebrannten DVDs und CDs verwendet werden

23

(https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2015/Sicherheitsanalyse_TrueCrypt_19112015.html). Dies wird damit begründet, dass derzeit aktive Schadsoftware auf dem Rechner die Sicherheitsmechanismen komplett umgehen kann.

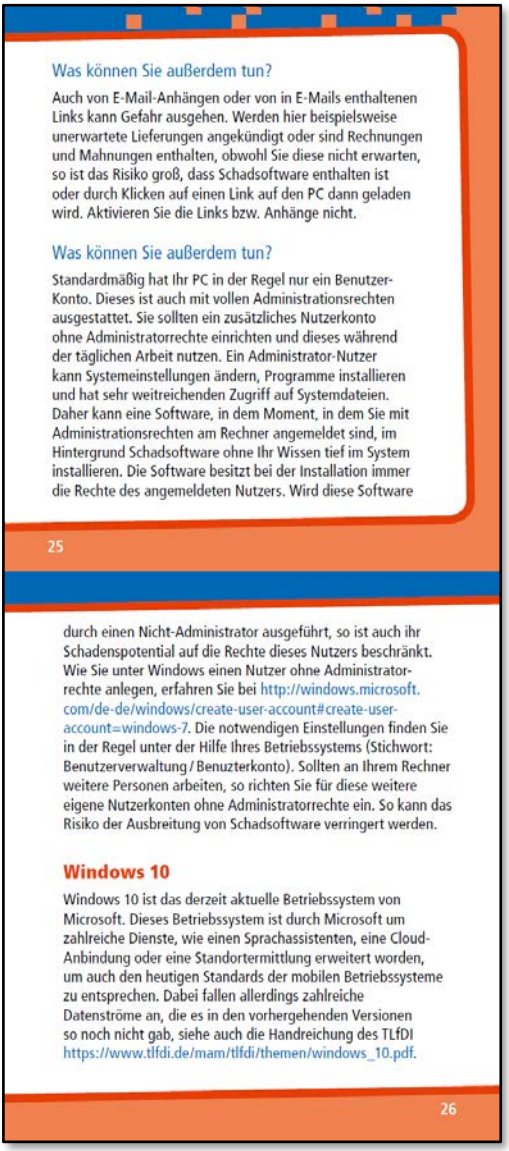
Absicherung des PCs

Um zu verhindern, dass Schadsoftware auf Ihren PC gelangt, sollten Sie unbedingt folgende zusätzliche Maßnahmen ergreifen:

Was können Sie tun?

Benutzen Sie immer aktuelle Antiviren-Programme und Firewalls. IT-Fachzeitschriften bieten Ihnen – auch online – i. d. R. eine Übersicht bekannter Antiviren-Programme, die meist kostenlos zur Verfügung stehen. Dies ist auch deshalb notwendig, da es noch keinen effektiven Schutz vor Viren auf Smartphones gibt (siehe Daten verschlüsseln) und evtl. infizierte Smartphone an den PC angeschlossen werden könnten. Ebenso sollten Sie darauf achten, immer die neusten Sicherheitsupdates vom Antiviren-Programm, vom Betriebssystem, vom Browser und den weiteren installierten Programmen durchgeführt zu haben.

24



Was können Sie außerdem tun?

Auch von E-Mail-Anhängen oder von in E-Mails enthaltenen Links kann Gefahr ausgehen. Werden hier beispielsweise unerwartete Lieferungen angekündigt oder sind Rechnungen und Mahnungen enthalten, obwohl Sie diese nicht erwarten, so ist das Risiko groß, dass Schadsoftware enthalten ist oder durch Klicken auf einen Link auf den PC dann geladen wird. Aktivieren Sie die Links bzw. Anhänge nicht.

Was können Sie außerdem tun?

Standardmäßig hat Ihr PC in der Regel nur ein Benutzer-Konto. Dieses ist auch mit vollen Administrationsrechten ausgestattet. Sie sollten ein zusätzliches Nutzerkonto ohne Administratorrechte einrichten und dieses während der täglichen Arbeit nutzen. Ein Administrator-Nutzer kann Systemeinstellungen ändern, Programme installieren und hat sehr weitreichenden Zugriff auf Systemdateien. Daher kann eine Software, in dem Moment, in dem Sie mit Administrationsrechten am Rechner angemeldet sind, im Hintergrund Schadsoftware ohne Ihr Wissen tief im System installieren. Die Software besitzt bei der Installation immer die Rechte des angemeldeten Nutzers. Wird diese Software

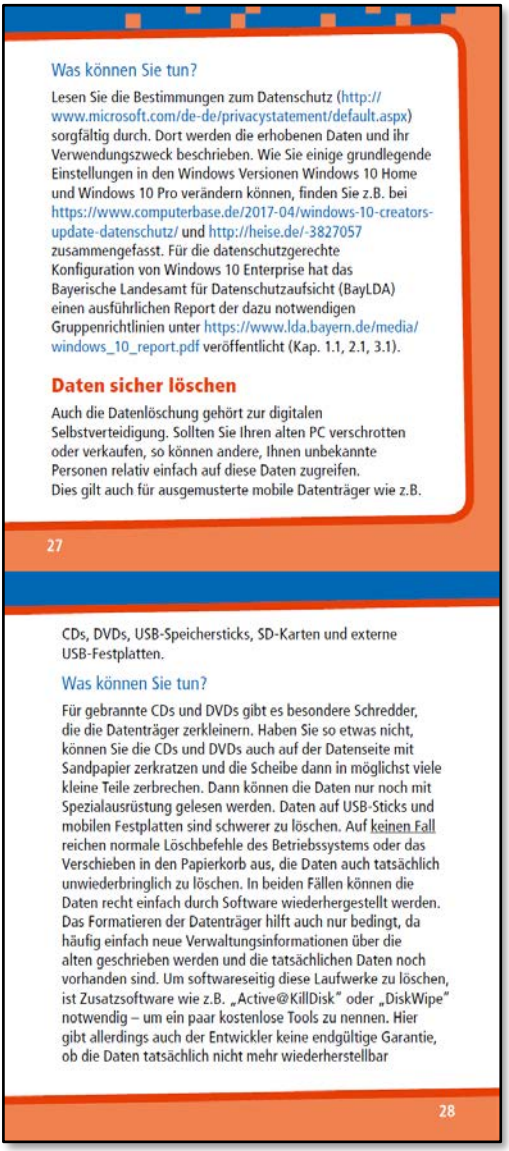
25

durch einen Nicht-Administrator ausgeführt, so ist auch ihr Schadenspotential auf die Rechte dieses Nutzers beschränkt. Wie Sie unter Windows einen Nutzer ohne Administrator-rechte anlegen, erfahren Sie bei http://windows.microsoft.com/de-de/windows/create-user-account#create-user-account=windows-7. Die notwendigen Einstellungen finden Sie in der Regel unter der Hilfe Ihres Betriebssystems (Stichwort: Benutzerverwaltung / Benutzerkonto). Sollten an Ihrem Rechner weitere Personen arbeiten, so richten Sie für diese weitere eigene Nutzerkonten ohne Administratorrechte ein. So kann das Risiko der Ausbreitung von Schadsoftware verringert werden.

Windows 10

Windows 10 ist das derzeit aktuelle Betriebssystem von Microsoft. Dieses Betriebssystem ist durch Microsoft um zahlreiche Dienste, wie einen Sprachassistenten, eine Cloud-Anbindung oder eine Standortermittlung erweitert worden, um auch den heutigen Standards der mobilen Betriebssysteme zu entsprechen. Dabei fallen allerdings zahlreiche Datenströme an, die es in den vorhergehenden Versionen so noch nicht gab, siehe auch die Handreichung des TLfDI https://www.tlfdi.de/mam/tlfdi/themen/windows_10.pdf.

26



Was können Sie tun?

Lesen Sie die Bestimmungen zum Datenschutz (http://www.microsoft.com/de-de/privacystatement/default.aspx) sorgfältig durch. Dort werden die erhobenen Daten und ihr Verwendungszweck beschrieben. Wie Sie einige grundlegende Einstellungen in den Windows Versionen Windows 10 Home und Windows 10 Pro verändern können, finden Sie z.B. bei https://www.computerbase.de/2017-04/windows-10-creators-update-datenschutz/ und http://heise.de/-3827057 zusammengefasst. Für die datenschutzgerechte Konfiguration von Windows 10 Enterprise hat das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) einen ausführlichen Report der dazu notwendigen Gruppenrichtlinien unter https://www.lda.bayern.de/media/windows_10_report.pdf veröffentlicht (Kap. 1.1, 2.1, 3.1).

Daten sicher löschen

Auch die Datenlöschung gehört zur digitalen Selbstverteidigung. Sollten Sie Ihren alten PC verschrotten oder verkaufen, so können andere, Ihnen unbekannte Personen relativ einfach auf diese Daten zugreifen. Dies gilt auch für ausgemusterte mobile Datenträger wie z.B.

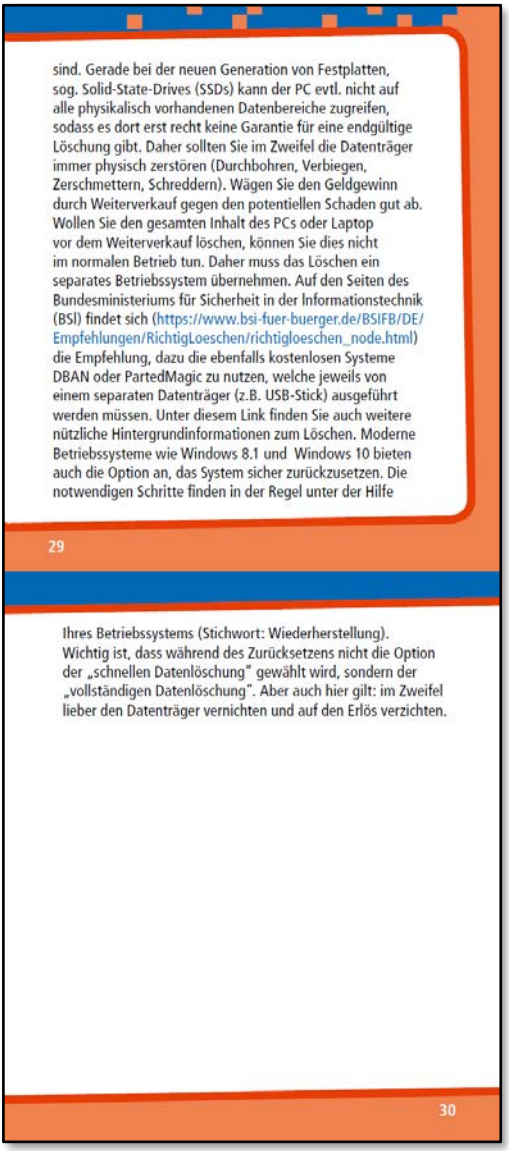
27

CDs, DVDs, USB-Speichersticks, SD-Karten und externe USB-Festplatten.

Was können Sie tun?

Für gebrannte CDs und DVDs gibt es besondere Schredder, die die Datenträger zerkleinern. Haben Sie so etwas nicht, können Sie die CDs und DVDs auch auf der Datenseite mit Sandpapier zerkratzen und die Scheibe dann in möglichst viele kleine Teile zerbrechen. Dann können die Daten nur noch mit Spezialausrüstung gelesen werden. Daten auf USB-Sticks und mobilen Festplatten sind schwerer zu löschen. Auf keinen Fall reichen normale Löschbefehle des Betriebssystems oder das Verschieben in den Papierkorb aus, die Daten auch tatsächlich unwiederbringlich zu löschen. In beiden Fällen können die Daten recht einfach durch Software wiederhergestellt werden. Das Formatieren der Datenträger hilft auch nur bedingt, da häufig einfach neue Verwaltungsinformationen über die alten geschrieben werden und die tatsächlichen Daten noch vorhanden sind. Um softwareseitig diese Laufwerke zu löschen, ist Zusatzsoftware wie z.B. „Active@KillDisk" oder „DiskWipe" notwendig – um ein paar kostenlose Tools zu nennen. Hier gibt allerdings auch der Entwickler keine endgültige Garantie, ob die Daten tatsächlich nicht mehr wiederherstellbar

28



sind. Gerade bei der neuen Generation von Festplatten, sog. Solid-State-Drives (SSDs) kann der PC evtl. nicht auf alle physikalisch vorhandenen Datenbereiche zugreifen, sodass es dort erst recht keine Garantie für eine endgültige Löschung gibt. Daher sollten Sie im Zweifel die Datenträger immer physisch zerstören (Durchbohren, Verbiegen, Zerschmettern, Schreddern). Wägen Sie den Geldgewinn durch Weiterverkauf gegen den potentiellen Schaden gut ab. Wollen Sie den gesamten Inhalt des PCs oder Laptop vor dem Weiterverkauf löschen, können Sie dies nicht im normalen Betrieb tun. Daher muss das Löschen ein separates Betriebssystem übernehmen. Auf den Seiten des Bundesministeriums für Sicherheit in der Informationstechnik (BSI) findet sich (https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/RichtigLoeschen/richtigloeschen_node.html) die Empfehlung, dazu die ebenfalls kostenlosen Systeme DBAN oder PartedMagic zu nutzen, welche jeweils von einem separaten Datenträger (z.B. USB-Stick) ausgeführt werden müssen. Unter diesem Link finden Sie auch weitere nützliche Hintergrundinformationen zum Löschen. Moderne Betriebssysteme wie Windows 8.1 und Windows 10 bieten auch die Option an, das System sicher zurückzusetzen. Die notwendigen Schritte finden in der Regel unter der Hilfe

29

Ihres Betriebssystems (Stichwort: Wiederherstellung). Wichtig ist, dass während des Zurücksetzens nicht die Option der „schnellen Datenlöschung" gewählt wird, sondern der „vollständigen Datenlöschung". Aber auch hier gilt: im Zweifel lieber den Datenträger vernichten und auf den Erlös verzichten.

30

3. Spezielle Tipps zum Smartphone

Zugang zum Smartphone sichern

Damit Ihr Smartphone oder Tablet nicht ohne Ihre Zustimmung von anderen genutzt werden kann und auch im Falle eines Diebstahls oder Verlusts geschützt ist, sollten Sie möglichst den Zugriff auf Ihr Gerät absichern.

Was können Sie tun?

Smartphones bieten in der Regel unterschiedliche Funktionen zur Zugangskontrolle an. Nutzen Sie diese. Entweder Sie verwenden z. B. ein sicheres Passwort (siehe Punkt „Datenvermeidung allgemein"), eine PIN oder Sie legen ein bestimmtes Muster fest, welches man auf dem Bildschirm zeichnen muss, um das Gerät nutzen zu können.
Wie dies auf Geräten von Apple funktioniert, finden Sie unter https://support.apple.com/de-de/HT204060. Die Anleitungen für das aktuelle Android-Betriebssystem (Version 6.0) finden Sie bei https://support.google.com/nexus/answer/2819522?hl=de

31

und für das aktuelle Windows Mobile Betriebssystem unter http://www.windowsphone.com/de-de/how-to/wp8/settings-and-personalization/lock-screen-faq.
Bitte beachten Sie, dass die Einstellungsmöglichkeiten bei Android-Geräten durch den Hersteller variieren können.

Smartphones und Schadsoftware

Sie kennen sicher Virenscanner für PCs. Auch für Smartphones gibt es heutzutage Software, die vorgibt, Dateien auf Viren untersuchen oder das Smartphone vor Schadsoftware schützen zu können. Durch die spezielle Architektur der App-Ausführung kann allerdings kein dem PC vergleichbarer Schutz hergestellt werden (siehe https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=3, Seite 19 ff.), sodass die Wirksamkeit dieser Virenscanner-Apps

© kotoyamagami – Fotolia

32

bezweifelt werden muss und nur für definierte Bereiche anwendbar ist. Das komplette Smartphone kann durch die Software nicht überprüft werden. Dennoch gibt es Software, die durch Regelwerke spezielle Prüfungen durchführen kann, eventuelle Bedrohungen identifizieren kann und in zugänglichen Bereichen (z.B. dem Browser) nach Viren und Bedrohungen sucht. Oft wird die Schadsoftware allerdings bereits mit einer App aus dem App-Store ausgeliefert. Hierzu kann keine wirksame Gegenmaßnahme empfohlen werden.

Was können Sie tun?

Installieren Sie daher nur Apps, die Sie wirklich benötigen und von App-Stores, die Sie kennen. Installieren Sie Apps als Einzeldateien (sog. APK-Files), wie sie manchmal als Download angeboten werden, nur, wenn Sie genau wissen was Sie tun. Diese Dateien werden durch niemanden kontrolliert und können auch modifiziert sein, d. h. einen Schadcode enthalten. Hilfreich ist auch, die Fachliteratur zu lesen und dort kritisch eingeschätzte Apps oder nicht mehr benötigte Apps wieder

33

zu deinstallieren. Wenn Sie Apps zur Verbesserung der Sicherheit Ihres Smartphones suchen, finden Sie eine Übersicht hier: https://www.av-test.org/de/antivirus/mobilgeraete/android/juli-2017/.

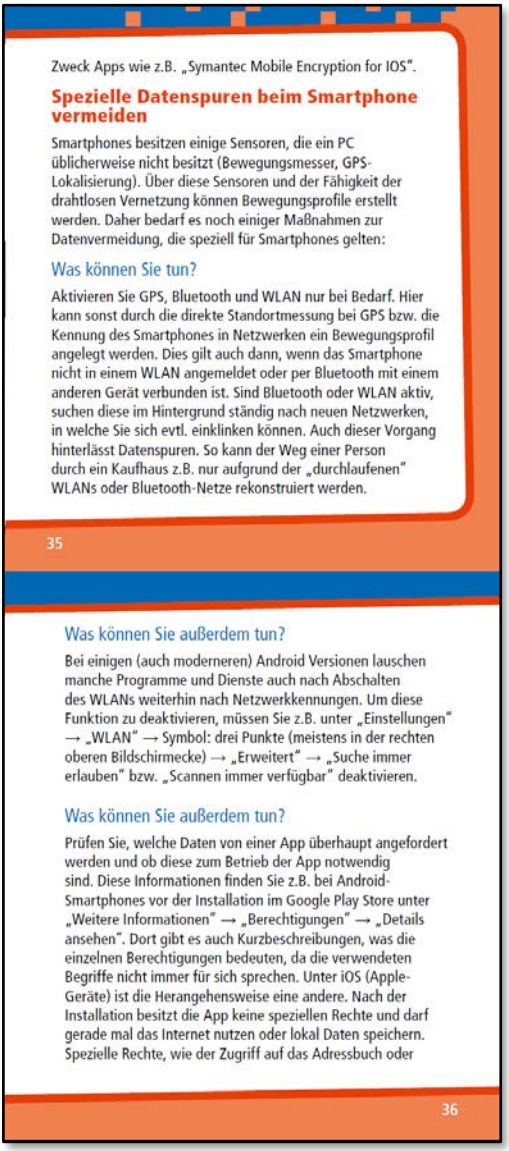
Daten verschlüsseln

Heutzutage werden die Daten auf dem Smartphone meist automatisch verschlüsselt und erst bei der Nutzung wieder entschlüsselt. Unter „Sichere Kurznachrichten und Chats" wurde bereits auf die Verschlüsselungsmöglichkeit in Chats und Messengern hingewiesen, womit Sie Ihre Kommunikation schützen können. Wenn Sie Daten durch Apps in die jeweilige Cloud speichern, können diese auch verschlüsselt werden.

Was können Sie tun?

Nutzen Sie Programme wie „BoxCryptor" oder „OpenPGP Keychain" um Daten, die in der Cloud gespeichert werden sollen zu verschlüsseln. Leider ist auf dem Gebiet der mobilen Apps noch viel Arbeit zu tun, die meisten Apps sind noch in einem experimentellen Stadium und können nicht bedenkenlos empfohlen werden. Lesen Sie sich die Kommentare und die Beschreibungen vor dem Gebrauch gut durch. Wollen Sie E-Mails verschlüsseln, gibt es zu diesem

34



Zweck Apps wie z.B. „Symantec Mobile Encryption for IOS".

Spezielle Datenspuren beim Smartphone vermeiden

Smartphones besitzen einige Sensoren, die ein PC üblicherweise nicht besitzt (Bewegungsmesser, GPS-Lokalisierung). Über diese Sensoren und der Fähigkeit der drahtlosen Vernetzung können Bewegungsprofile erstellt werden. Daher bedarf es noch einiger Maßnahmen zur Datenvermeidung, die speziell für Smartphones gelten:

Was können Sie tun?

Aktivieren Sie GPS, Bluetooth und WLAN nur bei Bedarf. Hier kann sonst durch die direkte Standortmessung bei GPS bzw. die Kennung des Smartphones in Netzwerken ein Bewegungsprofil angelegt werden. Dies gilt auch dann, wenn das Smartphone nicht in einem WLAN angemeldet oder per Bluetooth mit einem anderen Gerät verbunden ist. Sind Bluetooth oder WLAN aktiv, suchen diese im Hintergrund ständig nach neuen Netzwerken, in welche Sie sich evtl. einklinken können. Auch dieser Vorgang hinterlässt Datenspuren. So kann der Weg einer Person durch ein Kaufhaus z.B. nur aufgrund der „durchlaufenen" WLANs oder Bluetooth-Netze rekonstruiert werden.

35

Was können Sie außerdem tun?

Bei einigen (auch moderneren) Android Versionen lauschen manche Programme und Dienste auch nach Abschalten des WLANs weiterhin nach Netzwerkkennungen. Um diese Funktion zu deaktivieren, müssen Sie z.B. unter „Einstellungen" → „WLAN" → Symbol: drei Punkte (meistens in der rechten oberen Bildschirmecke) → „Erweitert" → „Suche immer erlauben" bzw. „Scannen immer verfügbar" deaktivieren.

Was können Sie außerdem tun?

Prüfen Sie, welche Daten von einer App überhaupt angefordert werden und ob diese zum Betrieb der App notwendig sind. Diese Informationen finden Sie z.B. bei Android-Smartphones vor der Installation im Google Play Store unter „Weitere Informationen" → „Berechtigungen" → „Details ansehen". Dort gibt es auch Kurzbeschreibungen, was die einzelnen Berechtigungen bedeuten, da die verwendeten Begriffe nicht immer für sich sprechen. Unter iOS (Apple-Geräte) ist die Herangehensweise eine andere. Nach der Installation besitzt die App keine speziellen Rechte und darf gerade mal das Internet nutzen oder lokal Daten speichern. Spezielle Rechte, wie der Zugriff auf das Adressbuch oder

36

die Standortlokalisation, werden beim ersten Gebrauch abgefragt. Hier sieht man also, welche Nutzeraktion dazu führt, dass die Daten benötigt werden und muss nach der Situation entscheiden, ob dies in diesem Fall sinnvoll erscheint. Prüfen Sie auch die Datenschutzerklärungen des App-Anbieters. Hier sind häufig Erklärungen zu finden, warum bestimmte Daten notwendig sind. Die Datenschutzerklärungen sind häufig nur im App-Store selber zu finden und selten Bestandteil der App. Sollten Ihnen Berechtigungen merkwürdig erscheinen, z.B. wenn eine Taschenlampen-App SMS versenden können will oder das Adressbuch benötigt, recherchieren Sie im App-Store nach alternativen Apps, die eine ähnliche Funktion „ohne Nebenwirkungen" bieten.

Daten sicher Löschen

Daten auf einem Smartphone sicher zu löschen ist schwierig. Einige Daten sind auf der SIM-Karte des Smartphones gespeichert und verschwinden, nachdem die Karte entfernt wurde. Speziell auf Smartphones sind das allerdings sehr wenige Daten. Kontakte, E-Mails, Kurznachrichten und Bilder liegen im Speicher des Gerätes selbst und können von dort auch nur mit den Systemaufrufen des Geräts gelöscht werden – im Zweifel sind die Daten also wiederherstellbar.

37

Was können Sie tun?

Aktivieren Sie die Verschlüsselung auf dem Gerät. Dadurch werden alle Daten verschlüsselt und ein Auslesen bringt zwar Daten hervor, diese sind aber nicht ohne weiteres interpretierbar. Wie dies für Android-Geräte funktioniert finden Sie unter https://support.google.com/nexus/answer/2844831?hl=de und die Anleitung für iPhones finden Sie bei https://www.apple.com/de/business/docs/iOS_Security_Guide.pdf. Bevor Sie Ihr Gerät weiterverkaufen, löschen Sie manuell alle Bilder, Nachrichten, E-Mails usw. und deinstallieren Sie danach alle Apps (Anleitung für Android: https://support.google.com/googleplay/answer/2521768?hl=de und für Apple-Geräte: https://support.apple.com/de-de/HT201274). Im letzten Schritt setzten Sie das Smartphone auf die Werkseinstellungen zurück (Anleitung für Android: https://support.google.com/android-one/answer/6088915?hl=en, Apple-Geräte sind nach dem Löschen aller Daten schon zurückgesetzt). Auch hier gilt im Zweifel: eine physikalische Zerstörung löscht am besten. Beachten Sie jedoch, dass vorher der Akku des Gerätes entfernt werden muss. Wird der Akku bei der Zerstörung beschädigt, kann ein Brand oder gar eine Explosion entstehen.

38

4. Spezielle Tipps zu Smartwatches und Fitnesstrackern

Tragbare Technikartikel (Wearables), wie Smartwatches oder Fitnesstracker, sind im Trend. Fitnesstracker messen die Bewegung und oft auch den Puls des Trägers während Smartwatches, neben der Zeitanzeige, Zusatzfunktionen wie Erinnerungen und Benachrichtigungen anzeigen, aber mitunter auch den Puls und die Aktivität (Sitzen, Gehen, Laufen, Fahren) des Trägers messen können. Auch gibt es den Trend, zunehmend GPS-Koordinaten aufzuzeichnen. Smartwatches gibt es mittlerweile, ähnlich wie Smartphones, von vielen Herstellern. Die Software basiert aber vor allen Dingen auf Android, „Android Wear" genannt, oder auf einer Apple Lösung, „WatchOS" genannt oder der Eigenentwicklung von Pebble (Uhr). In den allermeisten Fällen kommunizieren diese Geräte über Bluetooth mit Ihrem Smartphone, um die gesammelten Daten abzuspeichern oder empfangene Nachrichten anzuzeigen. Welche Smartwatch dabei mit

39

welchem Smartphone-System kompatibel ist, entnehmen Sie bitte im Zweifel der Beschreibung der Smartwatch. Zurzeit gilt, dass WatchOS ein iPhone mit iOS zur Kommunikation benötigt und Android Wear ein Smartphone mit Android und einer speziellen App benötigen. Besitzer einer Pebble Smartwatch können „mit beiden Welten" kommunizieren. Was geschieht mit den von der Smartwatch aufgenommenen Daten zur Aktivität und zum Puls? In der Regel sind die Daten nicht nur auf der Smartwatch gespeichert, sondern auch auf dem mit der Uhr gekoppelten Smartphone, um den Erfüllungsgrad von Trainingsprogrammen zu überwachen bzw. um dem Nutzer Tagesprofile zu seiner Aktivität anzuzeigen. Es gibt allerdings bereits Apps, welche die Gesundheitsdaten in deren Cloud speichern, z.B. Google Fit für Smartwatches mit Android Wear. Vorsicht: Einige Android-Smartwatches können bereits die Daten auch ohne das Smartphone direkt über WLAN in die Cloud laden.

Die Gefahren sind bei der Nutzung von Gesundheitsapps folgende: zum einen kann der Nutzer unbewusst oder ungewollt Daten an Google, Apple und Drittanbieter von Apps freigeben und zum anderen können die Daten auf dem Smartphone oder der Smartwatch durch Dritte eingesehen

40

werden. Laut Spiegel (Ausgabe 50/2015, Seite 15) geben einige Gesundheitsapps die vertraulichen Daten an bis zu 14 verschiedene Netzadressen weiter. Der Schnitt lag bei 5.

Was können Sie gegen ungewolltes Hochladen der Daten tun?

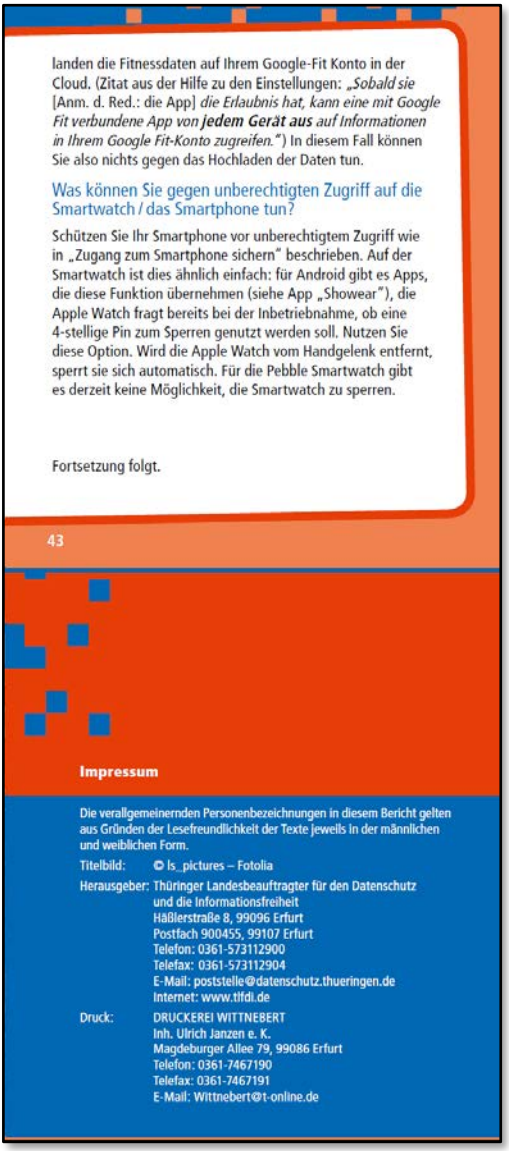
Hier hilft vor allen Dingen, sich vor der Nutzung einer Gesundheitsapp ausreichend zu informieren. Für das iPhone gibt es eine Schnittstelle, „HealthKit" genannt, welche die Daten zentral auf dem iPhone speichert. Die Steuerung der Datenzugriffe geschieht durch die App „Health". Durch eine weitere Schnittstelle, „ResearchKit" genannt, können die Daten auch an Apple übermittelt werden. Die Dokumenation zu ResearchKit finden Sie für Standardnutzer http://www.apple.com/de/researchkit/ und für tiefgreifendere Informationen für Entwickler http://researchkit.org/. In jedem Fall kann der Nutzer pro App entscheiden, welche Daten von welcher App einsehbar sind (http://www.apple.com/de/ios/health/).

Die Datenverarbeitung auf Android Smartphones ist meist app-basiert und nutzt nicht unbedingt, wie unter iOS auf iPhones, eine gemeinsame Basis zur Datenverwaltung. Hier muss der Nutzer pro Hersteller und eingesetzter App selbst

41

recherchieren, was mit den aufgenommenen Daten passiert, wo diese gespeichert sind und an wen diese Daten eventuell übertragen werden. Apps (auf der Smartwatch oder dem Smartphone), welche Google Fit benutzen, können über die Einstellung von Google-Fit (https://support.google.com/accounts/answer/6098255?hl=de) die Erlaubnis zum Zugriff auf die Daten gewährt oder entzogen werden. In jedem Fall

42



landen die Fitnessdaten auf Ihrem Google-Fit Konto in der Cloud. (Zitat aus der Hilfe zu den Einstellungen: *„Sobald sie* [Anm. d. Red.: die App] *die Erlaubnis hat, kann eine mit Google Fit verbundene App von* ***jedem Gerät aus*** *auf Informationen in Ihrem Google Fit-Konto zugreifen.“*) In diesem Fall können Sie also nichts gegen das Hochladen der Daten tun.

Was können Sie gegen unberechtigten Zugriff auf die Smartwatch / das Smartphone tun?

Schützen Sie Ihr Smartphone vor unberechtigtem Zugriff wie in „Zugang zum Smartphone sichern“ beschrieben. Auf der Smartwatch ist dies ähnlich einfach: für Android gibt es Apps, die diese Funktion übernehmen (siehe App „Showear“), die Apple Watch fragt bereits bei der Inbetriebnahme, ob eine 4-stellige Pin zum Sperren genutzt werden soll. Nutzen Sie diese Option. Wird die Apple Watch vom Handgelenk entfernt, sperrt sie sich automatisch. Für die Pebble Smartwatch gibt es derzeit keine Möglichkeit, die Smartwatch zu sperren.

Fortsetzung folgt.

43

Impressum

Die verallgemeinernden Personenbezeichnungen in diesem Bericht gelten aus Gründen der Lesefreundlichkeit der Texte jeweils in der männlichen und weiblichen Form.

Titelbild: © ls_pictures – Fotolia

Herausgeber: Thüringer Landesbeauftragter für den Datenschutz
und die Informationsfreiheit
Häßlerstraße 8, 99096 Erfurt
Postfach 900455, 99107 Erfurt
Telefon: 0361-573112900
Telefax: 0361-573112904
E-Mail: poststelle@datenschutz.thueringen.de
Internet: www.tlfdi.de

Druck: DRUCKEREI WITTNEBERT
Inh. Ulrich Janzen e. K.
Magdeburger Allee 79, 99086 Erfurt
Telefon: 0361-7467190
Telefax: 0361-7467191
E-Mail: Wittnebert@t-online.de

Stichwortverzeichnis

Vorbemerkungen zum Sprachgebrauch

Die verallgemeinernden Personenbezeichnungen in diesem Bericht gelten aus Gründen der Lesefreundlichkeit der Texte jeweils in der männlichen und weiblichen Form.

Impressum

Herausgeber:	Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit (TLfDI) Postfach 90 04 55, 99107 Erfurt Telefon: +49 (361) 57-3112900, Telefax: +49 (361) 57-3112904 E-Mail: poststelle@datenschutz.thueringen.de Internet: http://www.tlfdi.de
Druck:	THÜRINGER LANDESAMT FÜR BODENMANAGEMENT UND GEOINFORMATION
Layout Umschlag:	Druckerei Wittnebert, Erfurt Inh. Ulrich Janzen e. K. Internet: www.wittnebert.de
Endverarbeitung:	JVA Hohenleuben
Bildernachweis:	TLfDI
Redaktionsschluss:	31.05.2019