Tätigkeitsbericht 2015
des Unabhängigen Landeszentrums
für Datenschutz Schleswig-Holstein

BERICHTSZEITRAUM: 2013/2014

REDAKTIONSSCHLUSS: 15.02.2015

LANDTAGSDRUCKSACHE 18/2730

(35. TÄTIGKEITSBERICHT DES LANDESBEAUFTRAGTEN FÜR DATENSCHUTZ)

Dr. Thilo Weichert

Leiter des Unabhängigen Landeszentrums

für Datenschutz Schleswig-Holstein, Kiel

Impressum

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

(ULD SH)

Holstenstraße 98

24103 Kiel

Mail: mail@datenschutzzentrum.de

Web: www.datenschutzzentrum.de

Satz und Lektorat: Gunna Westphal, Kiel

Umschlaggestaltung: Martin Papp, Eyekey Design, Kiel

Druck: hansadruck, Kiel

Inhaltsverzeichnis

01

KERNPUNKTE

Modernes Informationsrecht

Die ULD-Dienststelle

1 Datenschutz und Informationsfreiheit in Schleswig-Holstein

Der Datenschutz in Schleswig-Holstein wird immer mehr geprägt durch nationale und europäische Vorgaben sowie durch das Internet und die hierüber bereitgestellten informationstechnischen Angebote. Für das Land bieten sich dabei enorme, viel zu wenig genutzte Gestaltungs- und Einflussmöglichkeiten.

1.1 Novellierung des Landesdatenschutzgesetzes

Das Landesdatenschutzgesetz (LDSG) wurde zuletzt Anfang 2012 geändert, um die europarechtlich geforderte Unabhängigkeit des Leiters des Unabhängigen Landeszentrums für Datenschutz (ULD) normativ abzusichern. Daneben erfolgten einige materiell-rechtliche Änderungen, z. B. zu Internetveröffentlichungen. Weiter gehende Änderungsvorschläge wurden vom Landtag nicht beschlossen (34. TB, Tz. 1.1). Nach Ansicht des ULD besteht weiterhin Novellierungsbedarf:

- Daten werden immer mehr ausschließlich elektronisch verarbeitet. Dies macht eine Verbesserung der Revisionssicherheit nötig, da anders eventuell vorgenommene Änderungen nicht mehr anhand einer Papierakte nachvollzogen werden können.
- Bisher erlaubt das LDSG gemeinsame Verfahren von Landesbehörden auf der Grundlage einer Rechtsverordnung. Der Bedarf an gemeinsamen Verfahren besteht auch auf kommunaler Ebene. Die dadurch mögliche Bündelung von Verantwortung würde zu einer starken Verwaltungsvereinfachung führen (Tz. 4.1.3).
- Behördliche Datenschutzbeauftragte können, müssen bisher aber nicht eingerichtet werden. Das Fehlen führt zu massiven Defiziten beim Datenschutzmanagement – bei kleinen Kommunen ebenso wie bei Ministerien.
- Derzeit gibt es keine gesetzliche Grundlage zur weitverbreiteten Verarbeitung von Steuerdaten durch Kommunen. Eine rechtliche Öffnung, ohne dass dabei das Steuergeheimnis gefährdet wird, ist geboten.

Weitere, eher redaktionelle Änderungen, etwa zur Begrifflichkeit oder zur Anwendbarkeit des Rechts, würden die Handhabbarkeit des LDSG weiter verbessern. Das ULD präsentierte die Änderungsvorschläge dem in der Regierung federführenden Innenministerium, den kommunalen Spitzenverbänden sowie Vertretern von Landtagsfraktionen. Den meisten Vorschlägen wurde zugestimmt. Die kommunalen Spitzenverbände kündigten aber ihren Widerstand gegen die verpflichtende Einrichtung behördlicher Datenschutzbeauftragter an und stellten in Aussicht, diese Änderung unter Verweis auf das Konnexitätsprinzip zu verhindern. Das Prinzip sieht vor, dass bei neuen gesetzlichen Aufgaben für die Kommunen die damit verbundenen Finanzen bereitgestellt werden müssen.

Das ULD legte dar, dass das Konnexitätsprinzip überhaupt nicht tangiert wird. Die obligatorische Bestellung behördlicher Datenschutzbeauftragter schafft keine neue Aufgaben, sondern regelt nur, wie diese wahrgenommen werden. Kommunen können die Aufgabe in Teilzeit erledigen lassen. Sie können sich hierfür auch zusammentun und einen gemeinsamen Beauftragten bestellen. Letztlich werden damit Kosten eingespart, da die ohnehin zu erledigenden Aufgaben – Vorabkontrolle, Umsetzung der Datenschutzverordnung, Mitarbeiterfortbildung und Datenschutzprüfungen – so von sachkundigen und zuverlässigen Personen wahrgenommen werden.

Herangezogene behördliche Datenschutzbeauftragte der Kommunen bestätigten diese Einschätzung des ULD. Dies führte bei den kommunalen Spitzenverbänden aber nicht zu einem Sinneswandel: Aus prinzipiellen Gründen wolle man auf die Konnexitätseinrede nicht verzichten.

Diese aus Sicht des ULD nicht nachvollziehbare Verweigerung führte bisher dazu, dass überhaupt keine inhaltliche Änderung des LDSG in Angriff genommen wurde. Konsequenz dessen ist, dass kommunale gemeinsame Verfahren nur mit großen rechtlichen Verrenkungen umgesetzt werden können. Die weitverbreitete Beauftragung Dritter

mit der Verarbeitung von kommunalen Steuerdaten bleibt schlicht rechtswidrig. Das ULD steht weiterhin zur Unterstützung der nötigen Änderungen bereit.

Was ist zu tun?

Die kommunalen Spitzenverbände sollten ihren Widerstand gegen den obligatorischen Datenschutzbeauftragten aufgeben. Die nötigen LDSG-Änderungen sind endlich umzusetzen.

1.2 „Lex Weichert“

Während sich das parlamentarische Interesse an den Inhalten des LDSG in Grenzen hielt, erregte die Streichung eines kurzen Satzes bzw. von zwei Worten in diesem Gesetz über viele Monate die Gemüter. Diese Änderung war schon anlässlich der 2011 verabschiedeten Gesetzesnovelle geplant. Nachdem zunächst alle datenschutzpolitischen Sprecher hierzu Zustimmung signalisiert hatten, besannen sich die damaligen Regierungsfraktionen neu.

§ 35 Abs. 1 LDSG alte Fassung

Der Landtag wählt ohne Aussprache die Landesbeauftragte oder den Landesbeauftragten für Datenschutz mit mehr als der Hälfte seiner Mitglieder für die Dauer von fünf Jahren. Die Wiederwahl ist nur einmal zulässig.

Die neuen Regierungsfraktionen brachten den Vorschlag ein, den Ausschluss der Wiederwahlmöglichkeit zu streichen. Ziel sollte es sein, dem bisherigen Amtsinhaber die Möglichkeit einer erneuten Kandidatur zu eröffnen. Insofern handelte es sich tatsächlich kurzfristig um einen „Lex Weichert“, wie dies von der Opposition genannt wurde. Diese lehnte den Vorschlag ab, weil die Amtszeitbeschränkung die unabdingbare Unabhängigkeit in dem Amt sichere. Vonseiten der Opposition wurde zudem vorgeschlagen, der Wahl der oder des Landesbeauftragten ein Auswahlverfahren vorzuschalten, bei dem nach einer öffentlichen Ausschreibung auf Vorschlag der Fraktion von einem Landtagsausschuss eine Vorauswahl durchgeführt würde. Der Ausschuss sollte alle oder ausgewählte Bewerbende in öffentlicher Sitzung anhören. Die Intention, durch ein offenes und öffentliches Auswahlverfahren möglichst fachkundige, erfahrene und unabhängige Personen für diese Aufgabe zu finden, wurde vom ULD unterstützt. Ein weiterer Vorschlag aus der Opposition des Landtags bestand darin, für die Wahl von Landesdatenschutzbeauftragten eine Zweidrittelmehrheit zu verlangen. Die Oppositionsvorschläge wurden vom Landtag verworfen, die mehrfache Wiederwahlmöglichkeit wurde beschlossen.

Bei der dann im Juli 2014 durchgeführten Wahl erhielt keiner der beiden Kandidaten die nötige absolute Mehrheit. Umgehend beantragten die Oppositionsfraktionen im Landtag, das Amt des Landesbeauftragten für Datenschutz in geeigneter Weise öffentlich auszuschreiben. Ende August 2014 endete die offizielle Amtszeit des bisherigen Amtsinhabers. Dieser nimmt seitdem das Amt kommissarisch wahr, wie dies das LDSG vorsieht.

1.3 Für ein modernes Transparenzrecht

Die Koalitionsvereinbarung der Regierungsparteien auf Landesebene betont gleich an mehreren Stellen die Bedeutung der Transparenz des Verwaltungshandelns für die demokratische Teilhabe und die Mitbestimmung der Bürgerinnen und Bürger und weist auf die digitalen Möglichkeiten bei Beteiligung und Dialog hin. Die Transparenz der Verwaltung wurde in diesem Zuge in Artikel 53 Verfassung des Landes Schleswig-Holstein aufgenommen. Damit wurde der Zugang zu amtlichen Informationen verfassungsrechtlich garantiert (Tz. 3.3).

In Hamburg wurde im Juni 2012 einstimmig ein Transparenzgesetz verabschiedet, mit dem die Verwaltung verpflichtet wird, verfügbare Informationen der Öffentlichkeit über das Internet bereitzustellen. Es geht damit über die Informationspflicht auf Antrag hinaus, wie sie auch in Schleswig-Holstein mit dem Informationszugangsgesetz besteht, und umfasst u. a. folgende Dokumente: Senatsbeschlüsse, Bürgerschaftsmitteilungen, Protokolle, Daseinsvorsorgeverträge, Organisations-, Geschäftsverteilungs- und Aktenpläne, Richtlinien, Fachanweisungen, Verwaltungsvorschriften, Statistiken, Gutachten, Studien, Geodaten, Umweltdaten, öffentliche Pläne, Subventions- und Zuwendungsvergaben oder wesentliche Unternehmensdaten städtischer Beteiligungen (34. TB, Tz. 1.3). Seit September 2014 lassen sich Millionen derartiger Dokumente online abrufen. Das öffentliche Interesse hieran ist enorm; die Resonanz auf das Angebot ist sehr gut. Die Informationsbereitstellung erfolgt mit Unterstützung von Dataport. In einigen Bundesländern bestehen Überlegungen, dem Hamburger Vorbild zu folgen.

Das ULD hat inzwischen Gespräche mit zivilgesellschaftlichen Initiativen, Parlamentariern und Angehörigen der Verwaltung geführt, welche Voraussetzungen geschaffen werden müssen, um ein derartiges Angebot auch für Schleswig-Holstein zu realisieren. Durch den städtischen Charakter und eine einheitliche Verwaltung, bei der elektronisches Dokumentenmanagement schon weit entwickelt ist, sind die Rahmenbedingungen für ein Transparenzregister in Hamburg günstiger als in einem Flächenland, dessen Verwaltung stark kommunal geprägt ist. Dies muss Schleswig-Holstein aber nicht davon abhalten, Vorbereitungen für eine aktive und systematische Bereitstellung von allgemeinen Verwaltungsinformationen zu treffen.

Hierbei kann auf die Erfahrungen in Hamburg zurückgegriffen werden. Bei der Etablierung von elektronischen Verfahren in der Verwaltung sollte darauf geachtet werden, dass Teile davon veröffentlichungsfähig gemacht werden können. Hierzu gehört, dass zwischen vertraulichen Informationen, etwa personenbezogener Art, und sonstigen Dokumenten unterschieden wird und dass Werkzeuge zur Anonymisierung und für die Recherchierbarkeit vorgesehen werden. Durch einen klaren rechtlichen Rahmen kann Verbindlichkeit bei der Verwaltung wie auch bei der interessierten Bevölkerung geschaffen werden. Auf die kommunale Selbstverwaltung und den unterschiedlichen Automatisierungsgrad in der Verwaltung sollte Rücksicht genommen werden. Dies kann dadurch erfolgen, dass den Kommunen die freiwillige Teilnahme an einem Landestransparenzregister angeboten und dass die informationstechnische Standardisierung in der Verwaltung gefördert wird.

Was ist zu tun?

Es sind die technischen, organisatorischen und rechtlichen Voraussetzungen für die aktive Bereitstellung von Verwaltungsinformationen auch in Schleswig-Holstein zu schaffen.

1.4 Die Dienststelle

Die strukturellen Rahmenbedingungen der Tätigkeit des ULD verändern sich stark. Damit einher gehen neue Erwartungen und Anforderungen. Waren Datenschutzbeauftragte ursprünglich Kontrollinstanzen zur Gewährleistung der Gesetzmäßigkeit der personenbezogenen Datenverarbeitung, so fiel ihnen immer mehr die Aufgabe eines umfassenden präventiven Datenschutzdienstleisters zu. Dieser Trend wurde für das ULD 2000 durch die neue Aufgabe „Informationsfreiheit“ bestätigt. Spätestens seit dem Urteil des Europäischen Gerichtshofes vom Mai 2014 zur Google-Suche kann nicht mehr geleugnet werden, dass den Datenschutzbehörden auch eine Wächterfunktion für die Wahrung der digitalen Meinungsfreiheit zugewachsen ist. Insofern erwies sich der schleswig-holsteinische Gesetzgeber als weitsichtig, als er 1991 die Beratung zu Fragen der Sozialverträglichkeit von Datenverarbeitung zu den Aufgaben des Landesbeauftragten machte.

Heute kann diese gesellschaftliche Aufgabe weiter gefasst mit digitalem Grundrechtsschutz beschrieben werden, zu dem sämtliche, insbesondere auch die demokratischen Grundrechte zu zählen sind. Nachdem Hinweise darauf bekannt wurden, dass

öffentliche deutsche Stellen personenbezogene Daten für sogenannte NATO-Todeslisten in Afghanistan übermittelt haben, bekommt selbst das grundgesetzliche Verbot der Todesstrafe eine digitale Komponente.

Digitaler Grundrechtsschutz bedeutet Parteinahme für den Menschen in der Informationsgesellschaft, der nicht nur von einem potenziell allwissenden Staat, dem „Big Brother", sondern auch von potenziell allwissenden privaten Unternehmen bedroht wird. Diese Parteinahme bedeutet nicht Parteilichkeit, sondern das Vertreten anderweitig nicht oder ungenügend organisierter Interessen und Werte. Diese Funktion kann nur bei weitgehender rechtlicher wie faktischer Unabhängigkeit wahrgenommen werden. Während diese Funktion von der öffentlichen Verwaltung des Landes und vielen Wirtschaftsunternehmen in Deutschland positiv aufgegriffen wird, zeigt sich – lokal in Schleswig-Holstein wie auch europaweit –, dass dominierende Informationstechnikunternehmen Datenschutzbehörden als Gegner statt als Partner behandeln.

Der Aufgabenzuwachs der Datenschutzbehörden ist schon seit Jahren in Schleswig-Holstein jedoch nicht mehr mit einer Ausstattung zusätzlicher finanzieller Ressourcen verbunden. Dies veranlasste das ULD, das seit 2007 aufgebaute Europäische Datenschutz-Gütesiegel in private Hände zu übertragen (Tz. 9.3). Damit ist keine Abkehr vom präventiven Ansatz des ULD verbunden, der zum Ausdruck kommt in einem umfassenden Beratungsangebot, dem Betrieb der DATENSCHUTZAKADEMIE Schleswig-Holstein (Tz. 13), drittmittelfinanzierten Forschungsprojekten zur Weiterentwicklung des Datenschutzes und datenschutzfreundlicher Technik (Tz. 8) sowie der Durchführung von Audit- und Gütesiegelverfahren (Tz. 9).

Das ULD erfüllt im Rahmen der Arbeitsteilung der deutschen Aufsichtsbehörden einige wichtige bundesweite Funktionen. Dies sind die Leitung des Arbeitskreises Sicherheit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, der Arbeitsgruppe Versicherungswirtschaft sowie der Unterarbeitsgruppe Geodaten und die Geschäftsführung des gemeinsam betriebenen virtuellen Datenschutzbüros als zentrales deutschsprachiges Datenschutzportal. Kooperationen erfolgen auch mit Verbraucherorganisationen, allen voran mit der Verbraucherzentrale Schleswig-Holstein und dem Verbraucherzentrale Bundesverband (vzbv), sowie Wirtschaftsverbänden, etwa der Digitalen Wirtschaft Schleswig-Holstein (DiWiSH) oder dem bundesweiten D21-Gütesiegel-Board.

Ende 2014 nahm das ULD einen Relaunch der eigenen Internetpräsentation vor. Die Masse der hierüber verfügbar gemachten Materialien und neue Möglichkeiten der Webseitenadministration legten diese Überarbeitung nahe. Mit den verfügbaren personellen Ressourcen war leider kein reibungsloser Übergang auf die neue Form der Präsentation möglich. Doch bietet die neue Webseitentechnik die Möglichkeit zu einer zukunftsoffenen Weiterentwicklung. Das ULD wird dauerhaft daran arbeiten, die Zugänglichkeit und Nutzbarkeit des Webangebotes zu verbessern, und nimmt insofern Anregungen gern entgegen. Um Informationsverluste zu vermeiden, wurden die Inhalte der alten Webseite eingefroren und sind unter den alten Deep Links weiterhin im Internet abrufbar.

https://www.datenschutzzentrum.de/uld-alt/index.html

1.5 Maulkorb für den Datenschutzbeauftragten?

Anfang 2012 berichtete die Zeitschrift „Der Spiegel", dass Apothekenrechenzentren nicht hinreichend anonymisierte Rezeptdaten an private medizinische Informationsdienstleister übermitteln, die diese für interessierte Stellen, insbesondere der Pharmaindustrie, in aufbereiteter Form bereitstellen. Dadurch ausgelöste Ermittlungen von Datenschutzaufsichtsbehörden bestätigten den Verdacht. Das insbesondere für schleswig-holsteinische Apotheken tätige Norddeutsche Apotheken-Rechenzentrum (NARZ) stellte umgehend seine pseudonyme Datenweitergabe ein und liefert nur noch aggregierte Daten an die Wirtschaft. Andere bundesweit, also auch in Schleswig-Holstein diese Apothekenleistung anbietende Unternehmen folgten diesem guten Beispiel nicht. Dies veranlasste den „Spiegel" im August 2013, erneut zu berichten und den Leiter des ULD damit zu zitieren, dass – unter Nennung des süddeutschen Hauptwettbewerbers des NARZ – es traurig wäre, „wenn die Dienstleister des Vertrauensberufs Apotheker erst durch Gerichtsprozesse zur Vertraulichkeit zu veranlassen wären". Es handele sich anscheinend um ein „lohnendes Geschäftsmodell"

durch „illegale Nutzung der Rezeptdaten“. Der Bericht provozierte weitere Presseanfragen beim ULD, anlässlich der diese Äußerungen bekräftigt wurden.

Das benannte Apothekenrechenzentrum in Süddeutschland, das ein Drittel aller deutschen Apotheken als Kunden hat, ließ daraufhin nichts unversucht, gegen die Äußerungen rechtlich vorzugehen, zunächst per Unterlassungsverpflichtungserklärung, dann per Antrag auf Erlass einer einstweiligen Anordnung. Tatsächlich entsprach das Verwaltungsgericht Schleswig (VG) diesem Antrag mit Beschluss vom November 2013. Es meinte, das ULD sei für die gemachten Äußerungen nicht zuständig; zuständig sei nur die lokale Aufsichtsbehörde, die das kritisierte Verfahren als rechtmäßig eingestuft hatte. Äußerungen über Unternehmen müssten anonymisiert erfolgen, eine kontroverse Diskussion unter Datenschutzbehörden müsse intern ausgetragen werden, auch wenn Apotheken in Schleswig-Holstein betroffen sind.

https://www.datenschutzzentrum.de/artikel/863-.html

Das im Beschwerdeverfahren angerufene Oberverwaltungsgericht Schleswig-Holstein (OVG) hob den Beschluss des VG in den wesentlichen Punkten auf und stellte das Recht des ULD zu öffentlicher Kritik wieder her. Ausdrücklich bestätigte das OVG, dass das ULD die nach seiner Ansicht rechtswidrige Praxis der Datenverarbeitung von Abrechnungszentren auch weiterhin als illegal und rechtswidrig bezeichnen dürfe, und dies sogar unter namentlicher Nennung. Es müsse allerdings die entsprechenden Äußerungen „als seine Auffassung kennzeichnen“ und dabei mit gebotener Sachlichkeit „zurückhaltend formulieren“. Das OVG blieb in seinem Beschluss allerdings die Antwort schuldig, worin die überzogene Argumentation zu sehen und weshalb diese nicht als ULD-Meinung zu erkennen gewesen sei. Das OVG vermied, ebenso wie schon das VG, eine inhaltliche Bewertung der vom ULD vorgelegten unstreitigen Fakten. Ungeachtet dessen ist mit dem Beschluss des OVG weiterhin eine qualifizierte öffentliche und kontroverse Datenschutzdebatte unter Beteiligung der Aufsichtsbehörden in Deutschland möglich.

https://www.datenschutzzentrum.de/uploads/medizin/apotheken/OVG-ULDvsVSA-28022014-anon.pdf

Soweit erkennbar, haben weder das süddeutsche noch weitere Apothekenrechenzentren ihre Übermittlungspraxis von nicht hinreichend anonymisierten Rezeptdaten beendet. Diese Praxis wird vom ULD weiterhin – anders als von einer süddeutschen Aufsichtsbehörde – als rechtswidrig bewertet (Tz. 4.6.8). Dieser sich täglich fortsetzende zigmillionenfache Datenschutzverstoß schädigt – nach Ansicht des ULD – nicht nur das Vertraulichkeitsversprechen der Apotheken, sondern auch die Marktsituation des NARZ als datenschutzkonform handelndes Rechenzentrum. Dass das ULD mit seiner Kritik auch in der Sache richtig liegt, mag man daraus ablesen, dass das betroffene in Süddeutschland gelegene Abrechnungszentrum die eigentliche gerichtliche Klärung bis heute vermieden hat. Es ging ihm offenbar nur darum, die öffentlich geäußerte Kritik einer Datenschutzaufsichtsbehörde, hier des ULD, zu unterbinden.

02

KERNPUNKTE

Edward Snowden

Europäischer Regelungsrahmen

IT-Sicherheitsgesetz

2 Datenschutz – global und national

Datenverarbeitung wird immer mehr geprägt und ist zugleich abhängig vom Internet. Dieses erweist sich durch Bereitstellung und Austausch von Daten, Bildern, Ton, Texten und Programmen als nützlich und segensreich für vieles: Information, Diskussion, Handel, politische Aktion, Vernetzung, Kunst, Unterhaltung und Spiel. Die Schattenseiten im Zusammenhang mit dieser Infrastruktur treten immer mehr ins öffentliche Bewusstsein: Ausforschung, Eindringen in die Privat- und Sozialsphäre, Spionage, Anprangerung, Diskreditierung, Rufmord, Manipulation, Desinformation, Werbebelästigung, Identitätsdiebstahl, Betrug. Das Netz kann zur Droge werden. Es ist Ziel und Mittel der digitalen Kriegsführung – des Cyberwarfare – geworden.

2.1 NSA, GCHQ und die deutsche Reaktion

Die Augen geöffnet über eine Schattenseite des Netzes hat seit Juni 2013 Edward Snowden. Dieser hatte umfangreiche Dokumente der Geheimdienste der USA und Großbritanniens – der National Security Agency (NSA) und des Government Communications Headquarters (GCHQ) – kopiert und diese verantwortungsbewussten Journalisten zur Auswertung und Veröffentlichung zur Verfügung gestellt. Damit hat er Licht in das Schattenreich dieser und anderer Geheimdienste gebracht, in dem täglich millionenfach gravierende Verletzungen des Rechts auf informationelle Selbstbestimmung stattfanden und weiterhin stattfinden. Mit den transparent gemachten Praktiken verletzen diese Geheimdienste nicht nur nationales Recht, sondern auch das Grundrecht auf Datenschutz gemäß Artikel 8 der Europäischen Grundrechtecharta und – wie der Menschenrechtsausschuss der Vollversammlung der Vereinten Nationen (UNO) im November 2013 festgestellt hat – auf Privatheit, wie es in Artikel 12 der Allgemeinen Erklärung der Menschenrechte und in Artikel 17 des Internationalen Paktes für zivile und politische Rechte gewährleistet ist.

Das Erstaunen über die Praktiken von NSA und GCHQ hielt sich im ULD in Grenzen – waren doch die technische und personelle Ausstattung dieser Geheimdienste, die für diese geltenden gesetzlichen Regelungen und deren Missachtung der informationellen Menschenrechte seit Langem bekannt. Erschreckend waren dann jedoch das Ausmaß der Überwachung und die Kaltschnäuzigkeit, mit der die Menschenrechtsverstöße begangen, gerechtfertigt und für die Zukunft angekündigt wurden. Erschreckend war auch die politische Reaktion der deutschen Politik auf diese Völkerrechtsverletzungen. Die Empörung beschränkte sich auf Oppositionspolitik; die offizielle Regierungspolitik gegenüber den verantwortlichen Staaten und Institutionen vermittelt den Eindruck, die verletzten Regeln seien disponibel.

Deutschland und Europa waren und sind aufgefordert, ein klares aktives Zeichen zu setzen gegen die globale Ausforschung durch NSA und GCHQ. Eine Vielzahl von diplomatischen, rechtlichen, organisatorischen, infrastrukturellen und technischen Maßnahmen war und ist weiterhin geboten. Einige Schritte wurden getan, etwa die Initiierung der erwähnten UNO-Resolution durch die Bundesregierung. Die praktisch wie auch symbolisch vielleicht wichtigste Maßnahme zur Verteidigung des Grundrechtes auf Datenschutz wäre es aber gewesen und ist es weiterhin, Edward Snowden in Deutschland und in Europa Schutz vor der Verfolgung durch die USA zu gewähren. Diese vom ULD im Juli 2014 aufgestellte Forderung wurde im November 2014 vom Schleswig-Holsteinischen Landtag mehrheitlich bekräftigt:

„Der Landtag bittet die Bundesregierung, dem Whistleblower Edward Snowden entweder einen sicheren Aufenthalt auf Grundlage des § 22 Aufenthaltsgesetz (AufenthG) in der Bundesrepublik Deutschland zu ermöglichen, da dies der Wahrung politischer Interessen der Bundesrepublik Deutschland dient, oder sich auf der Ebene der Europäischen Union für einen sicheren Aufenthalt in einem Mitgliedsland seiner Wahl einzusetzen. Dabei sind vorab alle rechtlichen Möglichkeiten zu prüfen und gegebenenfalls wahrzunehmen, die eine Auslieferung an die Vereinigten Staaten von Amerika oder andere Staaten wegen der von ihm veröffentlichten Geheimdokumente sicher ausschließen."

Die Forderung blieb bis heute unerfüllt. Es ist eine Schande, dass ein Aufklärer dort Schutz suchen muss, wo alles Mögliche zu Hause ist, nur nicht der

Schutz der Menschenrechte. Die EU und Deutschland bekennen sich feierlich zu den Grundrechten und zu den Werten der Aufklärung und erklären sich zum „Raum des Rechts der Sicherheit und der Freiheit". Zugleich verweigern sie einem Aufklärer, der sich zu diesen Prinzipien bekennt und sich für diese verdient gemacht hat wie kaum ein anderer, die Aufnahme in diesem Raum. Das ULD hat dargelegt, dass nicht nur eine moralische Pflicht, sondern im Interesse des Grundrechtsschutzes eine verfassungsrechtliche Pflicht der Bundesregierung besteht, durch die Aufnahme von Edward Snowden die Informationsgrundlage für den weiteren künftigen Grundrechtsschutz zu schaffen.

https://www.datenschutzzentrum.de/artikel/208-.html

Die Enthüllungen Snowdens hatten massive Auswirkungen auf die Tätigkeit des ULD. Die sich hierauf beziehenden Anfragen von Bürgerinnen und Bürgern, von Medien und aus der Verwaltung zeugen davon, dass viele aus den Erkenntnissen Konsequenzen zu ziehen bereit sind. Nachfragen bezogen sich insbesondere auf Möglichkeiten des Selbstschutzes, insbesondere auf Hilfen zur Verschlüsselung. Sehr erfreulich war aus ULD-Sicht die große Anzahl von Anfragen aus der heimischen Wirtschaft, bei der die Snowden-Erkenntnisse dazu führten, sich intensiver mit Datenschutz zu befassen.

Was ist zu tun?

Die deutsche Bundesregierung sollte Edward Snowden sichere Einreise und sicheren Aufenthalt in Deutschland gewähren.

2.2 Europäische Datenschutz-Grundverordnung

Wenngleich vor den Enthüllungen von Edward Snowden gestartet, ist die Europäische Datenschutz-Grundverordnung (EU-DSGVO) eine wichtige Teilantwort der Europäischen Union (EU) auf die mit seiner Hilfe veröffentlichten Fakten: Europa braucht ein einheitliches Datenschutzrecht mit einem hohen Standard, um ein gemeinschaftliches Gegengewicht gegen die insbesondere von den USA ausgehenden Datenschutzverstöße aufzubauen. Die EU-DSGVO ist der zentrale Teil einer geplanten umfassenderen europäischen Datenschutzreform, zu der auch der Entwurf einer Richtlinie „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr", also für den Datenschutz im Bereich Inneres und Justiz, gehört. Die Kommission stellte ihre Vorstellungen im Januar 2012 vor. Im Dezember 2012 präsentierte der Berichterstatter des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments (EP) seine Vorschläge, zu denen über 3.000 Änderungsanträge eingebracht wurden. Im Oktober 2013 einigte sich der Ausschuss auf das Reformpaket, das im März 2014 durch das Plenum des EP beschlossen wurde. Den Stand der Verhandlungen des Europäischen Rats fasst ein über 230 Seiten starkes Dokument vom Dezember 2014 zusammen.

Mit dem Beschluss des EP werden einige zentrale Defizite des Kommissionsvorschlages behoben. So soll die Macht der Kommission zugunsten eines kooperativen Entscheidungsprozesses des Europäischen Datenschutzausschusses zurückgedrängt werden. Das Verfahren der gegenseitigen Abstimmung der Datenschutzaufsichtsbehörden – das sogenannte Kohärenzverfahren – wird praktikabler gestaltet. Für die Zertifizierung sind verbindlichere Regelungen vorgesehen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder intervenierte immer wieder in der europaweit geführten Diskussion.

https://ssl.bremen.de/datenschutz/sixcms/detail.php?gsid=bremen236.c.9473.de

https://ssl.bremen.de/datenschutz/sixcms/detail.php?gsid=bremen236.c.7665.de

Dies war insbesondere notwendig, weil die Bundesregierung sich im Rat als einer der Hauptbremser in den Diskussionen mit dem fragwürdigen Argument profilierte, der hohe deutsche Daten-

schutzstandard dürfe nicht verloren gehen. Zugleich betätigte sich das im Bund federführende Ministerium des Innern als Sprachrohr für einen „risikobasierten" Regelungsansatz, mit dem das europaweit anerkannte Verbot mit Erlaubnisvorbehalt im Bereich der nicht öffentlichen personenbezogenen Datenverarbeitung aufgehoben werden soll. Dieses in den USA geltende Prinzip würde dazu führen, dass Unternehmen nur dann bei der Verarbeitung von Personendaten eingeschränkt wären, wenn dies durch spezifische Normen zur Verhinderung besonders benannter Risiken vorgesehen ist. Es sind Vertreter der US-Regierung sowie Lobbyisten der US-Unternehmen wie Google und Facebook, die hierfür trommeln. Dieser Ansatz steht im Widerspruch zur Rechtsprechung des Bundesverfassungsgerichtes und zur Europäischen Grundrechtecharta, die in Artikel 8 ein Grundrecht auf Datenschutz gewährleistet, das in einer globalen Informationsgesellschaft insbesondere auch von Privatfirmen gefährdet wird. Angesichts der technischen Möglichkeiten des Sammelns, Auswertens und Nutzens von Personendaten gilt die Feststellung des Bundesverfassungsgerichtes aus dem Jahr 1983 mehr denn je: Unter den Bedingungen der automatisierten Datenverarbeitung gibt es kein „belangloses" Datum mehr.

Signale aus dem Bundesministerium des Innern berechtigen zur Hoffnung, dass Deutschland seine bisherige Blockadehaltung aufgibt. Es geht nun darum, möglichst noch im Jahr 2015 im Rahmen der trilateralen Gespräche eine Einigung zu finden, sodass spätestens im Jahr 2017 die EU-DSGVO in Kraft treten kann.

Da von der EU-DSGVO eine ganzheitliche Regelung angestrebt wird, die für den öffentlichen wie für den nicht öffentlichen Bereich gilt, wird die Verordnung erhebliche Auswirkungen auf das Datenschutzrecht der deutschen Bundesländer haben. Dies bedeutet jedoch nicht das Aus für das Landesdatenschutzgesetz Schleswig-Holstein und für bereichsspezifische Landesgesetze. Vielmehr ist davon auszugehen, dass dem Landesgesetzgeber im öffentlichen Bereich im Sinne der Subsidiarität ein Regelungsrahmen geöffnet bleibt, der mit den bisherigen Regelungen weitgehend gefüllt werden kann. Ja, mehr als dies: Die Landes- und der Bundesgesetzgeber haben jetzt noch die Chance, durch innovative Regelungsansätze die europäische Diskussion mit zu beeinflussen.

Was ist zu tun?

Alle Beteiligten sind aufgefordert, durch eine qualifizierte intensive Diskussion dafür zu sorgen, dass so schnell wie möglich ein einheitlicher hoher Datenschutzstandard in Europa über eine Datenschutz-Grundverordnung zur Anwendung gebracht wird.

2.3 IT-Sicherheitsgesetz

Das Bundesministerium des Innern (BMI) veröffentlichte im August 2014 den Entwurf eines IT-Sicherheitsgesetzes. Dessen Anliegen – das Etablieren von Meldeverfahren bei Sicherheitsvorfällen, die informationstechnische Absicherung kritischer Infrastrukturen und die Etablierung und Umsetzung von einheitlichen hohen Standards im Bereich der Informationssicherheit – wird vom ULD nachdrücklich begrüßt.

Im Detail sieht das ULD jedoch starken Korrekturbedarf. Dieser basiert auf der nicht zutreffenden Annahme der Entwürfe, die Meldung und die Vorbeugung von IT-Sicherheitsangriffen ließe sich ohne die Verarbeitung personenbeziehbarer Daten realisieren. Dass dies nicht zutrifft, hat das ULD in der Studie zum „Monitoring durch Informationsfusion und Klassifikation zur Anomalieerkennung" (Tz. 8.4.1) dargelegt. Das Bestreben nach IT-Sicherheit und der Datenschutz in globalen Netzen bedürfen einer engen Verzahnung, die sich im IT-Sicherheitsgesetz widerspiegeln muss. Es droht anderenfalls eine Vorratsdatenspeicherung von Telekommunikationsnutzungsdaten über die Hintertür der IT-Sicherheitsvorsorge.

IT-Sicherheit deckt den Schutz des Rechts auf informationelle Selbstbestimmung nicht ab. Es ist aber auch ein Irrtum, dass IT-Sicherheit und Datenschutz nichts oder wenig miteinander zu tun

hätten. Auf dieser Annahme basieren die bisherigen Entwürfe. IT-Sicherheit kann zum Datenschutz in einem Spannungsverhältnis stehen. Dem muss durch Regelungen, die Transparenz und Datensparsamkeit in ein optimiertes Verhältnis zueinander bringen, Rechnung getragen werden. In dem im Dezember 2014 vom Bundeskabinett beschlossenen Entwurf wurde zwar eine bisher vorgesehene Regelung gestrichen, in der Telemedienanbieter verpflichtet werden, aus Sicherheitsgründen Nutzungsdaten zu speichern (BR-Drs. 643/14). Die darüber hinausgehenden, vom ULD benannten grundlegenden Defizite wurden aber noch nicht behoben. Wird zum Zweck der Erhöhung der IT-Sicherheit der Netzverkehr auf Risiken analysiert, kommt es zwangsläufig zur Speicherung von personenbeziehbaren Nutzungsdaten. Der im Gesetzgebungsverfahren befindliche Entwurf schafft hierfür und für die weitere Verarbeitung bisher aber keine hinreichend normenklaren und verhältnismäßigen Eingriffsgrundlagen.

Die ULD-Stellungnahme schlägt deshalb vor,

- für die zu IT-Sicherungsmaßnahmen notwendige personenbezogene Datenverarbeitung hinreichend bestimmte und verhältnismäßige Befugnisgrundlagen zu schaffen und
- die Bestrebungen des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) mit denen der Datenschutzaufsicht in Deutschland zu koordinieren.

https://www.datenschutzzentrum.de/artikel/877-.html

Was ist zu tun?

Im Gesetzgebungsverfahren muss der Entwurf für ein IT-Sicherheitsgesetz überarbeitet werden.

2.4 Für einen gesetzlichen Schutz von Whistleblowern

Seit Jahren wird in Deutschland – bisher erfolglos – über eine gesetzliche Verbesserung des Schutzes von Whistleblowern diskutiert. Die Bundesrepublik wurde im Juli 2011 vom Europäischen Gerichtshof für Menschenrechte (EGMR) im exemplarischen Fall „Heinisch“ wegen eines Verstoßes gegen die Freiheit der Meinungsäußerung verurteilt, nachdem eine Whistleblowerin erfolglos vor nationalen Gerichten gegen eine fristlose Kündigung vorgegangen war. Whistleblower sind Insider, in der Regel Arbeitnehmerinnen oder Arbeitnehmer, die aufgrund konkreter Anhaltspunkte im Zusammenhang mit der eigenen Tätigkeit zu der Überzeugung kommen, dass es in ihrem Umfeld zu Rechtsverstößen oder sonstigen gravierenden Missständen gekommen ist oder kommen wird, die intern mit ihren Hinweisen auf kein Gehör stoßen und sich daraufhin zur Verhinderung bzw. zum Abstellen des Missstands an Externe oder gar an die Öffentlichkeit wenden.

Ein solches Verhalten liegt im Interesse einer freiheitlichen, rechtsstaatlichen und demokratischen Gesellschaft. Der EGMR hat bekräftigt, dass dieses Verhalten schutzbedürftig ist. Bisher schützt unsere Rechtsordnung diejenigen, die unter dem Siegel von Verschwiegenheitspflichten gegen rechtliche oder gesellschaftliche Normen verstoßen. Letztlich werden Täter geschützt; diejenigen, die eine Tat aufklären, dürfen bestraft werden. Der Fall von Edward Snowden zeigt anschaulich, welche wichtige globale Funktion Whistleblowern zukommen kann. Zwar könnte die Bundesrepublik Snowden Schutz gewähren, ein rechtlicher Anspruch auf einen solchen Schutz lässt sich aber kaum begründen.

Selbstverständlich muss eine gesetzliche Regelung Sicherungen vorsehen, damit der Whistleblower-Schutz nicht missbraucht wird. Es bedarf für eine Verletzung von Geheimhaltungspflichten konkreter Anhaltspunkte; ein purer Verdacht kann nicht genügen. Zunächst muss intern Abhilfe angestrebt werden; nur wenn diese erfolglos ist oder wäre, kann und darf nach außen gegangen werden. Hierbei kann auch eine Abwägung zwischen dem – vermeintlichen – Missstand und den Folgen einer Veröffentlichung gefordert werden, wobei die Art und der Adressat der Preisgabe relevant sind. Da Whistleblower aber keine juristischen Experten sind, darf diese Anforderung nicht zu hoch sein. Der Schutz sollte sich insbesondere auf arbeitsrechtliche Folgen beziehen, ohne sich hierauf zu beschränken.

Auch ohne gesetzliche Regelung besteht die Möglichkeit, das Whistleblowing zu erleichtern, indem vertrauliche Wege zur Abgabe einer Beschwerde, die dann unabhängig und qualifiziert überprüft wird, eingerichtet werden. Im Hinblick auf Datenschutzverstöße besteht über die Datenschutzbeauftragten ein solcher Weg. Auch mit – zertifizierungsfähigen – elektronischen Meldeverfahren kann das Whistleblowing erleichtert und gefördert werden (Tz. 9.2.1).

Was ist zu tun?

Der Schutz von Whistleblowern sollte gesetzlich und durch die Einrichtung von vertraulichen Meldeverfahren verbessert werden.

2.5 Dopingbekämpfung – bitte datenschutzgerecht

Das Dilemma, in dem sich Sportlerinnen und Sportler, die an internationalen Wettbewerben teilnehmen wollen, befinden, hat sich nicht aufgelöst: Wenn sie nicht bereit sind, sich einer datenschutzwidrigen und teilweise entwürdigenden Prozedur bei den Dopingkontrollen und der dauernden Überwachung der Aufenthalte, der sogenannten Whereabouts, zu unterwerfen, wird ihnen gemäß dem weltweit vereinbarten Verfahren die Teilnahme an den Wettkämpfen verweigert (34. TB, Tz. 5.8). Von der Freiwilligkeit der eingeholten Einwilligungen kann keine Rede sein. Gespräche des ULD mit dem Landessportverband Schleswig-Holstein sowie auf Bundesebene – gemeinsam mit anderen Aufsichtsbehörden – mit der Nationalen Anti-Doping-Agentur (NADA) und dem Deutschen Olympischen Sportbund zeigten, dass den Sportfunktionären nicht wohl in ihrer Haut ist wegen der Eingriffe in die Privatsphäre der Sporttreibenden; doch Lösungen wurden – soweit erkennbar – nicht angegangen.

Im Spätsommer 2014 wurde ein erster Referentenentwurf des Gesetzes zur Bekämpfung von Doping im Sport bekannt, dessen erklärte Zielsetzung in der Bekämpfung des Einsatzes von Doping liegt, um die Gesundheit der Sportlerinnen und Sportler zu schützen, die Fairness und Chancengleichheit bei Sportwettbewerben zu sichern und damit die Integrität des Sports zu fördern. Hierzu sind in dem Entwurf Strafvorschriften vorgesehen sowie Regelungen, wie Anti-Doping-Ermittlungen unter Einbeziehung der NADA durchzuführen sind. Beim Verdacht gewerbs- oder bandenmäßigen Vorgehens der Doper und ihrer Helfeshelfer sollen gar Telekommunikationsüberwachungsmaßnahmen erlaubt werden.

Unter Federführung von Rheinland-Pfalz und Schleswig-Holstein verfassten die Datenschutzaufsichtsbehörden eine erste Stellungnahme gegenüber den zuständigen Bundesministerien des Innern und der Justiz, die den Regulierungsansatz begrüßt. Hinsichtlich der Normen zur Datenverarbeitung sind jedoch erhebliche Präzisierungen nötig. Für Jugendliche und bei Gesundheitsdaten sind besondere Schutzregeln aufzustellen. Es wird vorgeschlagen, unterhalb der verfassungsrechtlich per Gesetz regulierungsbedürftigen Wesentlichkeitsschwelle nach dem BDSG vorgesehene Verhaltensregeln festzulegen. Diese könnten dann international als Vorbild dienen.

Was ist zu tun?

Nach offizieller Vorlage des Entwurfes für ein Anti-Doping-Gesetz muss nach einer öffentlichen Diskussion gesetzlich festgeschrieben werden, wie Dopingbekämpfung und der Persönlichkeitsschutz optimal in Einklang zu bringen sind.

03

KERNPUNKTE

Datenschutzaudit des Landtags

Landesverfassung

3 Landtag

3.1 Auditierung Zutrittsberechtigungssystem und Videoüberwachung im Landtag

2014 wurden das Zutrittsberechtigungssystem und die Videoüberwachung des Landtags rezertifiziert. In beiden Bereichen müssen Sicherheitsaspekte und Privatsphäre von Abgeordneten und Besuchern des Landeshauses zu einem Ausgleich gebracht werden.

Das Zutrittsberechtigungssystem des Landtags wurde erstmalig 2004 vom ULD zertifiziert (27. TB, Tz. 3.1), die Videoüberwachung 2006 (29. TB, Tz. 3.1). Seit der letzten Rezertifizierung 2010 (33. TB, Tz. 3) wurden einige Änderungen an der eingesetzten Hardware vorgenommen. Insbesondere wird jetzt ein moderneres und sichereres Kartensystem eingesetzt. Weiterhin wird verhindert, dass Bewegungsprofile von Nutzern dieser Karten, insbesondere von Mitarbeitern des Landeshauses und Abgeordneten, erfasst werden. Hinsichtlich der Videoüberwachung des Außenbereichs des Geländes lag ein Augenmerk darauf, dass nicht relevante Bereiche ausgeblendet werden und die Speicherfristen auf das notwendige Maß reduziert wurden. Die Fehlerkontrolle wurde unter Einbeziehung des Datenschutzgremiums des Landtags verbessert. Die Auditierung im Landtag zeigt, dass Sicherheit und Privatsphäre kein unüberwindlicher Widerspruch sind.

Was ist zu tun?

Andere Stellen, die Zutrittssysteme und Videoüberwachung einsetzen, sollten sich am Landtag orientieren und die Möglichkeit einer Auditierung prüfen.

3.2 Unterrichtung eines Landtagsabgeordneten

Ein Abgeordneter bat das Innenministerium des Landes im Zuge der Diskussion um Gefahrengebiete nach dem Polizeirecht um Informationen über Anordnungen solcher Gebiete und deren Gründe. Die Gefahrengebietsausweisungen hatten unterschiedliche Kriminalitätslagen zum Hintergrund und reichten vom Einbruchsdiebstahl über Sexualdelikte und Fußballrowdytum bis hin zur Rockerkriminalität. Das Ministerium übermittelte die erbetenen Unterlagen – über hundert Seiten als PDF-Anhang – per unverschlüsselter E-Mail an die private Adresse des Abgeordneten. Dabei handelte es sich um tabellarische Überblicke sowie um ausführliche Begründungen der Anordnungen, die teilweise als „Verschlusssache – nur für den Dienstgebrauch“ (VS NfD) gekennzeichnet waren. Fast alle Nennungen von Personen – von sachbearbeitenden und leitenden Polizeibeamten und anordnenden Richterinnen und Richtern – waren schwarz markiert. Beim Einscannen wurde aber nicht verhindert, dass die händisch vorgenommenen Schwärzungen weiterhin lesbar blieben.

Der Landtagsabgeordnete veröffentlichte die Unterlagen auf seiner persönlichen Webseite. Dies löste Empörung aus, weil manche hierin eine Gefährdung der unzureichend geschwärzten Funktionsträger sahen. Der Vorgang war Gegenstand der Erörterungen des Datenschutzgremiums des Landtags. Dieses bat das ULD um die datenschutzrechtliche Bewertung der Datenübermittlung vom Innenministerium an den Abgeordneten, der die Informationen in seiner politischen Funktion, nicht als Privatperson erhalten hatte.

Während bei verwaltungsinternen Datenübermittlungen strenge Anforderungen an die Erforderlichkeit gestellt werden müssen, ist dies bei der Beantwortung von parlamentarischen Anfragen nicht möglich, da den Abgeordneten ein Beurtei-

lungsspielraum eingeräumt werden muss, was für deren Gesetzgebungs- und Kontrolltätigkeit erforderlich ist. Die Landesregierung ist verfassungsrechtlich zur Auskunft gegenüber der Legislative verpflichtet, nicht aber, wenn „gesetzliche Vorschriften oder Staatsgeheimnisse oder schutzwürdige Interessen Einzelner, insbesondere des Datenschutzes, entgegenstehen". Parlamentarier sind selbst zur Vertraulichkeit verpflichtet. Öffentliche Bedienstete müssen es hinnehmen, dass ihre Tätigkeit als Funktionsträger im Bedarfsfall auch namentlich vom Parlament kontrolliert wird.

Im konkreten Fall ist einiges schiefgegangen: Werden aus Datenschutzgründen Schwärzungen vorgenommen, so muss dies dazu führen, dass Namen nicht gelesen werden können, anderenfalls haben wir es eher mit Hervorhebungen zu tun. Angesichts der Menge der zu anonymisierenden Inhalte kann es leicht dazu kommen, dass nötige Schwärzungen vergessen oder übersehen werden. Dies war konkret der Fall. Ob die als VS-NfD eingestuften Dokumente tatsächlich so eingestuft werden mussten, ist zumindest fraglich. Will ein Absender, dass ein Empfänger eine Information in einer besonderen Form vertraulich behandelt, so sollte hierauf explizit hingewiesen werden. Bei der Übermittlung sensibler Unterlagen muss aber in jedem Fall eine Verschlüsselung erfolgen; Empfänger sollte eine offizielle, keine private Adresse sein; bei einer verwaltungsinternen Kommunikation sollte das besonders geschützte Landesnetz genutzt werden.

Das Datenschutzgremium des Landtags bewertete in eigener Zuständigkeit das Vorgehen des Abgeordneten. Zweifellos gehört es zu den Aufgaben von Abgeordneten, ihre Aktivitäten, auch soweit sie die Kontrolle der Verwaltung betreffen, für die Öffentlichkeit transparent zu machen, um diese dem demokratischen Diskurs zuzuführen. Dabei sind aber Geheimhaltungs- und Vertraulichkeitsbedürfnisse immer mit zu berücksichtigen.

3.3 Digitale Herausforderungen an die Landesverfassung

Im Dezember 2014 trat eine sehr weitgehende Änderung der Verfassung des Landes Schleswig-Holstein in Kraft. Dem waren umfassende Anhörungen und Beratungen des Landtags und dessen Sonderausschusses Verfassungsreform vorausgegangen. Da mit der Novelle auch den Herausforderungen der digitalen Gesellschaft begegnet werden sollte, gab das ULD eine Stellungnahme ab, in der darauf hingewiesen wurde, dass schon anlässlich der Verfassungsdebatte im Jahr 1997 der Landesbeauftragte für Datenschutz eine Regelung zur „Teilhabe an der Informationsgesellschaft" ohne Erfolg vorgeschlagen hatte. Bestehenden grund- bzw. menschenrechtlichen Defiziten sollte vorrangig mit nationalem oder gar internationalem Recht abgeholfen werden. Nachdem das Grundgesetz als deutsche Verfassung diesbezüglich noch keiner Überarbeitung unterzogen worden ist, kommt der Europäischen Grundrechtecharta eine zentrale Funktion zu, in der Grundrechte gemäß den modernen gesellschaftlichen und technischen Anforderungen zugesichert werden, u. a. der Schutz personenbezogener Daten und das Recht auf Zugang zu Dokumenten.

Insofern bleibt auch Landesverfassungen eine wichtige Funktion, nicht zuletzt als Vorbild für eine Überarbeitung der nationalen Verfassung. Die vom Landtag beschlossene Novellierung der Landesverfassung taugt tatsächlich als Vorbild: In einem Artikel 14 wird der Aufbau, die Weiterentwicklung und der Schutz digitaler Basisdienste und die Teilhabe der Bürgerinnen und Bürger sowie ein Benachteiligungsverbot beim Zugang zu Behörden und Gerichten gewährleistet. Mit Artikel 15 wird die digitale Privatsphäre der Bürgerinnen und Bürger geschützt. Und Artikel 53 sichert Transparenz zu: „Die Behörden des Landes, der Gemeinden und Gemeindeverbände stellen amtliche Informationen zur Verfügung, soweit nicht entgegenstehende öffentliche oder schutzwürdige private Interessen überwiegen. Das Nähere regelt ein Gesetz." Die Stellungnahme des ULD findet sich unter

http://www.landtag.ltsh.de/infothek/wahl18/umdrucke/2300/umdruck-18-2300.pdf

04

KERNPUNKTE

Vertrauenswürdiges E-Government

Sicherheit durch Datenverarbeitung

Berufsgeheimnisschutz

4 Datenschutz in der Verwaltung

4.1 Allgemeine Verwaltung

4.1.1 E-Government-Gesetz des Bundes

Anfang 2012 wurden die Datenschutzbeauftragten über den Entwurf eines Gesetzes zur Förderung der elektronischen Verwaltung informiert. Ziel des kurz „E-Government-Gesetz“ genannten Regelwerks ist die Schaffung der rechtlichen Voraussetzungen für eine rechtssichere elektronische Kommunikation für die öffentliche Verwaltung untereinander wie auch mit den Bürgerinnen und Bürgern. Selbst nach intensiver Überzeugungsarbeit blieb der Gesetzentwurf viele datenschutzrechtliche Wünsche schuldig, sodass das ULD im Mai 2013 versuchte, den Bundesrat über das Land zu Nachbesserungen zu veranlassen.

Es fehlte eine Verpflichtung für die Behörden zur Entgegennahme verschlüsselter Kommunikation. Die vorgesehene Kommunikation gemäß dem De-Mail-Gesetz sieht bisher keine zwingende Ende-zu-Ende-Verschlüsselung vor, wie sie etwa für die Übermittlung von Steuergeheimnissen verpflichtend ist (Tz. 6.2.1). Eine Nutzung von Pseudonym-Adressen ist nicht vorgesehen. Eine differenzierte fachanwendungsspezifische Zugangsmöglichkeit fehlte ebenso wie eine Regelung zum datenschutzkonformen Veröffentlichen von Daten im Internet, wie sie im LDSG besteht. In den nebengesetzlichen Regelungen wurde für das Sozialgesetzbuch vorgesehen, dass die Kommunikation zwischen Krankenkassen und Versicherten eine Authentisierung über die elektronische Gesundheitskarte erlaubt, die hierfür nicht konzipiert ist.

https://www.datenschutzzentrum.de/artikel/865-.html

Im Juli 2013 wurde das Gesetz ohne die geforderten Verbesserungen beschlossen. Das Gesetz ist auch für Behörden der Länder und der Kommunen anwendbar, wenn diese Bundesrecht ausführen. Hierzu gehört z. B. die Entgegennahme von mit qualifizierter Signatur versehenen Dokumenten oder die Ermöglichung eines elektronischen Bezahlverfahrens. Der Bund hat wegen der nötigen Einheitlichkeit bei der elektronischen Kommunikation der Verwaltung eine gewisse faktische Führungsrolle. Soweit die Forderungen der Datenschutzbeauftragten nicht umgesetzt wurden, bleiben diese auf der Tagesordnung. Dies gilt insbesondere für die Entgegennahme verschlüsselter elektronischer Kommunikation und die Ende-zu-Ende-Verschlüsselung. Letztere ist angesichts der umfassenden Kommunikationsüberwachung durch Geheimdienste ein absolutes Muss zur Sicherstellung einer vertrauenswürdigen Kommunikation mit Bürgerinnen und Bürgern.

Was ist zu tun?

Das E-Government-Gesetz ist in der Verwaltung umzusetzen. Darüber hinausgehend sind Maßnahmen zur Gewährleistung einer vertrauenswürdigen elektronischen Kommunikation nötig.

4.1.2 E-Government-Rahmenvertrag zwischen Dataport und CSC

Durch Presseberichte wurde bekannt, wie intensiv das US-amerikanische Unternehmen CSC mit US-Geheimdiensten und insbesondere mit der NSA kooperiert. CSC hat eine 100%ige Tochter in Deutschland, mit welcher der öffentliche für Kommunen und das Land tätige IT-Dienstleister Dataport einen E-Government-Rahmenvertrag abgeschlossen hat. Es bestand die nicht unbegründete Befürchtung, dass im Rahmen der Kooperation über die CSC Deutschland Solutions datenschutzrechtlich relevante Informationen über Daten, IT-Strukturen, Sicherheitsvorkehrungen u. Ä. der öffentlichen Verwaltung des Landes an US-Geheimdienste gelangt sind oder gelangen können, dass also diese Dienste die Kooperation für ihre Spionage in Schleswig-Holstein oder auch in anderen Dataport-Ländern nutzen.

Ein umfangreicher Fragenkatalog des ULD wurde von Dataport zeitnah bearbeitet und beantwortet. Eine Vor-Ort-Prüfung Dataports bei CSC Deutschland wie auch eine Prüfung der konkreten, über die Rahmenvereinbarung erteilten Aufträge ergab keine Hinweise auf eine Spionagetätigkeit. Im Rahmen der Aufträge hatten die CSC-Mitarbeitenden keinen direkten Zugriff auf personenbezogene Daten von Bürgerinnen und Bürgern oder auf Personalaktendaten. Wohl aber waren die CSC-Mitarbeitenden in IT-Projekte beratend eingebunden, sodass möglicherweise sicherheitsrelevantes Strukturwissen über IT-Verfahren der Verwaltung bekannt wurde. Betroffen waren davon auch sensible IT-Verfahren, etwa der Polizei oder des Finanzverwaltungsamtes.

Im konkreten Zusammenhang stellte sich die Frage, inwieweit bei der Vergabe von öffentlichen Aufträgen Hinweise auf organisatorische, wirtschaftliche oder vertragliche Verstrickungen mit fremden Geheimdiensten berücksichtigt werden müssen bzw. dürfen. Das Gesetz gegen Wettbewerbsbeschränkungen verpflichtet zur Gleichbehandlung der Bieter. Vergabekriterien sind Fachkunde, Leistungsfähigkeit, Gesetzestreue und Zuverlässigkeit. Diese Merkmale können einem Unternehmen nicht auf Verdacht abgesprochen werden, das in anderen Zusammenhängen mit fremden Geheimdiensten kooperiert. Gesetzesverstöße müssen von Gewicht und Relevanz für den Auftrag sein. Demgemäß erließ das Bundesinnenministerium im April 2014 einen Erlass, in dem bei sicherheitsrelevanten Aufträgen die Abgabe einer No-Spy-Erklärung gefordert werden kann. Darin muss der Auftragnehmer versichern, dass er rechtlich nicht verpflichtet ist, vertrauliche Daten an ausländische Geheimdienste und Sicherheitsbehörden weiterzugeben. Im Juni 2014 entschied die Vergabekammer des Bundes, dass „die Kriterien für die Eignung eines Bieters nicht durch den Auftraggeber beliebig erweitert werden können, sondern dass der in den Europäischen Richtlinien vorgegebene Katalog der zulässigen Eignungsanforderungen bzw. der Ausschlussgründe“ abschließend sei.

Dies ändert nichts daran, dass für die Abwicklung des konkreten Auftrages ein Bieter die nötige Vertraulichkeit glaubhaft zusichern muss. Bestehende Offenbarungspflichten nach US-Recht und konkrete Hinweise auf Vertraulichkeitsprobleme sind damit nicht nur datenschutzrechtlich, etwa bei der Auftragsdatenverarbeitung, sondern auch vergaberechtlich relevant. Dataport hat die Vorgaben, Bedingungen und vertraglichen Regelungen für seine Vergaben noch einmal verschärft. Die aktuelle Ausschreibung für einen E-Government-Rahmenvertrag in Schleswig-Holstein verlangt so konsequent, „die Glaubwürdigkeit von Dataport hinsichtlich seiner Verantwortung für Vertraulichkeit und Sicherheit von Daten umfassend zu gewährleisten. Dies schließt die Beziehungen des Bieters zu den mit ihm verbundenen Unternehmen in Drittstaaten ausdrücklich ein.“ Diese Vorgaben eignen sich als Muster bei vergleichbaren Vergabeverfahren.

Was ist zu tun?

Bei der Vergabe von öffentlichen Aufträgen an private Unternehmen mit Datenschutzrelevanz muss und kann durch Vergabeanforderungen sichergestellt werden, dass der Auftrag nicht für Spionagezwecke missbraucht wird.

4.1.3 Zentrale Stellen im kommunalen Bereich

Die Regelung im Landesdatenschutzgesetz (LDSG) zu gemeinsamen Verfahren trägt schon jetzt vielen Anforderungen der modernen IT-Praxis Rechnung und ebnet den Weg zu einer modernen E-Government-Infrastruktur. Die gemeinsame Datenverarbeitung öffentlicher Stellen bzw. der Rückgriff auf gemeinsame Dienstleister ist längst Praxis. Die Verhandlungsmacht über die Modalitäten und technischen und organisatorischen Maßnahmen verschiebt sich allerdings zunehmend auf die Anbieterseite. Dem begegnet die Übertragung der Verantwortung für die Ordnungsmäßigkeit des Verfahrens auf eine zentrale Stelle. Mit der Spiegeldatenbank im Meldewesen finden diese rechtlichen Gestaltungsmöglichkeiten nun eine exemplarische erfolgreiche Anwendung. Die Einrichtung einer zentralen Stelle bedarf einer Rechtsverordnung. Das ist für Landesbehörden ein gangbarer Weg und trägt dem besonderen Risiko landesweiter zentralisierter Datenbestände Rechnung.

Für den kommunalen Bereich besteht mit dem Gesetz über kommunale Zusammenarbeit die Möglichkeit, Aufgaben zu übertragen oder auf eigens zu gründende Körperschaften übergehen zu lassen. Um die Vorteile zentraler Stellen für die IT-Sicherheit und den Datenschutz im kommunalen Sektor fruchtbar zu machen, ist eine Anpassung des LDSG wünschenswert (Tz. 1.1). Unter vergleichbaren formellen und materiellen Anforderungen, bei denen die Rechte aller Beteiligten und die Transparenz gewahrt werden müssen, könnte analog dem Gesetz über kommunale Zusammenarbeit die datenschutzrechtliche Verantwortung für eine gemeinsame zentralisierte IT-Umgebung einer zentralen Stelle übertragen werden.

Was ist zu tun?

Bei der Novellierung des LDSG sollten gemeinsame Verfahren für den kommunalen Bereich zugelassen werden.

4.1.4 Kostenfreies WLAN in Gemeinden

Es ist zu begrüßen, wenn Gemeinden den Nutzerinnen und Nutzern von Büchereien oder den Besucherinnen und Besuchern des Rathauses bürgernah einen kostenfreien WLAN-Zugang anbieten. Da die Bundesbeauftragte für den Datenschutz zuständig ist für den Datenschutz im Telekommunikationsrecht, kann das ULD nur beraten.

Vor der Bereitstellung eines WLAN-Zugangs müssen einige Rechtsfragen geklärt werden. Haftungsrisiken für Rechtsverstöße der Nutzer sollten vermieden werden. Es stellt sich die Frage, ob hierfür die namentliche Registrierung und Protokollierung aller Aktivitäten statthaft sei. Das ist nicht der Fall. Erfolgt das Angebot kostenfrei, ist eine Erhebung von Nutzerdaten für Abrechnungszwecke nicht erforderlich und unzulässig. Das Interesse, sich gegen unberechtigte Forderungen und Rechteinhabern zu verteidigen, rechtfertigt nicht die Verletzung des Fernmeldegeheimnisses.

Entscheidet sich eine Gemeinde zum Eigenbetrieb von WLAN, muss sie eine Reihe unterschiedlicher Anforderungen erfüllen. Im Gegenzug entfällt weitgehend ein Haftungsrisiko für Rechtsverletzungen durch Nutzer. Es bedarf eines Sicherheitskonzepts; ein Sicherheitsbeauftragter ist zu bestellen; die Einhaltung des Telekommunikationsgeheimnisses ist effektiv zu gewährleisten.

Das WLAN kann auch durch einen externen Dienstleister angeboten werden. Die Betroffenen müssen klar erkennen können, wer ihre Daten verarbeitet und wer welche Leistung konkret erbringt. Wird die von einer Gemeinde veranlasste Einrichtung eines Hotspots vollständig von einem Dritten erbracht, ist aus Transparenzgründen eindeutig auf die Identität des Anbieters hinzuweisen. Dies muss auch offline sichergestellt werden, z. B. per Aushang oder Aufsteller.

https://www.datenschutzzentrum.de/artikel/398-.html

4.1.5 Entwicklungen zum Verfahren „KoPers-Land“

Die Landesregierung will mit dem Projekt „KoPers – Kooperation Personaldienste“ das Personalwesen in Schleswig-Holstein modernisieren und zukunftsfähig gestalten. Das ULD berät die Beteiligten und prüft die Ergebnisse aus den laufenden Vorabkontrollen.

Die Gehaltsabrechnung erfolgt für die Landesverwaltung schon seit Längerem zentral durch das Finanzverwaltungsamt. Die Personalverwaltung wurde dagegen in ca. 400 Dienststellen der Landesverwaltung dezentral erledigt. Die Bereiche Versorgung, Besoldung und Entgelt werden bisher mit dem Verfahren „PERMIS-A“, Aufgaben der Personalverwaltung mit dem Verfahren „PERMIS-V“ durchgeführt. Personaldaten der Lehrkräfte werden im Bereich des Ministeriums für Schule und Berufsbildung mit dem Verfahren „PERLE“ verarbeitet. Die Staatskanzlei übernimmt bei KoPers nun die Funktion einer zentralen Stelle und wird damit für das Verfahren verantwortlich. Vorgesehen sind u. a. die Module Abrechnung, Verwaltung, operatives Berichtswesen, Personalkostenhochrechnung, Organisationsmanagement, Self-Services, Bewerbermanagement, Aus- und Fortbildung und Veranstaltungsmanagement. Als zentrale Stelle muss die Staatskanzlei gewährleisten, dass angemessene Maßnahmen zur Datensicherheit getroffen, eine Verfahrensdokumentation und ein Verfahrensverzeichnis angefertigt sowie Test- und Freigabeverfahren durchgeführt werden. Dabei hat sie die Funktion einer Auftraggeberin gegenüber Dataport, das KoPers im Wege einer Auftragsdatenverarbeitung betreibt.

KoPers unterliegt der Vorabkontrolle durch die Staatskanzlei, wobei vor Inbetriebnahme die Zulässigkeit der Datenverarbeitung sowie die getroffenen technisch-organisatorischen Sicherheitsmaßnahmen erfolgreich geprüft werden müssen. Wegen der Vielzahl von Modulen erfolgt die Vorabkontrolle fortlaufend in Einzelschritten, die nach Abschluss des Projekts zu einem Gesamtergebnis zusammengeführt werden sollen.

Im Rahmen der Prüfung durch das ULD liegt ein besonderes Augenmerk auf dem Löschkonzept, dem technischen Schutz vor Veränderung von Daten, dem Protokollierungskonzept und in diesem Zusammenhang auf den Zugriffsrechten bezüglich der Protokolldaten sowie auf der Testdokumentation.

Ein Teilprojekt von KoPers ist die Einführung einer elektronischen Personalaktenhaltung. Dabei müssen die beamtenrechtlichen Vorgaben eingehalten werden. Die Staatskanzlei signalisierte, dass die Forderung des ULD zur Verwendung einer qualifizierten elektronischen Signatur zur Gewährleistung der Manipulationssicherheit der Akten beachtet bzw. umgesetzt wird.

Was ist zu tun?

Mit KoPers soll ein verwaltungseffizientes Verfahren der Personalabrechnung und -verwaltung realisiert werden. Das Gelingen dieser zukunftsorientierten Lösung wird auch davon abhängen, ob die datenschutzrechtlichen und -technischen Vorgaben eingehalten werden.

4.1.6 „KoPers-Kommunen“

Auch auf kommunaler Ebene sollen die Beteiligten von KoPers profitieren. Eine wichtige zentrale Rolle übernimmt die Versorgungsausgleichskasse der Kommunalverbände in Schleswig-Holstein (VAK).

Hauptmodule des Verfahrens „KoPers-Kommunen“ sind ein Personalmanagement mit Mitarbeiterportal, Zeitwirtschaft mit Personaleinsatzplanung, Bezüge- und Entgeltabrechnung, Reisekostenabrechnung, Personalkostenplanung, Personalentwicklung, Bewerberverwaltung sowie die Einführung einer elektronischen Personalakte. Die VAK bietet den Kommunen auf vertraglicher Basis an, als zentrale Stelle die Verfahrensverantwortung und gegebenenfalls zusätzlich die Verantwortung für die zu verarbeitenden personenbezogenen

Daten zu übernehmen. Damit muss sie u. a. für die Erstellung einer Verfahrensdokumentation und die Einhaltung der technisch-organisatorischen Vorgaben Sorge tragen. Schon heute übernimmt die VAK für einen Teil der Kommunen des Landes verschiedene Aufgaben, wie etwa die Gewährung von Versorgungsbezügen an Bedienstete, die Übernahme von Nachversicherungsbeiträgen an die gesetzlichen Rentenversicherungsträger und die Gehaltsabrechnung, also das Auszahlen von Besoldung, Vergütungen und Löhnen.

Eine erste Sichtung der IT-Dokumentation einer Kommune zu KoPers ergab, dass den Anforderungen an eine ordnungsgemäße Verfahrensdokumentation nicht genügt wurde. Über eine Zentralisierung dieser administrativen Aufgaben ist es einfacher, insgesamt einen ordnungsgemäßen Betrieb sicherzustellen. Mit Blick auf KoPers stehen den Kommunen im Rahmen einer beabsichtigten Kooperation mit der VAK zwei Wege offen: Einerseits kann eine Kommune auf Basis des Gesetzes über die Versorgungsausgleichskasse der Kommunalverbände in Schleswig-Holstein die Verfahrensverantwortung und zusätzlich die Verantwortung für die zu verarbeitenden personenbezogenen Daten auf die VAK per Vertrag übertragen. Damit obliegt allein der VAK die Verpflichtung zur Dokumentation des Verfahrens (Einsatz der Informationstechnik, getroffene Sicherheitsmaßnahmen und das Vorgehen bei Test und Freigabe), die Verantwortung für die Gewährleistung der Rechte betroffener Beschäftigter (Auskunft, Berichtigung, Benachrichtigung, Widerspruch gegen die Datenverarbeitung, Löschung und Sperrung), der Abschluss von Verträgen mit Auftragsdatenverarbeitern und die Durchführung von Vorabkontrollen.

Eine Kommune kann aber auch auf vertraglicher Grundlage ausschließlich die Verfahrensverantwortung auf die VAK übertragen. In diesem Fall behält die Kommune für die zu verarbeitenden Daten eine datenschutzrechtliche Verantwortung, z. B. für die Gewährleistung der Rechte betroffener Beschäftigter.

Das ULD befindet sich mit der VAK und den behördlichen Datenschutzbeauftragten mehrerer Kommunen im regelmäßigen Kontakt und führt vor allem mit der VAK Gespräche dazu, welche Inhalte die zugrunde liegende Verfahrensdokumentation aufweisen muss. Die Kommunen können dabei ihre Hinweise und Bedürfnisse in den Dialog einbringen.

Was ist zu tun?

Den Kommunen in Schleswig-Holstein wird empfohlen, mit der VAK Kontakt aufzunehmen und an den regelmäßig stattfindenden Sitzungen der VAK mit dem ULD teilzunehmen. So können sie prüfen, ob für sie eine Übertragung der Verfahrensverantwortung und/oder der Verantwortung für die zu verarbeitenden personenbezogenen Daten für KoPers auf die VAK in Betracht kommt.

4.1.7 Verfahren „eBeihilfe“ beim Finanzverwaltungsamt

In Schleswig-Holstein und Hamburg kommt das Fachverfahren „PERMIS-B“ zum Einsatz, mit dessen Hilfe die Beihilfeberechnung und -festsetzung erfolgt. Verarbeitet werden sensible Gesundheitsdaten. Bei der Prüfung der technisch-organisatorischen Anforderungen an das Verfahren stellte das ULD wiederholt Mängel fest, die zu einer förmlichen Beanstandung führten.

Mit dem Verfahren „eBeihilfe“ ist nun die Einführung eines vollelektronischen Beihilfeprozesses, also einer vollständigen automatischen Belegerfassung, -erkennung und -prüfung geplant. Die Beschaffung der Erkennungssoftware erfolgt durch den gemeinsamen Dienstleister Dataport. Das Scannen, die automatische Dokumentenklassifikation und -extraktion und die manuelle Nachbearbeitung sollen in jedem Bundesland zentral durchgeführt werden. Die manuelle Erfassung mit PERMIS-B soll enden. Sämtliche Papierunterlagen sollen eingescannt und ausschließlich elektronisch weiterverarbeitet werden.

Im November 2012 hatte das Finanzverwaltungsamt dem ULD zugesagt, die erforderliche Verfahrensdokumentation zu erstellen. Da eine ausreichende Dokumentation nicht vorgelegt wurde, teilte das ULD dem Finanzverwaltungsamt mit, dass die Aufnahme des Produktivbetriebs nicht möglich ist. Für Tests mit Echtdaten bedarf es einer Installations- und Konfigurationsdokumentation der verwendeten Geräte und der Dienstanweisungen zur Testdurchführung. Es fehlte ein Netzplan. Nachweise für eine ordnungsgemäße Datenverarbeitung im Auftrag mit dem ausgewählten Dienstleister konnten nicht vorgelegt werden. Eine Bewertung der Testergebnisse hatte das Finanzverwaltungsamt nicht vorgenommen. Da das Verfahren eBeihilfe Bestandteil der Beihilfebearbeitung mittels PERMIS-B ist, stellt dessen Einführung eine wesentliche Änderung im Verfahren dar, die vor Aufnahme des Produktivbetriebs vorabkontrollpflichtig ist.

Bei einer Vor-Ort-Kontrolle im Juli 2013 stellte das ULD fest, dass die gesetzlich geforderte Sicherheitsdokumentation sowie Datenflussdiagramme und Speicherortangaben fehlten. Die Speicherfristen waren nicht in einem Löschkonzept begründet. Für die Teststufen im Testkonzept fehlte die Angabe der rechtlichen Grundlagen. Für betroffene Personen ist eine Einsicht in Personalakten auf Basis von PERMIS-B nur am Bildschirm eines Mitarbeiters des Finanzverwaltungsamts und nicht im Wege der Zurverfügungstellung von Papier möglich. Das festgestellte Verfahren der Personalakteneinsicht verstößt gegen die Vorgaben des Landesbeamtenrechts. Mängel wurden auch im Zusammenhang mit der Einhaltung gesetzlicher Aufbewahrungsfristen festgestellt. Das ULD sprach eine förmliche Beanstandung gegenüber dem Finanzverwaltungsamt aus und informierte das Finanzministerium als zuständige Rechtsaufsichtsbehörde.

Im September 2013 musste das ULD erneut eine förmliche Beanstandung in Aussicht stellen, nachdem das Finanzverwaltungsamt immer noch kein Löschkonzept sowie weitere Unterlagen vorgelegt hatte. Zwischenzeitlich liegen dem ULD auswertbare Unterlagen vor, die derzeit geprüft werden.

Was ist zu tun?

Eine Verfahrensdokumentation muss nach den gesetzlichen Vorschriften vor Aufnahme des Produktivbetriebs vorliegen. Vor einer technischen Umsetzung muss hierfür ausreichend Zeit eingeplant werden.

4.1.8 Personalakten-Digitalisierung bei der Förde Sparkasse Kiel

Die Förde Sparkasse Kiel plante die Digitalisierung der bei ihr vorhandenen papiergebundenen Personalakten und ließ sich hierbei vom ULD beraten. Die Lösungsvorschläge des ULD wurden vonseiten der Sparkasse berücksichtigt.

Das Kreditinstitut ist an 87 Standorten in der Region mit ca. 1.300 Mitarbeitern vertreten. Für seine Mitarbeiter führte die Förde Sparkasse Kiel bisher Papierpersonalakten, die digitalisiert werden sollten. Für das als Anstalt des öffentlichen Rechts betriebene Institut gelten bei der Verarbeitung von Beschäftigtendaten die personalaktenrechtlichen Vorschriften des Landesbeamtenrechts. Technisch-organisatorische Anforderungen, Aufbewahrungsfristen, Einsichtsrechte und die Personalaktenstruktur unterliegen damit besonderen gesetzlichen Vorgaben. Bei der Beauftragung eines Dienstleisters, der die Digitalisierung der Akten übernimmt, wurden die Bestimmungen zur Auftragsdatenverarbeitung eingehalten. Zur Sicherstellung des technisch-organisatorischen Datenschutzes sagte die Förde Sparkasse zu, im Rahmen der Digitalisierung der Personalakten qualifizierte elektronische Signaturen zu verwenden. Eine doppelte Aktenführung – digital und parallel auf Papier – sollte vermieden werden. Andere Verfahren zu einer vergleichbaren Gewährleistung der Manipulations- und Beweissicherheit der Dokumente gibt es nicht. Damit gewährleistet die Förde Sparkasse Kiel einen Sicherheitsstandard, der künftig auch in der Landesverwaltung im Teilprojekt „KoPers – digitale Personalakte“ (Tz. 4.1.5) umgesetzt werden soll.

Was ist zu tun?

Bei der Planung und Organisation von IT-Projekten sind frühzeitig Konzepte zur Einhaltung datenschutzrechtlicher Vorgaben zu erstellen. Projektträger und andere Beteiligte sind aufgerufen, dem positiven Beispiel der Förde Sparkasse Kiel zu folgen.

4.1.9 Normierungsunsinn beim Bundesbeamtengesetz

Das Gesetzgebungsvorhaben der Bundesregierung zur Änderung des Bundesbeamtengesetzes (BBG) und weiterer dienstrechtlicher Vorschriften wurde im Januar 2015 vom Deutschen Bundestag abschließend behandelt. Eine Anhörung der Datenschutzaufsichtsbehörden der Länder während des Gesetzgebungsverfahrens erfolgte nicht, obwohl das Gesetz in rechtswidriger Weise in deren Aufsichtskompetenzen eingreift. Ferner wurde irrigerweise normiert, dass die Beauftragung eines Arztes zur Feststellung eines bestimmten Gesundheitszustands durch den ärztlichen Dienst einer öffentlichen Stelle des Bundes im datenschutzrechtlichen Sinn eine Auftragsdatenverarbeitung sei. Leider hatte auch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) eine Beteiligung der Datenschutzaufsichtsbehörden der Länder nicht in die Wege geleitet.

Mit einer Neuregelung im BBG soll es dem ärztlichen Dienst der personalverwaltenden Behörde ermöglicht werden, eine andere öffentliche oder nicht öffentliche Stelle mit einer ärztlichen Untersuchung zu beauftragen. Gegenüber nicht öffentlichen Stellen verbleibt dabei die Festlegung, welche gesundheitlichen Parameter festgestellt werden sollen, dem ärztlichen Dienst der personalaktenführenden Stelle. Die Beauftragung der nicht öffentlichen Stelle zur Vornahme einer ärztlichen Untersuchung ist keine Auftragsdatenverarbeitung. Mangels Weisungsgebundenheit in Bezug auf die Ausführung der ärztlichen Tätigkeit und den verbleibenden Handlungsspielraum für den Arzt bei der Begutachtung sowie angesichts der Eigenständigkeit der Aufgabenwahrnehmung ist eine solche Zuordnung systemwidrig und schlicht falsch, mit der Folge, dass völlig unklar ist, welche Verantwortung jeweils den Beteiligten zukommt. Mangels Klarstellungen in der Gesetzesbegründung ist keine Weisungsgebundenheit dieser Stelle anzunehmen. Der Schwerpunkt der Tätigkeit des beauftragten Facharztes liegt in der eigenverantwortlichen Untersuchung des Gesundheitszustands einer Person im Hinblick auf bestimmte Parameter, nicht in einer vorgegebenen Verarbeitung personenbezogener Daten.

Gemäß dem neuen BBG soll der Auftraggeber in einem Vertrag zur Auftragsdatenverarbeitung mit einer beauftragten nicht öffentlichen Stelle festlegen, dass der Auftragnehmer eine Kontrolle durch den oder die BfDI nach näher bestimmten Regelungen des Bundesdatenschutzgesetzes zu dulden hat. Es ist nicht ausgeschlossen, vertraglich zwischen Auftraggeber und Auftragnehmer Kontrollrechte zu vereinbaren. Eine Einräumung hoheitlicher Befugnisse oder eine Veränderung der gesetzlichen Zuständigkeiten kann damit aber nicht verbunden sein. Dies verstieße gegen die Vorgaben der europäischen Datenschutzrichtlinie und die Kompetenzzuweisung im Bundesdatenschutzgesetz für die Datenschutzaufsichtsbehörden in Bezug auf nicht öffentliche Stellen. So kann z. B. die BfDI keine hoheitlichen Beanstandungen gegenüber einer nicht öffentlichen Stelle in Schleswig-Holstein aussprechen, mit Ausnahme der Telekommunikations- und Postunternehmen, für die sie zuständig ist. Die BfDI ist bei der im BBG erwähnten vertraglichen Vereinbarung darauf beschränkt, die im Rahmen einer Kontrolle gewonnenen Ergebnisse in einem Verfahren gegen die auftraggebende Stelle des Bundes zu verwerten. Sie kann zudem die Ermittlungsergebnisse an die für den Auftragnehmer zuständige Datenschutzaufsichtsbehörde des Landes weitergeben.

Die im BBG geregelte Kompetenzverteilung missachtet die bestehenden Rollenzuordnungen und führt zu rechtlicher Verunsicherung. Dazu tragen auch unsinnige Normverweise in der Novelle bei, etwa der auf die Regelung zu den Tätigkeitsberichten der BfDI.

Was ist zu tun?

Das Gesetz sollte zum nächstmöglichen Zeitpunkt nachgebessert werden. Durch eine verbesserte Kommunikation zwischen BfDI und Datenschutzaufsichtsbehörden der Länder können derartige Gesetzgebungsfehler vermieden werden.

4.2 Polizei und Verfassungsschutz

Der Novellierungsbedarf des Landesverwaltungsgesetzes (LVwG) hat sich verstärkt. Nach wie vor gibt es keine gesetzliche Grundlage für die Durchführung von Sicherheitsüberprüfungen anlässlich von Großveranstaltungen (34. TB, Tz. 4.2.2). Im Gesetz sind immer noch Regelungen bzw. Verweise enthalten, die das Bundesverfassungsgericht als verfassungswidrig aufgehoben hat. Die Streichung der Beteiligungspflicht des ULD beim Erlass von polizeilichen Errichtungsanordnungen hat sich nicht bewährt. In der Praxis ist die Aufzeichnung von 110-Notrufen üblich, doch fehlt für diesen Eingriff in das Telekommunikationsgeheimnis eine gesetzliche Ermächtigung (32. TB, Tz. 4.2.4). Durch die Weiterentwicklung von @rtus gerät die polizeiliche Datenverarbeitung immer mehr auf eine schiefe Ebene, worunter das Vertrauen in die Rechtmäßigkeit des polizeilichen Handelns immer mehr leidet (Tz. 4.2.1).

Aufgrund aus Grundrechtssicht schlechten Erfahrungen mit gesetzlich geregelten „Gefahrengebieten“ in Hamburg diskutierte der Schleswig-Holsteinische Landtag über die hierzu in Schleswig-Holstein gültige Regelung im LVwG. Anders als in Hamburg befugt diese Regelung zur Durchführung von Anhalte- und Sichtkontrollen, nicht aber zu Identitätsfeststellungen. Dies hat zur Folge, dass personenbezogene Daten bei anlasslosen Kontrollen durch die Polizei nur gespeichert werden, wenn im Einzelfall konkrete verdachtsbegründende Anhaltspunkte vorliegen. Dessen ungeachtet sind die zugelassenen Kontrollen verdachtsunabhängige Grundrechtseingriffe, welche die Gefahr begründen, dass sie im Hinblick auf bestimmte Personengruppen diskriminierend und stigmatisierend genutzt werden. Das ULD hält eine Aufhebung der Regelung für begrüßenswert, aber nicht für verfassungsrechtlich geboten. Es empfahl dem Landtag im Rahmen einer Überarbeitung des LVwG zur Wahrung der Verhältnismäßigkeit und zur Erhöhung der Transparenz gesetzliche Präzisierungen und Verbesserungen im Hinblick auf den Begriff der „polizeilichen Lageerkenntnisse“ und der Wahrscheinlichkeit eines Schadenseintritts. Außerdem empfahl das ULD, die Regelung des LVwG zur Identitätsfeststellung auf „Straftaten von erheblicher Bedeutung“ zu beschränken.

http://www.landtag.ltsh.de/infothek/wahl18/umdrucke/3100/umdruck-18-3105.pdf

Der vom ULD gegenüber dem Innenministerium und Parlamentariern kommunizierte Handlungsbedarf hatte bisher keine gesetzgeberischen Schritte zur Folge.

4.2.1 10 Jahre @rtus – über die gesetzlichen Grundlagen hinausgewachsen

@rtus ist vor zehn Jahren in Betrieb gegangen. Was zunächst als reines Vorgangsbearbeitungssystem konzipiert war, wurde im Laufe der Zeit zu einer Kombination aus Vorgangsbearbeitungs-, Informations- und Auswertesystem. Umso wichtiger, aber auch schwieriger ist die Differenzierung bei den Zwecken der jeweiligen gespeicherten Daten: Dienen sie der Vorgangsbearbeitung, als Information für künftige Verfahren oder zur Dokumentation des polizeilichen Handelns? Jeder Zweck erfordert andere Datenarten, andere Zugriffsberechtigungen und andere Aufbewahrungsfristen – und unterschiedliche Rechtsgrundlagen.

@rtus dient weiterhin in erster Linie der Bearbeitung polizeilicher Vorgänge. Daraus folgen zwei weitere Aufgaben der @rtus-Vorgangsbearbeitung (@rtus VBS): die Verwaltung der Vorgänge und die Dokumentation des polizeilichen Handelns. Gleichzeitig wird @rtus als Informations- und Auswerte-

system eingesetzt: @rtus-Recherche und @rtus-Auswertung (34. TB, Tz. 4.2.1). Diese Systeme übernehmen einen definierten Katalog von Daten aus dem Vorgangsbearbeitungssystem @rtus. Die Speicherung der Daten in @rtus-VBS dient also neben der Vorgangsbearbeitung als Quelle für die Informations- und Auswertesysteme @rtus-Recherche und @rtus-Auswertung.

Weder das LVwG noch die Errichtungsanordnungen für @rtus-VBS bilden diese unterschiedlichen Zwecke ab. Die verfahrensübergreifende Nutzung spielt faktisch eine große Rolle, ist aber gesetzlich kaum ausgeprägt. Das LVwG konzentriert sich auf die Vorgangsbearbeitung, Vorgangsverwaltung und -dokumentation. Auf diesen Zwecken und den entsprechenden Regelungen des LVwG beruhen auch die Errichtungsanordnungen für @rtus-VBS. Damit ist die tatsächliche Nutzung von @rtus-VBS-Daten aber nicht erschöpfend beschrieben. Zwecks Vorgangsbearbeitung dürfen die Daten nur durch die sachbearbeitende und gegebenenfalls beteiligte Dienststelle für den jeweiligen Vorgang und zeitlich nur bis zur Abgabe des Verfahrens an die Staatsanwaltschaft gespeichert und verwendet werden. Letzteres schreibt das LVwG ausdrücklich vor.

Im Anschluss an die Vorgangsbearbeitung dürfen die @rtus-Daten nach dem LVwG nur noch für die Vorgangsverwaltung und -dokumentation verwendet werden; die Nutzung ist erheblich eingeschränkt. Vorgangsverwaltung bedeutet, dass Daten gespeichert und genutzt werden dürfen, soweit dies zum Auffinden von Vorgängen und der Überprüfung ihres Bearbeitungsstandes erforderlich ist. Die Dokumentation behördlichen Handelns dient der Gewährleistung eines effektiven Rechtsschutzes in Bezug auf polizeiliches Handeln. Hierfür sind nicht alle Daten eines Vorgangs erforderlich, und nur wenige Personen benötigen Zugriff auf diese Daten.

§ 190 LVwG

Zur Vorgangsverwaltung und zur befristeten Dokumentation behördlichen Handelns können personenbezogene Daten gespeichert und nur zu diesem Zweck verarbeitet werden.

Das Interesse der Polizei an der Speicherung und Nutzung der Vorgänge in @rtus geht über die Sachbearbeitung und die Dokumentation für den Rechtsschutz der Betroffenen hinaus. Die gespeicherten Daten werden – mit Einschränkungen – auch für Recherchen genutzt (34. TB, Tz. 4.2.1 – @rtus-Recherche), etwa um Zusammenhänge zwischen mehreren Straftaten zu erkennen. Sie werden für die Erstellung von personenbezogenen und nicht personenbezogenen Lagebildern verwendet. Damit dienen die Daten nicht mehr nur dem laufenden Vorgang, für den sie erhoben wurden, sondern stehen auch für andere Vorgänge zur Verfügung.

Eine gesetzliche Grundlage, die die Speicherung und Verwendung von personenbezogenen Daten für künftige Strafverfahren erlaubt, wird in den Errichtungsanordnungen nicht genannt. Das LVwG erlaubt zwar eine Speicherung und Nutzung von Daten zu diesem Zweck, sieht hierfür aber enge Grenzen vor. Speichern darf die Polizei Daten über Verdächtige einer Straftat, wenn sie eine Prognose getroffen hat, dass wegen Art oder Ausführung und Schwere der Tat sowie der Persönlichkeit des Tatverdächtigen Wiederholungsgefahr besteht. Wenn dieser Rahmen für die polizeifachlichen Erfordernisse einer Speicherung von @rtus-Daten zu eng ist, muss der Gesetzgeber entscheiden, ob und in welchem Umfang er eine weiter gehende Speicherung zulassen will. Eine Erweiterung der Speicherungs- und Nutzungsbefugnisse ist möglich; allerdings muss eine Relevanzschwelle bestehen bleiben. Nur auf diese Weise kann verhindert werden, dass jeglicher Kontakt mit der Polizei ausgewertet und in anderen Zusammenhängen verwendet werden kann.

Bis zur Schaffung einer neuen gesetzlichen Befugnis dürfen die @rtus-Daten nur zur Bearbeitung der eigenen Vorgänge, zu deren begrenzter Dokumentation und bei schwereren Straftaten und Vorliegen einer spezifischen Wiederholungsgefahr auch für künftige Zwecke gespeichert und genutzt werden. Die tatsächliche Speicherung und Nutzung von Daten in @rtus geht über diesen gesetzlichen Rahmen weit hinaus.

§ 189 Abs. 1 Satz 4 LVwG

Die Polizei kann darüber hinaus bei personenbezogenen Daten, die sie im Rahmen von Strafermittlungsverfahren über Personen gewonnen hat, die einer Straftat verdächtig sind, weiterhin in abrufbarer Weise speichern, verändern und nutzen, wenn wegen der Art oder Ausführung und Schwere der Tat sowie der Persönlichkeit der oder des Verdächtigen die Gefahr der Wiederholung besteht und wenn dies zur Aufklärung oder Verhütung einer künftigen Straftat erforderlich ist.

Das ULD hat das Innenministerium mehrfach hierauf hingewiesen und dringend eine Anpassung des LVwG angemahnt. Nachdem das Innenministerium keinen Änderungsbedarf gesehen hat, musste das ULD die Errichtungsanordnung für @rtus-Vorgangsverwaltung und -dokumentation beanstanden.

Neugestaltung des Löschkonzepts für @rtus

Mittlerweile liegt dem ULD ein Entwurf des Innenministeriums für ein neues Löschkonzept für @rtus vor. Die derzeitige Speicherung aller Vorgänge für fünf Jahre entspricht nicht dem Gesetz, das eine Differenzierung vorschreibt (34. TB, Tz. 4.2.1 – @rtus-VBS – Evaluierung notwendig).

Der vorgelegte Entwurf ist vielversprechend. Er differenziert nach Vorgängen – z. B. Strafverfahren gegen bekannte oder unbekannte Straftäter, Ordnungswidrigkeiten oder Gefahrenabwehrberichten –, nach Personen – z. B. Beschuldigten, Anzeigenden, Geschädigten, Zeugen –, aber vor allem danach, zu welchen Zwecken die Daten jeweils erforderlich sind. So sollen Daten über Beschuldigte bei manchen Straftaten auch nach Abschluss eines Strafverfahrens noch gespeichert bleiben, weil sie für andere Verfahren relevant sein können. Auch einige Berichte sollen nach Beendigung des Vorgangs gespeichert bleiben, weil sie wichtige Informationen – z. B. zur Aufklärung von Serienstraftaten – enthalten können. Das Konzept des Innenministeriums legt nach unterschiedlichen Zwecken Löschfristen fest und differenziert auch hinsichtlich der Zugriffsrechte nach Vorgängen und Personen.

Damit kann für die Praxis eine ausgewogene Lösung erzielt werden, die den polizeilichen Belangen und den Persönlichkeitsrechten der Betroffenen genügt. Diese kann aber nicht darüber hinwegtäuschen, dass es im LVwG keine ausreichende Grundlage für dieses Konzept gibt, soweit es um die Speicherung für künftige Verfahren geht.

@rtus-Data Warehouse – Kriminalitätslage mit Personenbezug

Mit der Einrichtung eines Data Warehouse hat für @rtus eine neue Episode begonnen. Die @rtus-Daten stehen für Auswertungen nach unterschiedlichsten Kriterien und im Prinzip für alle erdenklichen Zwecke zur Verfügung. Das erste Auswerteverfahren ist bereits in Betrieb: die Kriminalitätslage. Weitere Auswertungen werden folgen.

Für die personenbezogene automatisierte Auswertung von Daten enthält das Landesverwaltungsgesetz keine ausreichenden Regelungen. Es erlaubt lediglich den einfachen Abgleich von personenbezogenen Daten mit einer Datei und die weitaus schwerwiegendere Rasterfahndung mit Daten von unterschiedlichen Behörden und nicht öffentlichen Stellen. Beide Vorschriften erfassen nicht die massenhafte Auswertung eigener polizeilicher Daten. Aus diesem Grund hat die Projektgruppe @rtus-Data Warehouse zunächst nur nicht personenbezogene Auswertungen des Data-Warehouse-Bestands geplant.

Vor diesem Hintergrund hat das ULD unter der zusätzlichen Prämisse, dass das Landesverwaltungsgesetz zeitnah angepasst wird, dem Verfahren zugestimmt. Bei einer Kontrolle stellte sich kurz nach Aufnahme des Wirkbetriebs des Verfahrens „Kriminalitätslage“ heraus, dass personenbezogene bzw. -beziehbare Daten verarbeitet und dem Nutzer angezeigt werden: die Straße mit Hausnummer und die Vorgangsnummer des jeweiligen Datensatzes aus @rtus. Dies ist unter den bestehenden rechtlichen Regularien nicht erlaubt. Das ULD beanstandete, nachdem das Landespolizeiamt keine Änderung vornahm, das Verfahren „Kriminalitätslage“ als einen Verstoß gegen das Landesverwaltungsgesetz.

Schutzbedarfsfeststellung für das Verfahren @rtus

Auf Initiative des ULD wurde der Schutzbedarf der polizeilichen Informationsverarbeitung in @rtus durch das Landespolizeiamt überprüft. Es stellte sich heraus, dass der bisher festgelegte Schutzbedarf der gespeicherten personenbezogenen Daten zu gering war. Die Landespolizei legte den Schutzbedarf „sehr hoch“ fest. Im Juli 2013 wurde dem ULD mitgeteilt, dass mangels zur Verfügung stehender Ressourcen keine Konsequenzen aus dem von der Polizei selbst festgestellten Schutzbedarf gezogen werden. Diese Aussage des Innenministeriums ist aus Sicht des ULD nicht vertretbar. Die Gewährleistung eines ausreichenden Sicherheitsstandards gemäß dem Schutzbedarf ist für die Verarbeitung höchst sensibler Daten durch die Polizei des Landes eine elementare, nicht verzichtbare Grundvoraussetzung. Der Verzicht hierauf war vom ULD ebenfalls zu beanstanden.

Was ist zu tun?

Der Gesetzgeber muss erkennen, dass @rtus in der Praxis längst viel mehr als ein Vorgangsbearbeitungssystem ist, und den normativen Rahmen für einen gesetzes- und grundrechtskonformen Einsatz von @rtus in allen seinen Facetten schaffen.

4.2.2 Polizeilicher Informations- und Analyseverbund (PIAV)

Dem föderalen Staatsaufbau der Bundesrepublik folgend, obliegen die Aufgaben der Gefahrenabwehr und Strafverfolgung grundsätzlich den Polizeien der Länder. In besonders geregelten Ausnahmefällen sind sie dem Bund übertragen. Aus dieser Verteilung zwischen Bund und Ländern folgt, dass die Länder für die informationstechnische Erledigung ihrer Aufgaben eigene Datenverarbeitungsverfahren geschaffen haben, was einen erheblichen personellen und finanziellen Ressourceneinsatz erfordert. Die Länder sind in gesetzlich fest umrissenen Fällen verpflichtet, Daten an das BKA zu übermitteln, das Zentralstellenaufgaben erfüllt und das bundesweite Informationssystem der Polizei – INPOL – betreibt. Wird künftig alles anders sein?

Seit einiger Zeit gibt es konkrete polizeiliche Planungen, die Datenverarbeitung an neuen Anforderungsprofilen auszurichten. Aus Gründen der Effizienz sollen die Meldedienste (Verpflichtung der Polizeien der Länder, dem BKA Daten aus definierten Deliktsbereichen in festgelegter Form zum frühesten Zeitpunkt zu übermitteln) in der bisherigen Form abgeschafft und Auswerte- und Analysefunktionen verbessert werden. Angesichts der – unbegrenzten – Möglichkeiten der elektronischen Datenverarbeitung scheint dies sinnvoll und naheliegend.

Vom neuen Polizeilichen Informations- und Analyseverbund, kurz PIAV, versprechen sich die Polizeien des Bundes und der Länder deutliche Verbesserungen in der täglichen Arbeit. Aus Datenschutzsicht handelt es sich dabei um ein komplexes IT-Vorhaben, das vieles mehr als auf den ersten Blick erkennbar verändert.

PIAV soll die bestehenden Meldedienste ablösen und die Informationen barrierefrei in sogenannte Dateiencluster überführen. Die Dateiencluster enthalten Daten aus mehreren, unter kriminalistischen Gesichtspunkten zusammengehörigen Einzeldateien. Viele Fragen sind noch offen: Aus welchen Deliktsbereichen sollen im Rahmen des Verfahrens „PIAV“ Daten an das BKA übermittelt werden? Werden die Inhalte 1:1 gegenüber den bisherigen Meldediensten abgebildet, oder werden zusätzliche Daten einbezogen? Und kann bei einer derartigen Dateienarchitektur die Zweckbindung der gespeicherten Daten garantiert werden?

Die vorliegenden Konzeptunterlagen lassen nicht erkennen, was in PIAV unter Analyse zu verstehen ist: Welche Daten werden einbezogen, und nach welchen Regeln werden sie analysiert? Sind clusterübergreifende Analysen vorgesehen? Wenn ja, für welche Fallkonstellationen und für welchen Nutzerkreis? Dürfen freitextliche Dokumente, die möglicherweise Informationen über Dritte enthalten, ebenfalls gespeichert und in eine Analyse einbezogen werden?

Obwohl all diese Fragen noch nicht abschließend beantwortet sind, soll der Pilotbetrieb für ein Dateiencluster Mitte 2016 in Betrieb gehen.

Die Bund/Länder-Projektgruppe beim BKA hat also noch einige Probleme aus dem Weg zu räumen, bevor PIAV starten kann. Das ULD hat den Innenminister des Landes Schleswig-Holstein im Januar 2013 auf diese Problematik hingewiesen. Das ULD hat zudem deutlich gemacht, dass dieses Projekt insgesamt hochgradig kostenintensiv ist und Auswirkungen für die Polizei des Landes Schleswig-Holstein frühzeitig geklärt werden sollten. Das ULD hat Beratung in Fragen des Datenschutzes angeboten. Im Herbst 2013 startete eine Arbeitsgruppe im Landespolizeiamt zur Begleitung des IT-Vorhabens. Das ULD nimmt bei Bedarf an den Gesprächen teil.

Was ist zu tun?

Die bestehenden rechtlichen Unklarheiten müssen zeitnah ausgeräumt werden, um eine rechtskonforme Datenverarbeitung zu ermöglichen.

4.2.3 Data Center Polizei

Die Polizei des Landes möchte ihre IT-Verfahren bei Dataport in einem gemeinsamen Data Center mit den Polizeien Hamburgs und Bremens betreiben und erhofft sich davon vor allem Rationalisierungseffekte. Diese dürfen jedoch nicht so weit gehen, dass die datenschutzrechtlich gebotene Trennung der drei beteiligten Länderpolizeien aufgehoben wird.

Das ULD hat daher gemeinsam mit dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit und der Landesbeauftragten für Datenschutz und Informationsfreiheit Bremen auf Folgendes hingewiesen:

- Durch die Verlagerung von Verfahren in das „Data Center Polizei dürfen keine gemeinsamen Verfahren entstehen, die den Daten verarbeitenden Stellen der unterschiedlichen Länder Zugriff auf die personenbezogenen Daten der jeweils anderen Länder ermöglichen. Die Orientierungshilfe „Mandantenfähigkeit“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (34. TB, Tz. 6.1) ist zu beachten.
- Soweit personenbezogene Daten länderübergreifend ausgetauscht werden, ist dies nur bei Vorliegen der gesetzlichen Voraussetzungen zulässig. Dies gilt auch für die Einrichtung automatisierter Abrufverfahren.
- Für einen Betrieb des Data Center Polizei ist eine gemeinsame Festlegung von Schutzbedarfen und zusätzlichen Sicherheitsmaßnahmen wünschenswert und Voraussetzung für die Realisierung von Rationalisierungsgewinnen.
- Für die Erstfestlegung von Sicherheitsmaßnahmen und für deren Fortschreibung sowie für Kontrollen zur tatsächlichen Umsetzung von Sicherheitsmaßnahmen ist ein Gremium der Auftraggeber zu bilden, das dauerhaft die Aufgabe eines gemeinsamen Datenschutz- und IT-Sicherheitsmanagements für das Data Center Polizei wahrnimmt und die Beauftragung von gemeinsamen Sicherheitsmaßnahmen und die Kontrolle ihrer Umsetzung verantwortet.

Was ist zu tun?

Der Betrieb der IT-Verfahren der Polizei in einem gemeinsamen „Data Center Polizei“ mit Hamburg und Bremen ist nur zulässig, wenn die Trennung der Daten der jeweiligen Länder voneinander technisch gewährleistet ist.

4.2.4 Videoüberwachung zur Gefahrenabwehr

Der Einsatz von Videotechnik nimmt nicht nur bei nicht öffentlichen Stellen stetig zu. Auch Polizei und Kommunen setzen zur Unterstützung ihrer Aufgabenerfüllung zunehmend auf Kameraüberwachung. Im Berichtszeitraum hat sich das ULD mit Kameras auf öffentlichen Plätzen in mehreren

Städten in Schleswig-Holstein sowie mit eingebauten Kameras in Funkstreifenwagen der Landespolizei befasst.

Videoüberwachung auf öffentlichen Plätzen

In mehreren Städten haben die Kommunalverwaltungen in Zusammenarbeit mit der Polizei zur Gefahrenabwehr auf öffentlichen Plätzen Überwachungsanlagen errichtet (dazu auch 33. TB, Tz. 4.2.9). Seit 2008 wurde in Leck die Hauptstraße im Bereich einer Diskothek mit Kameras überwacht. In Neumünster ist seit 2011 der gesamte Bereich des Großfleckens mit Kameras ausgestattet. Seit 2014 sind in Elmshorn im Umfeld des Bahnhofs Videokameras installiert. Betreiber ist in allen Fällen die kommunale Ordnungsbehörde. Die Videobilder werden aber an die örtliche Polizeidienststelle übertragen, wo eine Beobachtung erfolgt und Aufzeichnungen gefertigt werden.

Von der Überwachung sind alle Personen betroffen, die z. B. täglich mit dem Zug zur Arbeit fahren, im Stadtzentrum einkaufen, Ärzte aufsuchen, Angelegenheiten im Rathaus erledigen oder sich mit Freunden im Café treffen. Deshalb sieht das Landesverwaltungsgesetz eine Überwachung solcher Plätze nur im Ausnahmefall vor. Sie ist nur an Kriminalitäts- und Gefahrenschwerpunkten und nur zum Schutz gewichtiger Rechtsgüter wie Leben oder Gesundheit erlaubt. Nach dem Gesetz handelt es sich nicht um eine Dauermaßnahme; alle sechs Monate muss geprüft werden, ob die Voraussetzungen dafür weiterhin vorliegen. Das ULD bezweifelt, dass alle Überwachungsmaßnahmen die strengen Anforderungen erfüllen.

In Leck sind die Kameras im Berichtszeitraum deaktiviert worden und werden in Kürze vollständig abgebaut. Die Videoüberwachung in Neumünster wurde vom ULD nach einer Eingabe geprüft. Die Entwicklung der Kriminalität und die aktuelle Gefahrensituation für den Großflecken, wie sie im Evaluierungsbericht der Polizei beschrieben werden, erfüllen nach Ansicht des ULD nicht die Voraussetzungen eines Kriminalitäts- und Gefahrenschwerpunkts, was wir der Stadt Neumünster mitteilten. In Elmshorn stellte das ULD bei einer Vor-Ort-Kontrolle fest, dass sich die Überwachung auf den Platz vor dem Bahnhof und die Fußgängerunterführungen beschränkt. Erfreulich ist die datensparsame Gestaltung des Systems. Auf dem Überwachungsmonitor bei der Polizei Elmshorn werden Personen verpixelt angezeigt. Die Aufzeichnung erfolgt sowohl verpixelt als auch unverpixelt, die Zugriffe auf die unverpixelten Aufzeichnungen sind technisch sowie organisatorisch eng begrenzt. Da der Bahnhof Elmshorn täglich von vielen Pendlern genutzt wird, ist hier besonders darauf zu achten, dass keine langfristige Beobachtung von Personen und keine Profilbildungen ermöglicht werden.

§ 184 Abs. 2 LVwG

Allgemein zugängliche Flächen und Räume dürfen mittels Bildübertragung beobachtet werden, soweit dies zur Aufgabenerfüllung nach § 162 erforderlich ist. Der offene Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen oder Bildaufzeichnungen in und an allgemein zugänglichen Flächen und Räumen, die Kriminalitäts- oder Gefahrenschwerpunkte sind, ist zulässig, soweit Tatsachen die Annahme rechtfertigen, dass Schäden für Leib, Leben oder Freiheit oder gleichgewichtige Schäden für andere Rechtsgüter zu erwarten sind. Die Maßnahme nach Satz 2 ist örtlich auf den erforderlichen Bereich zu beschränken und auf sechs Monate zu befristen. Eine Verlängerung ist nur zulässig, sofern die Voraussetzungen nach Satz 2 weiterhin vorliegen.

Videokameras in Funkstreifenwagen

Die Landespolizei hat begonnen, ihre Funkstreifenwagen mit Videoüberwachungsanlagen auszustatten. Dies dient der Eigensicherung der Polizeibeamten bei polizeilichen Maßnahmen, insbesondere bei Verkehrskontrollen.

Dafür werden in den Fahrzeugen Kameras eingebaut, die nach vorne und für die Fahrzeuge der Autobahnreviere auch nach hinten ausgerichtet sind. Die Kameras werden bei Verkehrskontrollen automatisch aktiviert, wenn das Anhaltesignal – der Schriftzug „STOP POLIZEI“ – betätigt wird. Daneben ist auch eine manuelle Auslösung der Kameras möglich. Nach Aktivierung zeichnen die Kameras das Geschehen auf. Die Aufzeichnungen werden für 72 Stunden gespeichert. Für die Betroffenen soll der Aufzeichnungsvorgang dadurch erkennbar sein, dass an der Kamera eine rote Kontrollleuchte leuchtet. Die Polizeibeamten sind zudem per Dienstanweisung verpflichtet, die Betroffenen zu Beginn der Kontrolle auf den Einsatz der Anlage hinzuweisen.

Das ULD hat gegenüber dem Landespolizeiamt eine kritische Stellungnahme zu der Maßnahme abgegeben, insbesondere zur automatischen Aufzeichnung nach Betätigung des Anhaltesignals bei

Verkehrskontrollen. Jede mit einem modernen Funkstreifenwagen durchgeführte Verkehrskontrolle wird so erfasst, ganz unabhängig davon, ob es im Einzelfall Anhaltspunkte für die Ausübung von Gewalt gegen die Polizeibeamten gibt. Polizeiliche Verkehrskontrollen sind anlasslos zulässig, sodass auch völlig unauffällige Autofahrer kontrolliert und dabei aufgezeichnet werden können. Selbst wenn die Kontrolle ohne Vorkommnisse verläuft, bleiben die Aufzeichnungen für drei Tage gespeichert.

Die undifferenzierte Aufzeichnung sämtlicher Maßnahmen kann nach Auffassung des ULD nicht mit dem abstrakten Gefährdungspotenzial solcher Situationen begründet werden. Das ULD hat angeregt, die Maßnahme technisch so umzusetzen, dass eine Aufzeichnung erst im tatsächlichen Bedarfsfall erfolgt. Die Speicherdauer ist unverhältnismäßig lang. Unzureichend ist weiterhin die Transparenz für die Betroffenen. Die Information des Betroffenen muss vor Beginn der Überwachung erfolgen. Dem genügt weder der mündliche Hinweis noch die Kontrollleuchte an der Kamera.

§ 184 Abs. 3 LVwG

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

Was ist zu tun?

Die Polizei sollte die Videoüberwachung sparsam und maßvoll einsetzen. Technische Lösungen sollten nicht nur zur Optimierung der Überwachung entwickelt und herangezogen werden, sondern auch zur Stärkung der Persönlichkeitsrechte der Betroffenen.

4.2.5 Versammlungsgesetz

Der Schleswig-Holsteinische Landtag hat im Berichtszeitraum einen Gesetzentwurf zum Versammlungsrecht in Schleswig-Holstein beraten, zu dem das ULD Stellung genommen hat. Grundlage ist ein Gesetzentwurf der Fraktion der FDP (LT-Drs. 18/119), zu dem alle Fraktionen Änderungsvorschläge vorgelegt haben.

Der Entwurf sowie auch die Änderungsvorschläge befassen sich intensiv mit der Videoüberwachung von Versammlungen. Gegenüber dem noch geltenden Versammlungsrecht des Bundes bringen die Konzepte aller Fraktionen die Grundrechte der Versammlungsfreiheit und der informationellen Selbstbestimmung deutlich stärker zur Geltung. Insbesondere der Änderungsantrag der Regierungsfraktionen sieht eine ausgewogene Regelung der Videoüberwachung vor. Danach dürfen Bild- und Tonaufnahmen von individualisierten Personen nur bei erheblichen Gefahren für die öffentliche Sicherheit angefertigt werden. Übersichtsaufnahmen sind nur bei Versammlungen unter freiem Himmel zugelassen, nicht bei Versammlungen in geschlossenen Räumen. Da Übersichtsaufnahmen nur für den Zweck der Leitung und Lenkung des Polizeieinsatzes bei großen und unübersichtlichen Versammlungen vorgesehen sind, ergibt sich auch kein Bedarf für Übersichtsaufnahmen in geschlossenen Räumen. Bei den Übersichtsaufnahmen besteht keine Notwendigkeit zur Aufzeichnung, da ausschließlicher Zweck der Übertragung in die Einsatzleitzentrale die dortige Koordinierung des Einsatzes ist. Diese Klarstellungen sind aus grundrechtlicher Sicht zu begrüßen. Übersichtsaufnahmen stellen aufgrund ihrer Streubreite einen schwerwiegenden Grundrechtseingriff dar und können erhebliche Einschüchterungseffekte auslösen. Der Verzicht auf Übersichtsaufzeichnungen

verhindert, dass Bilder von der gesamten Versammlung oder von größeren Teilen im Nachhinein personenbezogen ausgewertet werden, ohne dass Anhaltspunkte für eine Gefahr vorlagen.

Was ist zu tun?

Der Landtag sollte den Gesetzentwurf zum Versammlungsrecht in Schleswig-Holstein zügig beschließen. Übersichtsaufnahmen in geschlossenen Räumen und Übersichtsaufzeichnungen unter freiem Himmel sollten nicht erlaubt werden.

4.2.6 Mitteilung über psychisch auffällige Personen an das Gesundheitsamt

Das ULD erfuhr durch eine Eingabe von einer polizeilichen Datenweitergabe an das Gesundheitsamt. Die Polizei hatte eine Strafanzeige von zwei Personen aufgenommen; einer von diesen war der Polizei bekannt. Gemäß dem Eindruck der Polizei verhielten sich die beiden psychisch auffällig, weshalb sie zunächst eine Person aus dem Umfeld der Anzeigenden befragte. Letztlich meinte die Polizei, bei der einen Person bestünden Anzeichen für Verfolgungswahn, und leitete „zuständigkeitshalber" den Vorgang an das Gesundheitsamt „mit der Bitte um Kenntnisnahme und weitere Veranlassung" weiter.

Das ULD beanstandete die Datenübermittlung, für die es keine Rechtsgrundlage gab. Ohne Einwilligung des Betroffenen dürfen personenbezogene Daten an die Gesundheitsbehörde nur zur Abwehr einer konkreten erheblichen Eigen- oder Fremdgefährdung übermittelt werden. Eine solche lag bei dem Petenten nicht vor.

Generell sind Entscheidungen in solchen Situationen für Polizeibeamte schwierig. Ihnen fehlen Informationen über die Betroffenen und die fachliche Qualifikation, um eine zuverlässige Prognose über das künftige Verhalten der Betroffenen anstellen zu können. Gehen von den Betroffenen erst zu nehmende Gefahren aus, muss die Polizei tätig werden. Andererseits kann nicht jedes aus Sicht der Polizei auffällige oder abweichende Verhalten zum Anlass für weitere Maßnahmen und Übermittlungen an andere Behörden genommen werden. Geschieht dies ohne Kenntnis und ohne den Willen der Betroffenen, greift die Polizei gravierend in deren Selbstbestimmungsrechte ein – nicht nur in informationeller Hinsicht. Um die Polizeibeamten von ihrer Verantwortung ein Stück weit zu entlasten, hat das ULD empfohlen, in Zweifelsfällen eine pseudonyme Mitteilung an das Gesundheitsamt zu machen. Erst dann, wenn das Gesundheitsamt die tatsächlichen Voraussetzungen für eine Datenübermittlung bejaht, sollten die Personenangaben übermittelt werden.

4.2.7 Hosting der Amtsdatei DIANA beim Bundesamt für Verfassungsschutz

Die Verfassungsschutzbehörde des Landes hat mit dem Bundesamt für Verfassungsschutz (BfV) eine Verwaltungsvereinbarung über das Hosting ihrer Amtsdatei DIANA beim BfV geschlossen. Zwar wurden einige der Kritikpunkte des ULD zu einem Vorentwurf (34. TB, Tz. 4.2.6) berücksichtigt, nicht aber der grundlegende Konfliktpunkt. Die geschlossene Vereinbarung geht nicht von einer Datenverarbeitung im Auftrag aus, sondern von einer Amtshilfe auf der Grundlage der Gesetzgebungskompetenz des Bundes für die Zusammenarbeit der Länder im Bereich Verfassungsschutz und der allgemeinen Zusammenarbeits- und Unterstützungspflicht von Bund und Ländern im Verfassungsschutzgesetz des Bundes. Datenschutzrechtlich schafft diese Konstruktion keine Klarheit. Während bei der Datenverarbeitung im Auftrag klar ist, welche Stelle die datenschutzrechtliche Verantwortung trägt und mit welchen Mitteln sie verpflichtet ist, diese gegenüber dem

Auftragnehmer wahrzunehmen, bleibt bei der von Verfassungsschutzbehörde und BfV gewählten Konstruktion vieles offen. Zwar soll nach der Vereinbarung die Verfassungsschutzbehörde die Verantwortung für die in der Amtsdatei gespeicherten Daten und für die Verarbeitung der Daten behalten. Entsprechende Weisungs- und Kontrollbefugnisse für die Verfassungsschutzbehörde gegenüber dem BfV enthält die Vereinbarung jedoch nicht. Damit ist die Weitergabe von personenbezogenen Daten durch die Verfassungsschutzbehörde an das BfV rechtlich nicht privilegiert als Datenverarbeitung im Auftrag. Es handelt sich um eine Datenübermittlung, die einer gesetzlichen Grundlage bedarf. Die allgemeine Unterstützungspflicht der Verfassungsschutzbehörden genügt hierfür nicht, denn sie bezieht sich nicht ausdrücklich auf die Verarbeitung personenbezogener Daten und würde schon gar nicht alle Daten umfassen. Soweit für das Hosting personenbezogene Daten an das BfV übermittelt werden, ist dies mangels gesetzlicher Grundlage rechtswidrig.

4.2.8 Vorsicht, Extremist!

Ein Petent beschwerte sich, weil im Rahmen seines Einbürgerungsverfahrens die Verfassungsschutzbehörde der Einbürgerungsbehörde eine Auskunft erteilt hat. Das ULD stellte fest, dass der Petent in der Verbunddatei NADIS der Verfassungsschutzbehörden des Bundes und der Länder sowie in einer Amtsdatei der schleswig-holsteinischen Behörde erfasst war. Für beide Speicherungen war die hiesige Verfassungsschutzbehörde verantwortlich. Die Datenverarbeitung wurde mit einer Betätigung des Petenten in einer extremistischen Bestrebung begründet. Bei genauerem Hinsehen bezweifelte das ULD die Zulässigkeit der Erfassung und Speicherung der Daten, weil die Anforderungen des Landesverfassungsschutzgesetzes (LVerfSchG) nicht vorlagen, beanstandete dies förmlich und forderte die Löschung der durch die Verfassungsschutzbehörde gespeicherten Daten. Ein vermuteter, durch Tatsachen nicht begründeter Verdacht der Betätigung in einer extremistischen Bestrebung genügt nicht, um Daten zu speichern. Das LVerfSchG verlangt das Bestehen tatsächlicher Anhaltspunkte für die Teilnahme der betroffenen Person an einer verfassungsfeindlichen Bestrebung oder Tätigkeit. Diese tatbestandliche Voraussetzung konnte die Verfassungsschutzbehörde im konkreten Fall nicht darlegen. Die Daten sind daraufhin gelöscht worden.

Was ist zu tun?

Die Verfassungsschutzbehörde muss vor jeder Datenspeicherung die gesetzlichen Voraussetzungen prüfen. Ein bloßer Verdacht reicht nicht aus, um Daten in Dateien der Verfassungsschutzbehörde zu erfassen.

4.3 Justizverwaltung

4.3.1 Funkzellenabfragen

Im Berichtszeitraum hat das ULD eine Stichprobe von Funkzellenabfragen in Strafverfahren geprüft. Ausgewählt wurden elf Verfahren, in denen jeweils eine oder mehrere nicht individualisierte Funkzellenabfragen durchgeführt worden sind. Bei einer nicht individualisierten Funkzellenabfrage werden von Mobilfunkanbietern alle Verkehrsdatensätze erhoben, die an einem Ort in einem von der Ermittlungsbehörde festgelegten Zeitraum erzeugt worden sind. Dies können Telefo-

nate, SMS oder Datenverbindungen zum Internet sein. Mit der Abfrage soll in der Regel ermittelt werden, welche Anschlussinhaber sich in der Nähe eines Tatortes aufgehalten haben. Häufig wird dieses Mittel bei dem Verdacht einer Serienstraftat angewandt, um zu prüfen, ob an unterschiedlichen Tatorten dieselben Telefonnummern oder Mobilfunkgeräte auftauchen.

Da der Grundrechtseingriff solcher Abfragen aufgrund ihrer Streubreite und der Einbeziehung von Telekommunikationsdaten schwer wiegt, stellt das Gesetz an ihre Zulässigkeit hohe Anforderungen. Sie sind nur bei schwerwiegenden Straftaten zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Es bedarf der Anordnung durch ein Gericht. Nach Abschluss sind die von der Maßnahme betroffenen Personen zu benachrichtigen – allerdings nur diejenigen, deren Identität ermittelt wurde und die von der Maßnahme erheblich betroffen waren.

Die Stichprobenprüfung des ULD hat folgende Erkenntnisse erbracht:

- Allen elf Verfahren der Stichprobe lagen schwerwiegende Straftaten zugrunde, die die gesetzlichen Voraussetzungen erfüllten.
- Die Prüfung der gesetzlichen Voraussetzungen war oftmals nur unzureichend dokumentiert, insbesondere im Hinblick auf die Verhältnismäßigkeit der Maßnahme und das Fehlen anderer Ermittlungsansätze.
- Teilweise befanden sich die von den Providern übermittelten Verkehrsdatensätze ohne Kennzeichnung in der Ermittlungsakte; überwiegend waren sie allerdings in einem gekennzeichneten Sonderband gespeichert.
- In einigen Fällen hat die Staatsanwaltschaft die Löschung der Funkzellendaten verfügt, sobald das Verfahren – z. B. durch Einstellung mangels Beweisbarkeit – abgeschlossen war. In anderen Fällen ist eine Löschung unterblieben. In einigen Fällen wurde nach Einstellung des Verfahrens die weitere Aufbewahrung angeordnet, da die Daten bei einer Wiederaufnahme des Verfahrens benötigt werden könnten.
- Eine nachträgliche Benachrichtigung der Betroffenen ist nur in einem der geprüften Fälle vorgenommen worden. In vielen Fällen wurden Betroffene nicht identifiziert und aus diesem Grund auch nicht benachrichtigt. Identifizierte Betroffene in anderen Verfahren wurden mit der Begründung nicht benachrichtigt, sie seien nur unerheblich betroffen.
- Bei den in der Stichprobe geprüften Verfahren wurde also das Mittel der Funkzellenabfrage nur für die Aufklärung von Straftaten angewandt, die konkret von erheblichem Gewicht waren. Häufig erfolgten parallel oder nachträglich Telekommunikationsüberwachungen, Observationen oder andere Maßnahmen. Die häufig geäußerte Annahme, die nicht individualisierte Funkzellenabfrage entwickle sich zu einer Standardmaßnahme, kann anhand der Stichprobe für Schleswig-Holstein nicht bestätigt werden. Gleichwohl unterscheidet sich diese Maßnahme aufgrund ihrer Streubreite signifikant von anderen Ermittlungsmethoden. Sie erzeugt in besonderem Maße eine Gefahr für Unbeteiligte, in die Ermittlungen einbezogen zu werden. Dieser Umstand wurde in den Verfahren nur unzureichend berücksichtigt. Dies begann bereits mit teilweise fehlender oder unzureichender Verhältnismäßigkeitsprüfung bei der Anregung der Maßnahme. Verbesserungen sind insbesondere nach der erfolgten Auswertung der Daten nötig. Die Frage der Löschung der Daten wurde in jedem Verfahren unterschiedlich, teilweise auch gar nicht beantwortet. Insofern sind klare Vorgaben erforderlich, die eine einheitliche datensparsame Verwendung der Funkzellendaten gewährleisten. Nahezu komplette Fehlanzeige besteht in puncto Transparenz. Von der Datenerhebung und -verarbeitung erfährt die Mehrheit der Betroffenen, von den Beschuldigten und ganz wenigen Mitbetroffenen abgesehen, nichts.
- Das Landeskriminalamt hat auf Anregung des ULD die Verfahrensregelungen für die Landespolizei überarbeitet. Doch sind die drängenden Fragen der Löschung der Daten und der Benachrichtigung der Betroffenen von dieser Regelung nicht erfasst. Da hierüber die Staatsanwaltschaft entscheidet, kann eine landesweite Regelung nur durch die Justiz getroffen werden.

Was ist zu tun?

Das Verfahren bei nicht individualisierten Funkzellenabfragen ist verbesserungsbedürftig. Es muss sichergestellt werden, dass die Daten frühestmöglich gelöscht werden. Verbesserungsbedürftig ist außerdem die Transparenz für die Betroffenen.

4.3.2 eAkte im Strafverfahren

Es zeichnet sich ab, dass die elektronische Akte (eAkte) für das Strafverfahren in näherer Zukunft eingeführt wird. Eine Vielzahl der damit verbundenen datenschutzrechtlichen Herausforderungen müssen über die Strafprozessordnung gelöst werden; es bleiben offene Fragen hinsichtlich der praktischen Umsetzung.

Es ist zu klären, wo die Akte geführt wird und in welchem Umfang Zugriffe der beteiligten Stellen möglich sein sollen. Bislang gibt es eine Papierakte, die von der Polizei, der Staatsanwaltschaft und dann dem Gericht – gemeinsam – geführt wird und in die alle für das Strafverfahren relevanten Informationen aufgenommen werden. Der maßgebliche Inhalt des Strafverfahrens ist gebündelt in einer Akte zusammengefasst. So kann kein Zweifel aufkommen, welche Unterlagen für das Verfahren relevant sind. Die elektronische Datenverarbeitung der am Strafverfahren beteiligten Stellen ist dagegen streng voneinander getrennt. Elektronisch verfügt jede Stelle über die Stammdaten des Verfahrens, die üblicherweise in elektronischen Vorgangsverwaltungssystemen gespeichert werden. Dies sind die Angaben über Beschuldigte, Geschädigte, Zeugen, Verteidiger und andere Verfahrensbeteiligte, Angaben zum Tatvorwurf und zum Gang des Verfahrens. Jede Stelle verfügt über ein eigenes Vorgangsverwaltungssystem, das nach eigenen Regeln betrieben wird und allenfalls über eng definierte Austauschschnittstellen mit den Systemen der anderen Stellen verfügt. Darüber hinaus liegen bei der beteiligten Stelle allenfalls diejenigen Aktenbestandteile elektronisch vor, die sie selbst erzeugt hat. Dieser im Vergleich zur Strafakte erheblich eingeschränkte Datenbestand wird bei der Polizei bereits jetzt für weitere Zwecke als für die reine Bearbeitung des konkreten Falls genutzt (Tz. 4.2.1), etwa zur Recherche für andere Strafverfahren oder für Auswertungen.

Die Grundelemente der Datenverarbeitung im Strafverfahren müssen auch bei Einführung der eAkte erhalten bleiben: Es muss gewährleistet sein, dass der gesamte Akteninhalt als Ganzes verfügbar ist. Außerdem muss die informationelle Trennung der am Verfahren beteiligten Stellen gewährleistet bleiben. Die Notwendigkeit, allen Stellen für das jeweilige Verfahren den Akteninhalt elektronisch zur Verfügung zu stellen, darf nicht dazu führen, dass die Stellen diesen über das Verfahren hinaus für Recherchen und Auswertungen nutzen können.

Was ist zu tun?

Die elementaren Datenschutzstandards müssen bei der elektronischen Aktenführung im Strafverfahren gesetzlich, organisatorisch und technisch gewährleistet bleiben.

4.3.3 Öffentlichkeitsfahndung im Internet

Die Justizministerkonferenz befasste sich im November 2013 mit den Möglichkeiten der Öffentlichkeitsfahndung in Facebook und anderen sozialen Netzwerken. Das geltende Recht erlaubt Öffentlichkeitsfahndung in sozialen Netzwerken nicht. Die Richtlinien für das Straf- und Bußgeldverfahren regeln, dass private Internetanbieter für die Öffentlichkeitsfahndung grundsätzlich nicht eingeschaltet werden sollen. Vor einer möglichen Änderung dieser Richtlinien hat die Justizministerkonferenz die Konferenz der Datenschutzbeauftragten beteiligt.

Die Konferenz der Datenschutzbeauftragten hält eine Nutzung sozialer Netzwerke privater Betreiber für sehr problematisch. Durch die weltweit recherchierbare Veröffentlichung wird in schwerwiegender Weise in die Grundrechte der Betroffenen eingegriffen. Einmal veröffentlichte Inhalte lassen sich im Internet nur sehr schwer und oft nicht restlos löschen. Bereits deshalb forderte die Konferenz spezifischere gesetzliche Regeln für die Öffentlichkeitsfahndung über das Internet. Eine Öffentlichkeitsfahndung bei privaten Anbietern ermöglicht diesen, die Nutzungsdaten für eigene Zwecke zu verarbeiten. Das, was für öffentliche Stellen generell gilt, ist auch auf die Öffentlichkeitsfahndung anzuwenden (Tz. 7.1). Es steht Strafverfolgungsbehörden nicht zu, rechtswidrige Verarbeitung von Nutzungsdaten zu unterstützen, indem Anbieter in Anspruch genommen werden, die das Telemediengesetz nicht beachten.

Wollen Strafverfolgungsbehörden Öffentlichkeitsfahndung über private Internetanbieter durchführen, so sind folgende Anforderungen zu beachten:

- Die Öffentlichkeitsfahndung darf nur auf Diensten von Anbietern erfolgen, die den datenschutzrechtlichen Vorgaben des Telemediengesetzes entsprechen.
- Die zur Öffentlichkeitsfahndung verwendeten personenbezogenen Daten dürfen von den Strafverfolgungsbehörden nur auf Servern gespeichert werden, die im eigenen Verantwortungsbereich stehen.
- Kommentierungsfunktionen müssen deshalb deaktiviert sein; die Kommunikation zwischen den Strafverfolgungsbehörden und den Nutzern darf nicht im sozialen Netzwerk erfolgen.
- Die Weitergabe und der automatisierte Abruf der personenbezogenen Daten aus dem Internet durch Webcrawler und ähnliche Dienste müssen so weit wie technisch möglich verhindert werden.
- Die Öffentlichkeitsfahndung bei privaten Internetanbietern muss verhältnismäßig sein. Diese Fahndungsmethode darf nur im Einzelfall bei schwerwiegenden Straftaten erlaubt sein. Art, Umfang und Dauer der jeweiligen Maßnahme müssen im Einzelfall durch die beantragende Staatsanwaltschaft konkret bestimmt werden; hierzu gehört auch eine Begründung für die Wahl der Fahndungsmethode.

https://www.datenschutz-hamburg.de/uploads/media/Entschliessung_87.DSK_OEffentlichkeitsfahndung.pdf

Was ist zu tun?

Die Justiz sollte gut abwägen, ob sie Öffentlichkeitsfahndungen auch bei privaten Internetbetreibern zulässt. Zumindest sind die genannten Anforderungen zu berücksichtigen.

4.3.4 Vollzugsgesetze zum Jugendarrest und Erwachsenenvollzug

Das ULD wirkte an zwei Gesetzgebungsverfahren für den Justizvollzug mit. Der Gesetzentwurf der Landesregierung für ein Jugendarrestvollzugsgesetz, zu dem das ULD eine Stellungnahme abgab, wurde vom Landtag beschlossen. Darin sind für den Jugendarrest Kontrollmöglichkeiten

bei Besuchen, Telefongesprächen und beim Schriftverkehr geregelt. Der Regierungsentwurf war diesbezüglich jedoch zu unbestimmt und erlaubte zu weitgehende und unverhältnismäßige Kontrollen. Die vom ULD angemahnten Beschränkungen der Überwachungsbefugnisse wurden vom Landtag vollständig übernommen. Erfreulich ist auch, dass auf eine Ermächtigung zur heimlichen Videoüberwachung, die in einem Vorentwurf der Landesregierung aus der vorigen Wahlperiode vorgesehen war, verzichtet wurde.

Noch in Arbeit befindet sich ein Gesetzentwurf für ein Strafvollzugsgesetz. Das federführende Justizministerium bezog dieses Mal das ULD schon bei der Erstellung des Entwurfs eng mit ein, sodass das ULD in einer Arbeitsgruppe Vorschläge zur Gestaltung der Datenschutzvorschriften einbringen konnte.

4.3.5 Schweigepflichtentbindung für Suchtberater

Schweigepflichtentbindungserklärungen, die von Inhaftierten gegenüber externen Suchtberatern in Schleswig-Holstein abgegeben werden, sind so zu gestalten, dass sie eine vertrauliche Beratung fördern, aber dabei nicht die Ziele des Vollzugs beeinträchtigen.

Inhaftierte können während des Strafvollzuges nicht nur Leistungen von internen, sondern auch von externen Suchtberatern in Anspruch nehmen. Die externen Suchtberater, Sozialarbeiter und Sozialpädagogen sind keine Beschäftigten der Strafvollzugsanstalt. Für die Durchführung des Strafvollzuges benötigt die Vollzugsanstalt Kenntnis von bestimmten Informationen, die im Zusammenhang mit der externen Suchtberatung des Inhaftierten stehen. Mit der Übermittlung dieser personenbezogenen Informationen wird die berufliche Schweigepflicht der Sozialarbeiter und Sozialpädagogen eingeschränkt, wofür es einer gesetzlichen Ermächtigung bedarf. Eine solche fehlt für die Übermittlung der Informationen an Vollzugsanstalten in Schleswig-Holstein. Daher wird auf eine Schweigepflichtentbindungserklärung zurückgegriffen, mit der der Inhaftierte die externen Suchtberater ausdrücklich von der Schweigepflicht entbindet und damit seine Einwilligung in die Datenübermittlung an die Strafvollzugsanstalt erteilt.

Eine wirksame Einwilligungserklärung setzt eine hinreichende Information des Inhaftierten vor der Abgabe der Erklärung und deren Freiwilligkeit voraus. Die Informationspflicht umfasst Angaben über die verantwortliche Stelle, den bzw. die Empfänger, den Betroffenen, den Umfang und die Art der Daten, den Verwendungszweck, die Freiwilligkeit und die Widerrufsmöglichkeit. Der Inhaftierte ist ferner über die Folgen aufzuklären, wenn er die Schweigepflichtentbindungserklärung verweigert, wobei dies deren Freiwilligkeit nicht einschränken darf. Ob eine freie Entscheidung des Erklärenden vorliegt, muss wegen des bestehenden Abhängigkeitsverhältnisses zwischen dem Inhaftierten und dem Vollzugspersonal generell kritisch gesehen werden. Maßstab für die Beurteilung der Freiwilligkeit ist, ob der Inhaftierte eine eigenständige Entscheidung darüber treffen kann, dass er der dargelegten Verwendung seiner personenbezogenen Daten zustimmt und die externen Suchtberater von der Schweigepflicht entbindet.

Das ULD beriet bei der Formulierung eines Musterformulars für eine Schweigepflichtentbindungserklärung von Inhaftierten gegenüber externen Suchtberatern, die als Rechtsgrundlage für die Übermittlung von Informationen an die Strafvollzugsanstalt herangezogen werden kann. Der Inhaftierte muss dabei über die Folgen einer verweigerten Erklärung aufgeklärt werden, ohne dass diese Aufklärung der Freiwilligkeit entgegensteht. So soll er entscheiden können, ob er möchte, dass die Suchtberatung für vollzugliche Entscheidungen – wie vorzeitige Haftentlassung oder Lockerungen – berücksichtigt wird oder nicht. Das ULD stellte dem Ministerium für Justiz, Kultur und Europa des Landes Schleswig-Holstein Formulierungen für eine einheitliche Handhabung zur Verfügung.

Was ist zu tun?

Für eine einheitliche und rechtskonforme Handhabung von Schweigepflichtentbindungserklärungen, die von Inhaftierten gegenüber externen Suchtberatern abgegeben werden, sollte in Schleswig-Holstein das Musterformular als Grundlage verwendet werden, das vom ULD mit konzipiert wurde.

4.3.6 Das Verwertungsverbot des BZRG im Strafvollzug

Das Bundeszentralregistergesetz (BZRG) regelt ein Verwertungsverbot, das auch im Strafvollzug beachtet werden muss. Danach dürfen die Tat und die Verurteilung dem Betroffenen im Rechtsverkehr nicht mehr vorgehalten werden, wenn die Eintragung über die Verurteilung im Register getilgt worden ist oder wenn sie zu tilgen ist und keine der gesetzlich geregelten Ausnahmen eingreift. Die Regelung verbietet auch im Strafvollzug die Verwendung von Angaben zu früheren Verurteilungen des Inhaftierten, die vielleicht aus anderen Gründen bekannt sind, in dem Bundeszentralregister jedoch bereits getilgt sind bzw. zu tilgen sind.

Was ist zu tun?

Die Strafvollzugsbehörde hat sich zu vergewissern, dass die im Strafvollzug für vollzugliche Entscheidungen herangezogenen Angaben zu den Inhaftierten nicht dem Verwertungsverbot des BZRG unterliegen.

4.3.7 Adressierung von behördlichen Schriftstücken an Gefangene

Ein außerhalb Schleswig-Holsteins inhaftierter Gefangener berichtete dem ULD über einen Auskunftsantrag an das Justizministerium Schleswig-Holstein nach dem Informationszugangsgesetz (IZG). Die Auskunftserteilung erfolgte jedoch nicht an ihn, sondern an die Vollzugsanstalt. Das Justizministerium bestätigte, dass es generelle Praxis ist, Schreiben der schleswig-holsteinischen Aufsichtsbehörde, also des Justizministeriums, an Gefangene in Vollzugsanstalten anderer Bundesländer an die jeweiligen Vollzugsanstalten zu richten. Dies ist nach Ansicht des ULD rechtswidrig, da für die Übermittlung personenbezogener Daten an die Justizvollzugsanstalt im Einzelfall eine Rechtsgrundlage bestehen muss. Bei einer Auskunft nach dem IZG ist nicht erkennbar, dass deren Kenntnis für die Vollzugsbehörde erforderlich ist. Das Justizministerium sagte zu, Schreiben künftig direkt an die Gefangenen zu richten. Sieht das Ministerium es im Einzelfall nach entsprechender Prüfung für erforderlich an, so wird die Justizvollzugsanstalt durch eine Abschrift benachrichtigt.

Was ist zu tun?

Gefangene haben das Recht auf eine vertrauliche Kommunikation mit Behörden. Auch Schreiben, die nicht von der Postkontrolle ausgenommen sind, sind direkt an die Gefangenen und keinesfalls an die Justizvollzugsanstalt zu adressieren.

4.3.8 Gerichtliche Berichtsanforderungen über politisch relevante Verfahren

In Strafverfahren, die in der Öffentlichkeit und im parlamentarischen Raum auf ein erhebliches Interesse stoßen, ist es üblich, dass die Staatsanwaltschaften und Gerichte dem Justizministerium Bericht erstatten. Staatsanwaltschaften sind hierzu durch eine Anordnung des Justizministeriums über Berichtspflichten in Strafsachen ausdrücklich verpflichtet. Das Justizministerium soll hierdurch in die Lage versetzt werden, parlamentarische sowie Presseanfragen direkt zu beantworten. Ein Abgeordneter des Schleswig-Holsteinischen Landtags bat das ULD, diese Praxis datenschutzrechtlich zu überprüfen.

Solche Berichte mit personenbezogenen Inhalten können nach dem Landesdatenschutzgesetz zulässig sein. Die Übermittlung setzt voraus, dass die Daten für die Erfüllung der durch Rechtsvorschrift zugewiesenen Aufgaben des Empfängers erforderlich sind. Die Kenntnis des Justizministeriums über den Stand von Verfahren ist unter bestimmten Voraussetzungen erforderlich, um gegenüber dem Parlament sowie den Medien sprech- und auskunftsfähig zu sein. Hierbei handelt es sich um gesetzliche und verfassungsrechtliche Aufgaben des Ministeriums. Die Fälle, über die berichtet wird, und der Umfang der Berichte im Einzelfall müssen sich jeweils auf das erforderliche Maß beschränken. Soweit es möglich ist, sollten die Berichte anonymisiert werden.

4.3.9 Ungeschwärzte Kontoauszüge für die Justiz – Prüfung bei Rechtspflegern

Einem Beklagten wurde in einem familiengerichtlichen Verfahren Prozesskostenhilfe gewährt; die Verfahrenskosten wurden gestundet. Nach einer gewissen Zeit überprüfte das Gericht die wirtschaftlichen Verhältnisse erneut, um zu entscheiden, ob die Stundung aufgehoben werden kann. Für diese Prüfung hat der Rechtspfleger die vollständigen ungeschwärzten Kontoauszüge vom Beklagten für die zurückliegenden sechs Wochen angefordert. Die Frage des ULD, ob eine teilweise Schwärzung der Kontoauszüge durch den Beklagten möglich ist (31. TB, Tz. 4.5.1), verneinte das Gericht. Sofern die Angaben im Kontoauszug auch nur teilweise geschwärzt würden, sei die gesetzlich vorgeschriebene Überprüfung der Selbsterklärung über die wirtschaftlichen Verhältnisse nicht oder nur noch eingeschränkt möglich.

Das ULD beanstandete die Aufforderung zur Vorlage ungeschwärzter Kontoauszüge. Für die Überprüfung kann auf eine vollständige Aufstellung aller Einnahmen und Ausgaben zugegriffen werden, auf der die Beträge erkennbar sind. Der Grundsatz der Verhältnismäßigkeit verlangt aber die Zulassung von Schwärzungen in den Buchungstexten, wenn das Geheimhaltungsinteresse das Interesse an der Prüfung einer Buchung überwiegt. Dies kann bei Sollbuchungen über geringere Beträge und bei besonders geschützten personenbezogenen Daten – z. B. bei Angaben über ärztliche Behandlungen, Mitgliedsbeiträge an politische Parteien oder Gewerkschaften oder Zahlungen an Religionsgemeinschaften – der Fall sein. Auch das Bundessozialgericht erkennt in solchen Fällen das überwiegende Interesse des Betroffenen an, diese Angaben unkenntlich zu machen.

Das ULD wies darauf hin, dass das Gericht die von den Betroffenen zur Prüfung eingereichten Kontoauszüge nur in dem erforderlichen Umfang zur Akte nehmen darf. Nicht erforderliche Kontoaus-

züge müssen dem Betroffenen zurückgegeben oder vernichtet werden.

Nach Auffassung des Gerichts und des Justizministeriums unterliegt dieser Sachverhalt nicht der Kontrolle des ULD, da die Aufforderung zur Vorlage der Kontoauszüge durch einen Rechtspfleger erging. Rechtspfleger sind nach dem Gesetz unabhängig und weisungsfrei. Die Kontrolle durch das ULD ist nach dem LDSG hingegen nur ausgenommen bei Tätigkeiten, die in richterlicher Unabhängigkeit ausgeübt werden. Die im Grundgesetz verankerte richterliche Unabhängigkeit ist etwas anderes als die gesetzliche Unabhängigkeit der Rechtspfleger. Das Justizministerium sieht im Hinblick auf die Prüfkompetenz des ULD keinen Unterschied zwischen Rechtspflegern und Richtern und möchte eine grundsätzliche Klärung der damit verbundenen Rechtsfragen herbeiführen.

Was ist zu tun?

Der Zahlungsgrund kann besonders schutzwürdige Interessen der Betroffenen berühren. In solchen Fällen haben die Betroffenen einen Anspruch, bei Vorlage von Kontoauszügen Angaben zum Zahlungsgrund unkenntlich zu machen.

4.3.10 forumSTAR

Bei den Amtsgerichten und Landgerichten wird derzeit die Anwendung „MEGA“ durch „forumSTAR“ abgelöst (34. TB, Tz. 6.4.4). An der Verfahrenseinführung sind mehrere Stellen beteiligt. Die Gesamtverantwortung trägt das Justizministerium. Dort sind die Lenkungsgruppe, die Koordinierungsstelle, die Qualitätssicherung, das Controlling und das technische Projekt angesiedelt. Daneben gibt es beim Schleswig-Holsteinischen Oberlandesgericht eine Projektgruppe „forumSTAR“. Diese betreibt die fachliche Gestaltung des Verfahrens und die fachliche Administration, also z. B. die Rollenverwaltung. Die zentralen Komponenten des Verfahrens, eine Datenbank mit Adressdaten (u. a. von Rechtsanwälten) und ein Fileserver mit Formularen, werden bei Dataport betrieben. Angewendet wird das Verfahren bei den Gerichten der ordentlichen Gerichtsbarkeit, die damit personenbezogene Daten von Verfahrensbeteiligten erfassen und verarbeiten.

Aus dieser Arbeitsteilung ergeben sich unterschiedliche Aufgaben und Verantwortlichkeiten, die klar voneinander abgegrenzt werden müssen. Das Landesdatenschutzgesetz (LDSG) enthält eine Regelung für automatisierte Verfahren, die gemeinsam von mehreren Stellen betrieben werden. Danach kann die Verantwortung für die Gewährleistung der Ordnungsmäßigkeit des automatisierten Verfahrens von der Verantwortung für die gespeicherten Daten abgetrennt und auf eine zentrale Stelle übertragen werden. Dies ist für das Verfahren forumSTAR durch die oben beschriebene Aufgabenverteilung faktisch erfolgt. Zwar werden die Daten in der Anwendung forumSTAR von den Gerichten gespeichert. Die Verantwortung für die Ordnungsmäßigkeit des Gesamtverfahrens forumSTAR liegt aber beim Justizministerium.

Daraus ergeben sich für die Gewährleistung der Ordnungsmäßigkeit sowie der Kontrollfähigkeit des Verfahrens folgende Konsequenzen: Gemäß dem LDSG sind die zentrale Stelle sowie Einzelheiten über Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung durch Rechtsverordnung festzulegen. In dieser Verordnung ist das Zusammenwirken der zentralen Stelle mit den Daten verarbeitenden Stellen, hier den Gerichten, sowie die Aufteilung von Aufgaben und Verantwortlichkeiten zu regeln. Diese Festlegungen sollten Grundlage für die nach dem LDSG und der Datenschutzverordnung (DSVO) zu erstellenden Dokumente sein.

Die unterschiedlichen Verantwortlichkeiten wirken sich auf den Test und die Freigabe der Verfahrenskomponenten aus. Den Regelungen in der DSVO liegt der Gedanke zugrunde, dass Tests und Freigaben, die gestuft erfolgen können, sich auf einzelne Bestandteile des Verfahrens beziehen können. Für die oben beschriebene Aufteilung von Aufgaben und Verantwortlichkeiten für das Ver-

fahren forumSTAR folgt daraus, dass jede der beteiligten Stellen eine Freigabe für die von ihr zu verantwortenden Komponenten erteilen muss und diese zuvor entsprechend zu testen hat. Die zentralen technischen Komponenten müssen vom Justizministerium getestet und freigegeben werden. Für die fachlichen Komponenten liegt diese Zuständigkeit bei der Projektgruppe beim OLG. Den Gerichten obliegt der Test der dezentral vor Ort betriebenen Komponenten und deren Freigabe.

Auch die nach der DSVO zu erstellende Verfahrensdokumentation muss entsprechend der beschriebenen Verantwortlichkeiten erstellt werden. Automatisierte Verfahren können dabei in Teilbereiche gegliedert werden, für die jeweils eine eigene Dokumentation zu erstellen ist. Das Justizministerium hat dem ULD einen Entwurf für die Rechtsverordnung zur Stellungnahme übersandt. Danach übernimmt das Justizministerium als zentrale Stelle die Verantwortung für die Ordnungsmäßigkeit des Verfahrens.

Was ist zu tun?

Die Verordnung für die Einrichtung einer zentralen Stelle sollte zügig erlassen werden, damit die Verantwortlichkeiten der beteiligten Stellen klar geregelt sind.

4.4 Verkehr

Die Zeiten, in denen das Verkehrsgeschehen im Hinblick auf den Datenschutz überschaubar und begrenzt war, sind vorbei. Der Flugverkehr ist schon seit Längerem ein überwachungsintensiver Sektor. Es folgen nun die öffentlichen Verkehrsmittel und der Individualverkehr.

4.4.1 Videoüberwachung in öffentlichen Verkehrsmitteln

In Bahnhöfen kooperiert die Deutsche Bahn schon seit Jahren mit der Bundespolizei bei der Videoüberwachung. Zum Jahresende 2014 kündigte die Bahn an, die Bahnhöfe bundesweit durch Installation von 700 weiteren Kameras sicherer machen zu wollen. Als Begründung wurde angeführt, die Fahrgäste würden dies fordern; das subjektive Sicherheitsgefühl würde erhöht. Derartige subjektive Aspekte können in keinem Fall die mit der Videoüberwachung verbundenen Grundrechtseingriffe rechtfertigen. Jede einzelne Kamera bedarf in ihrer konkreten Ausgestaltung einer rechtlichen Legitimation. Gefühlte Sicherheit ist trügerisch; im Notfall kann die Kamera nicht zur Hilfe eilen. Eine Vielzahl wissenschaftlicher Untersuchungen belegt, dass von Kameras nur in wenigen Fällen ein messbarer präventiver Effekt ausgeht. Zur Aufklärung von Straftaten sind aufgezeichnete Videobilder oft wenig tauglich, etwa weil die Täter auf nicht erfasste Räume ausweichen oder weil sie ihre Identifizierbarkeit bewusst erschweren.

Seit jeher können Fahrgäste die Züge der Bahn unbeobachtet nutzen. Kontrollen beschränkten sich auf das Vorzeigen der nötigen Fahrkarte. Doch hatten es der Busverkehr und der städtische Personennahverkehr schon vorgemacht: Inzwischen soll nach dem Willen der Landesregierung gemäß den Vergabevoraussetzungen für Schienenpersonennahverkehrsleistungen auch in den Zügen umfassend Videotechnik installiert werden. Dies war Anlass für das ULD, den Dialog mit den Eisenbahnverkehrsunternehmen und der Landesweiten Verkehrsservicegesellschaft Schleswig-Holstein (LVS) zu suchen. Das ULD wies darauf hin, dass das hier anwendbare Bundesdatenschutzgesetz keine umfassende und flächendeckende Videoüberwachung erlaubt, weil dies unverhältnismäßig wäre. Gefahrenlagen und Straftaten, zu

deren Vermeidung und Aufklärung Videoüberwachung einen Beitrag leisten könnte, sind in der Fläche in Schleswig-Holstein selten und bewegen sich im Bahnverkehr eher im niederschwelligen Bereich. Dies führte aber leider nicht zum Verzicht auf die Vergabeanforderung durch die LVS, weshalb sich der Landtag mit dem Thema befassen musste und das ULD gegenüber dem Wirtschaftsausschuss eine Stellungnahme abgab. Ergänzend wies das ULD darauf hin, dass selbst für den Fall einer zulässigen Kamerainstallation folgende Aspekte zu beachten sind:

- Eindeutige Kennzeichnung der überwachten Räume,
- Bereitstellung von überwachungsfreiem Fahrgastraum,
- Ausschluss der Toiletten von der Überwachung,
- Beschränkung der maximalen Speicherdauer auf drei Tage,
- Beschränkung auf Videobeobachtung bzw. bei Erforderlichkeit auf ein Ringspeicherkonzept ohne Vernetzung,
- Vorliegen eines Datenschutzkonzeptes, das die verfolgten Zwecke und die Verarbeitung, Nutzung/Auswertung und Löschung der Daten mit entsprechenden Zugriffsregelungen und Verfahrenssicherungen festlegt.

http://www.landtag.ltsh.de/infothek/wahl18/umdrucke/2200/umdruck-18-2256.pdf

Das Wirtschaftsministerium teilte mit, dass neu bestellte Züge der Regionalbahn Schleswig-Holstein sowie der Nordbahn gemäß den Vorgaben der LVS mit Kameras ausgestattet sein werden. Dies verursacht nicht nur finanzielle, sondern auch grundrechtliche Kosten. Zugleich ist dies ein überflüssiges Arbeitsbeschaffungsprogramm für das ULD, das nun umfassend kontrollieren muss, ob die strengen gesetzlichen Anforderungen eingehalten werden.

Was ist zu tun?

Der Zugverkehr in Schleswig-Holstein sollte frei von Videoüberwachung bleiben.

4.4.2 Datenschutz im Auto

Ähnlich wie bei der Internetdatenverarbeitung besteht die Gefahr, dass durch datenschutzwidrige Technikgestaltung und das nur begrenzte datenschutzbewusste Konsumverhalten der Autohalter, Autofahrerinnen und -fahrer die „überwachungsfreie Fahrt für freie Bürger“ zur nostalgischen Forderung von Oldtimerfans wird. Interesse an den personenbeziehbaren Daten haben viele, allen voran Hersteller und Werkstätten, aber auch Versicherungen, die erste Angebote mit fahrverhaltensabhängigen Tarifen machen, die IT- und die Werbeindustrie. Dies war der Grund, weshalb sich der 52. Deutsche Verkehrsgerichtstag in Goslar im Januar 2014 in dem Arbeitskreis VII mit dem Thema „Wem gehören die Fahrzeugdaten?“ befasste, wozu das ULD einen Beitrag leistete und aus Datenschutzsicht zu begrüßende Empfehlungen an die Politik formulierte.

http://www.deutscher-verkehrsgerichtstag.de/images/empfehlungen_pdf/Gesamt_Empfehlungen_52._VGT_2014.pdf

Die Konferenz der Datenschutzbeauftragten richtete zu diesen Fragestellungen eine Unterarbeitsgruppe ein, die sich mit den vielfältigen mit der Digitalisierung des Autos und dessen multimedialer Vernetzung verbundenen Datenschutzfragen befasste. Der deutsche Verband der Automobilindustrie (VDA) hat inzwischen erkannt, dass der Datenschutz von Fahrern, Haltern und sonstigen Kfz-Nutzenden ein marktrelevantes Thema ist und dass diesbezüglich „Compliance“ gefordert ist. Nicht zuletzt die auf extensives Datensammeln ausgerichtete Konkurrenz aus den USA, die weniger von den dortigen Automobil- als von den IT-Unternehmen ausgeht, stärkt die Bereitschaft

zur Etablierung höherer Datenschutzstandards in Europa. In den weiteren Gesprächen zwischen Datenschützern und Kfz-Herstellern muss es darum gehen, klare Standards festzulegen. Am Ende sollten verbindliche Verhaltensregeln, also gesetzlich anerkannte „Codes of Conduct" stehen, die auch umgesetzt werden.

https://www.vda.de/de/themen/innovation-und-technik/vernetzung/datenschutz-prinzipien-fuer-vernetzte-fahrzeuge.html

Was ist zu tun?

Bei dem Dialog mit den Kfz-Herstellern sollten nationale und mittelfristig europäische hohe Datenschutzstandards vereinbart und festgeschrieben werden.

4.4.3 eCall

Ab April 2018 sollen alle neuen Personenkraftwagen und leichten Nutzfahrzeuge in der EU verpflichtend mit „eCall" ausgestattet werden, ein in der Kfz-Elektronik installiertes Verfahren, mit dem automatisch oder manuell bei einem Unfall, z. B. beim Auslösen des Airbags oder einer Panne, ein Notruf an die Nummer 112 ausgelöst wird. Dies soll über eine voreingestellte mobile Datenübertragung inklusive Standortdatum an die nächste Rettungsleitstelle erfolgen. Automatisch soll eine Tonverbindung aufgebaut werden, um eine Kommunikation zwischen Rettungsleitstelle und Insassen zu ermöglichen. Die EU-Kommission erhofft sich mit diesem System wegen der dadurch ermöglichten schnelleren adäquaten Hilfe eine Senkung der Zahl der Unfalltoten um bis zu 2.500 im Jahr. Im Juni 2013 gab die EU-Kommission bekannt, dass sie EU-weit einheitliche technische Standards festgelegt hat. Das EU-Parlament soll das Verordnungspaket im März 2015 absegnen.

Der Regelungsvorschlag zielt auf Transparenz für die Betroffenen, Datensparsamkeit und Zweckbindung der verarbeiteten Daten ab. Offen ist noch die konkrete technisch-organisatorische Umsetzung. Zugleich sieht die Verordnung vor, dass es den Fahrzeugherstellern und unabhängigen Anbietern unbenommen bleiben soll, die dann installierte Technik für zusätzliche Notfalldienste und „Dienste mit Zusatznutzen" zu verwenden. Es geht den EU-Gremien nicht nur um ein zusätzliches Instrument der Verkehrssicherheit, sondern auch darum, in der Kfz-Informationstechnik zunächst für diesen Dienst einheitliche Standards einzuführen und zugleich eine technische Plattform für eine weiter gehende Informatisierung des Autos zu schaffen.

Die bordeigene Mobilfunkeinheit soll nur dann Verbindung zum Netz aufnehmen, wenn tatsächlich ein Notfallruf abgesetzt wird. Ein dauerndes Tracking mit der Bildung eines genauen Bewegungsbildes, wie es heute z. B. mit eingeschalteten Handys möglich ist, findet bei eCall nicht statt. Der Fahrer kann aber das System nicht abschalten. Dies wird damit gerechtfertigt, dass es beim eCall nicht nur um den Schutz des Fahrers, sondern auch von weiteren Verkehrsbeteiligten geht. Dies hat zwangsläufig in der lange dauernden Einführungsphase eine informationelle Ungleichbehandlung von Fahrten mit neuen und alten, noch nicht mit eCall ausgestatteten Autos zur Folge. Es ist fraglich, ob das angestrebte Ziel diese Einschränkung der informationellen Selbstbestimmung rechtfertigen kann.

Was ist zu tun?

Bei der technischen Umsetzung von eCall ist darauf zu achten, dass Wahlfreiheit, Transparenz, Datensparsamkeit und Datensicherheit gewahrt bleiben.

4.4.4 Pkw-Maut

Das Bundesverkehrsministerium stellte im Oktober 2014 einen Entwurf für ein Pkw-Maut-Gesetz vor, wonach Halterinnen und Halter von Personenkraftwagen (Pkws) eine Infrastrukturabgabe (Maut) entrichten müssen, wenn sie Autobahnen und Bundesstraßen nutzen. Halter von im Inland zugelassenen Pkws sollen die Abgabe vorab beim Kraftfahrtbundesamt (KBA) per Lastschrift entrichten, wozu dort in einem Infrastrukturabgaberegister Angaben zum Pkw, zur Kontobeziehung sowie zur Entrichtung der Abgabe gespeichert werden sollen. Halter ausländischer Pkws sollen Zeitvignetten erwerben können.

Die Überwachung der Einhaltung der Abgabenpflicht obliegt dem Bundesamt für Güterverkehr (BAG). Hierzu sollten zunächst folgende Daten erhoben und weiterverarbeitet werden: Bild des Kfz, Name und Anschrift des Kfz-Führers, Ort und Zeit der Kfz-Nutzung, Kfz-Kennzeichen und abgaberelevante Kfz-Merkmale. Über eine mindestens 13 Monate dauernde Speicherung beim BAG sollte der Nachweis einer Nichtnutzung der Straßen zum Zweck der Rückerstattung der vorausbezahlten Abgabe ermöglicht werden. Der Entwurf enthielt zwar eine strenge Zweckbindung der Daten, hätte aber dazu geführt, dass zwecks möglicher Rückerstattung von wohl weniger als 1 % der tatsächlich erfolgten inländischen Mautzahlungen beim BAG sämtliche über Pkw-Maut-Kontrollstellen erfassten Kfz-Bewegungen mit Ort, Zeit und Foto von 100 % aller Pkws über ein Jahr lang elektronisch gespeichert worden wären. Trotz versprochener Zweckbindung forderten Polizeivertreter schon Zugriff auf die künftige Datenbank. Diese Vorratsspeicherung sämtlicher Pkw-Bewegungen in Deutschland wurde von den Datenschutzbeauftragten unisono heftig kritisiert.

https://www.datenschutz-hamburg.de/uploads/media/Entschliessung_DSK_PKW-Maut.pdf

Der im Dezember 2014 vom Bundeskabinett beschlossene Gesetzentwurf (BR-Drs. 648/14) sieht keine Bewegungsdatenbank beim BAG mehr vor. Inländer sollen ihren Nachweis für den Rückzahlungsanspruch und für das Nichtnutzen von Bundesstraßen selbst erbringen und glaubhaft machen, etwa durch ein Fahrtenbuch. Die umfassende zentrale Fahrtdatenspeicherung wird ersetzt durch individuelle Nachweissammlungen. Nachweiskonflikte im Fall von Rückforderungen sind vorhersehbar. Unabhängig davon wird dennoch eine umfassende Kontrolle des gesamten Pkw-Verkehrs mit einem Abgleich des Registers der zahlenden Pkws zugelassen. Auf das beim KBA geführte Register mit Zahlungsangaben will der Entwurf also ebenso nicht verzichten wie auf die elektronische Überwachung der Mautzahlung. Der Entwurf behauptet fälschlicherweise, damit „datensparsam“ vorzugehen. Datensparsam wäre, wenn auf die Umsetzung der Pkw-Maut völlig verzichtet würde oder man sich andere EU-Staaten zum Vorbild nähme, die mit einer Plakette und nicht mit Daten Mautgebühren erheben.

Was ist zu tun?

Das datenintensive Pkw-Maut-Verfahren sollte aufgegeben werden.

4.4.5 Auto ohne Parkschein geparkt? Bitte recht freundlich!

Verkehrsüberwacherinnen und Verkehrsüberwacher einer Stadt in Schleswig-Holstein fertigten bei der Kontrolle von Fahrzeugen, die auf Parkplätzen mit Parkschein- oder Parkscheibenpflicht abgestellt wurden, Digitalfotos des gesamten Fahrzeuginnenraumes an, wenn sie keine Parkscheibe bzw. keinen Parkschein vorfanden. Die Stadt rechtfertigte dies damit, dass in der Straßenverkehrsordnung lediglich vorgeschrieben sei, dass der Parkschein oder die Parkscheibe im Fahrzeug von außen gut sichtbar ausgelegt sein muss. Dem Fahrzeugführer bzw. der Fahrzeugführerin stünde es daher frei, den Parkschein auch hinter die Heckscheibe zu legen. Betroffene würden bei Bußgeldverfahren argumentieren, der Parkschein sei in den Fußraum des Fahrzeugs gefallen. Um eindeutig nachweisen zu können, dass Parkschein bzw. Parkscheibe nicht ausgelegt wurden, würde auch das Wageninnere fotografiert. Diese Vorgehensweise sei in vielen Städten in Schleswig-Holstein gängige Praxis. Das ULD kennt auch Städte, die lediglich ein Foto durch die Frontscheibe fertigen, wenn festgestellt wird, dass kein Parkschein oder keine Parkscheibe sichtbar ist.

Das ULD teilte der Stadt mit, dass es aus Gründen der Datensparsamkeit das Fotografieren des kompletten Innenraumes eines Fahrzeugs zur Beweissicherung für übertrieben hält. Das wegen der grundsätzlichen Bedeutsamkeit eingeschaltete Verkehrsministerium wurde um eine rechtliche Einschätzung gebeten. Dieses meint dagegen, dass das Fotografieren des gesamten Innenraumes eines Fahrzeuges im Einzelfall zulässig sein könne. Wegen der nicht eindeutigen Formulierung in der Straßenverkehrsordnung sei die Beschränkung des Fotografierens auf die Frontscheibe nicht durchsetzbar. Die Stadt hat mittlerweile mitgeteilt, dass sie zukünftig Einzelfallprüfungen vornehmen wird.

Die unklaren gesetzlichen Vorgaben zum Auslegen von Parkschein oder Parkscheibe im Fahrzeug haben letztlich unterschiedliche Vorgehensweisen im Land und teilweise übermäßige Datenerhebungen zur Folge. Das ULD regt deshalb eine Präzisierung der Vorschrift an. Kommunen sollten auch durch Allgemeinverfügung festlegen können, wo der Nachweis im Auto abgelegt werden muss. So könnte die bestehende Beweisunsicherheit datensparsam vermieden werden.

Was ist zu tun?

Die verbindlichen Normen über die Ablage von Parknachweisen im Auto sind zu präzisieren.

4.5 Soziales

4.5.1 GKV-Versorgungsstärkungs- und Präventionsgesetz

Der Entwurf eines Gesetzes zur Stärkung der Versorgung in der gesetzlichen Krankenversicherung sieht eine umfangreiche Befugniserweiterung für die gesetzlichen Krankenkassen vor (BR-Drs. 641/14). Zukünftig sollen die Versicherten Anspruch auf ein Krankengeldmanagement oder ein Krankenhausentlassungsmanagement durch ihre Kasse haben. Krankenkassen sollen umfassend prüfen, individuell beraten und mit entscheiden, welche Leistungen erforderlich sind. Sie sollen sogar Servicestellen einrichten können, um die Arzttermine ihrer Versicherten zu überwachen. Alles nur ein freundliches Angebot? Nein!

Wer würde ALDI seine Haushaltskasse überlassen, LIDL die Entscheidung über das Frühstück übertragen? Discounter sollten nicht wissen, wer was gerne isst, welche Lebensmittel man verträgt oder wie voll der Kühlschrank ist. Sie könnten auf eigennützige Gedanken kommen. Erhalten Kassen im System der gesetzlichen Krankenversicherung (GKV) neue Aufgaben, etwa des Krankengeld-

managements, bedeutet dies eine Abkehr von der bislang gesetzlichen vorgesehenen „Gewaltenteilung“ zwischen den Krankenkassen, Ärzten und dem Medizinischen Dienst der Krankenversicherung (MDK). Krankenkassen könnten Versicherte, aber auch Ärzte befragen und den Fortschritt der Genesung überwachen. Es müsste nicht mehr der Amtsarzt des MDK begutachten, wenn Zweifel an der Notwendigkeit einer Behandlung bestehen. Diese neuen Aufgaben würden dazu führen, dass die gesetzlichen Krankenkassen fast uneingeschränkt medizinische Daten ihrer Versicherten erheben, speichern und auswerten könnten.

Wir forderten das Land auf, diesen Gesetzesvorhaben auf Bundesebene nicht zuzustimmen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder forderte: „Keine gesetzliche Legitimierung von datenschutzrechtlichen Missständen beim Umgang mit Krankengeldbeziehern!“

http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/161214_EntschliessungSchlussMitDatenschutzrechtlichenMissstaendenBeimUmgangMitKrankengelsdbeziehern.pdf?__blob=publicationFile&v=1

Auch der aktuelle Entwurf eines Gesetzes zur Stärkung der Gesundheitsförderung und der Prävention (BR-Drs. 460/14) sieht eine umfangreiche Ausweitung der Befugnisse von Krankenkassen vor. Der Entwurf definiert für die Kassen Gesundheitsziele in Bezug auf konkrete Erkrankungen wie Brustkrebs, Depressionen und Diabetes. Versicherte haben zukünftig einen Anspruch auf Untersuchungen zur Früherkennung von Krankheiten. Ärzte sollen Risikofaktoren wie Adipositas, unausgewogene Ernährung, Bewegungsmangel, Rauchen, übermäßigen Alkoholkonsum oder starken chronischen psychosozialen Stress, ausgelöst etwa durch berufliche Belastungen oder Gewaltbelastung im sozialen und familiären Umfeld, erfassen und bewerten.

Wer regelmäßig an diesen Untersuchungen teilnimmt, soll einen Bonus erhalten. Ärzte können individuelle Präventionsleistungen, z. B. Bewegungsangebote in Sportvereinen, empfehlen. Die Krankenkassen übernehmen die Kosten hierfür aber nur, wenn der Versicherte eine ärztliche Bescheinigung vorlegt. So erfahren Krankenkassen, welche Versicherte zu viel trinken oder rauchen, sich nicht ausreichend bewegen oder Stress mit dem Partner haben. Nicht der Arzt entscheidet mehr über die Notwendigkeit von medizinischen Leistungen, sondern das tun künftig in diesen Fällen Krankenkassen.

Beide Gesetzentwürfe zielen darauf ab, den Krankenkassen eine neue Funktion und mehr Macht zu verleihen. Erklärte Absicht ist es, damit die Gesundheit der Bevölkerung zu verbessern. Dafür erhalten die Kassen gesundheitsrelevante Daten ihrer Mitglieder, die es ihnen ermöglichen, die ärztliche Praxis und das Verhalten der Versicherten zu dirigieren. Wirksame Korrektive und Kontrollen fehlen und sind auch nicht geplant. Die Patienten haben keine wirksame Lobby und können sich faktisch nicht wehren. Die Ärzte haben eine Lobby. Statt sich aber für eine effektive Machtbegrenzung und -kontrolle der Kassen einzusetzen, wehren sie sich dort, wo sie sich zu Unrecht von den Kassen kontrolliert fühlen, etwa bei der elektronischen Gesundheitskarte und der Telematikinfrastruktur (32. TB, Tz. 4.5.10). Leidtragende sind letztlich die Patientinnen und Patienten, deren informationelle und medizinische Selbstbestimmung und das informationelle Gleichgewicht im Gesundheitswesen insgesamt.

Was ist zu tun?

Die geplanten Gesetze zur Stärkung der Versorgung in der gesetzlichen Krankenversicherung und zur Stärkung der Gesundheitsförderung und der Prävention dürfen nicht dazu führen, dass bestehende (datenschutz-)rechtliche Grundprinzipien des Sozialleistungsrechts und damit die Rechte der Versicherten ausgehebelt werden.

4.5.2 Europäischer Sozialfonds – nur mit Einwilligung

Das Programm des Europäischen Sozialfonds (ESF) wurde neu aufgelegt. Es fördert mit Mitteln der Europäischen Kommission u. a. Maßnahmen zur Beschäftigung, zur sozialen Inklusion sowie zur Bildung und Ausbildung. Gegenüber den früheren Programmen wurden die Anforderungen der Europäischen Kommission an Kontrolle und Monitoring deutlich erhöht. Will das Land die Fördermittel einsetzen, muss es diese Vorgaben umsetzen. Dafür sind Statistiken und Daten über die Teilnehmenden für die Kommission vorzuhalten. Weiter ist die Prüfung langfristiger Ergebnisindikatoren durch Interviews nach Ende der Förderung vorgesehen, wofür Kontaktdaten der Teilnehmenden vorzuhalten sind. Die europarechtlichen Normen sind insoweit klar und sehen die Verarbeitung der Teilnahmedaten zwingend vor. Da bei den geförderten Maßnahmeträgern vielmals Berufsgeheimnisträger (Psychologen, Sozialpädagogen etc.) tätig sind, bedarf es für die notwendigen Auskünfte der Information und der Einwilligung der Teilnehmenden.

Die Teilnahme an den Maßnahmen darf vom Vorliegen der Einwilligung abhängig gemacht werden. Andernfalls ist die Refinanzierung nicht gesichert. Bei einigen Teilprogrammen ist die Angabe besonders sensibler Daten, etwa der Grad der Behinderung, die Zugehörigkeit zu einer Minderheit oder die Herkunft, vorgesehen. Weil sich die Angaben in keinem der Teilprogramme auf Fördervoraussetzungen beziehen, war den Teilnehmern die Möglichkeit einzuräumen, die Angabe zu diesen Daten ohne Nachteile zu verweigern.

Was ist zu tun?

Bei ESF-Maßnahmen sind vor Beginn der Maßnahme die Teilnehmenden umfassend über mögliche personenbezogene Übermittlungen und Kontrollen zu informieren und die hierfür nötigen Einwilligungen einzuholen.

4.5.3 Jugendhilfe – Netzwerkarbeit nur mit Einwilligung der Betroffenen

Wenn Familien Probleme haben und Kinder leiden, ist schnelle und frühe Hilfe gefragt. Jugendämter benötigen die Unterstützung der freien Träger der Jugendhilfe und sind auf eine enge Zusammenarbeit u. a. mit Beratungsstellen, den Schulen und Kindergärten, Kinderärzten, Hebammen, Sportvereinen, aber auch der Polizei und Kirche angewiesen. Man trifft sich in großer Runde, um Informationen auszutauschen und Hilfen abzustimmen. Zwangsläufig werden sensibelste Daten von Familien weitergegeben und offenbart. Unter welchen Voraussetzungen darf diese Netzwerkarbeit erfolgen?

Netzwerkarbeit soll einsetzen, bevor die Probleme in Familien zu groß werden. Um Gefährdungssituationen früh zu erkennen, tauschen die Teilnehmer regionaler Netzwerke ihre Erkenntnisse aus. Wer weiß etwas und wer könnte helfen? Die Netzwerkteilnehmer unterliegen jedoch unterschiedlichsten Schweigeverpflichtungen. Was einer Schule erlaubt ist, kann einem Kinderarzt verboten sein. Die Polizei muss berichten, darf aber vieles nicht erfahren. Dies führt in den Netzwerken zu Problemen und Missverständnissen. Damit die Zusammenarbeit funktioniert, müssen die Teilnehmer wissen, wer was darf.

In den Kreisen Dithmarschen, Steinburg, Schleswig-Flensburg und Pinneberg wurden die Jugendämter aktiv, luden das ULD ein und informierten sich zum Thema „Datenschutz“. Dabei bestätigte sich die Befürchtung, dass fehlendes Wissen nicht nur zu Unsicherheit, sondern zu Untätigkeit führt. Gemeinsam wurden Möglichkeiten der Zusammenarbeit aufgezeigt.

Auch in einer großen Runde kann über Problemfamilien gesprochen werden. Allerdings darf hierbei nicht die Identität der Betroffenen preisgegeben werden. Der Berichterstatter muss den Fall zunächst pseudonymisiert darstellen. Die Netz-

werkteilnehmer, die der Familie helfen können, bilden eine Arbeitsgruppe. Das Jugendamt klärt für diese Netzwerkteilnehmer, was zu beachten ist, bevor die Identität der Familie offengelegt wird. Viele Netzwerkteilnehmer benötigen eine Einwilligung der Betroffenen, eine Schweigepflichtentbindung, um sich beim Datenaustausch nicht strafbar zu machen. Gemeinsam mit dem Jugendamt haben wir Mustererklärungen entworfen, die sicherstellen, dass die betroffenen Familien ausreichend informiert und deren Daten nicht ohne Befugnis zwischen den Netzwerkteilnehmern ausgetauscht werden.

Wie eine Schweigepflichtentbindungserklärung datenschutzgerecht gestaltet werden kann, steht unter Tz. 4.6.5.

Was ist zu tun?

Eine Netzwerkarbeit in der Jugendhilfe setzt voraus, dass die Netzwerkteilnehmer nur befugt Daten der betroffenen Familien austauschen. Oftmals wird als Befugnis die Einwilligung der Familien benötigt. Das Jugendamt sollte geprüfte Mustereinwilligungserklärungen zur Verfügung stellen.

4.5.4 Kindertagesstättenpersonal und Genehmigungsbehörden

Die eigenen Kinder im Kindergarten in fremde Hände zu geben, hinterlässt bei vielen Eltern ein ungutes Gefühl. Sie wissen wenig über die Erzieherinnen und Erzieher, die jeden Tag die Betreuung übernehmen. Man hofft, dass die Träger der Kindertagesstätten ihr Personal gut ausgewählt, sich informiert haben und keine „dunkle Vergangenheit“ verborgen bleibt. Vertrauen ist gut, Kontrolle oftmals besser. Es ist zunächst nachvollziehbar, dass Kreise im Rahmen ihrer Aufsichtspflicht von den Trägern der Kindertagesstätten Führungs- und Fachzeugnisse, Lebensläufe oder Erste-Hilfe-Scheine des im Kindergarten beschäftigten Personals anfordern, um aus diesen Dokumenten eigene Personalakten zu erstellen.

Wie umfassend darf dieser Eingriff in die Privatsphäre des Kindergartenpersonals sein? Ein Träger von Kindertagesstätten war nicht bereit, dem Kreis die geforderten Unterlagen der Erzieherinnen und Erzieher zu übermitteln. Das ULD kam zu dem Ergebnis, dass es grundsätzlich genügen muss, wenn Träger der Kindertagesstätten diese Unterlagen bei Einstellung ihres Personals einfordern und speichern. Eine Weiterleitung von Kopien dieser Dokumente an den Kreis greift unangemessen in die Privatsphäre der Mitarbeiter ein. Eine allumfassende Kontrolle durch die Aufsichtsbehörden ist nicht erforderlich und gesetzlich nicht vorgesehen. Das Landesjugendamt sieht dies ebenfalls so und lehnt deshalb eine doppelte Personalaktenführung ab.

Das ULD hat ein stichprobenartiges Kontrollverfahren vorgeschlagen. Die Beschäftigten müssen dann vor ihrer Einstellung über diese Möglichkeit in Kenntnis gesetzt werden. Bei der Stichprobenprüfung kann festgestellt werden, ob der Träger der Einrichtungen die Auswahl des Personals pflichtgemäß und nach den vom Kreis gesetzten Maßstäben trifft. Wie oft und durch welche Maßnahmen die Stichproben durchgeführt werden, ist nach Maßgabe des Erforderlichen festzulegen.

Was ist zu tun?

Kreise dürfen Führungszeugnisse der Beschäftigten in Kindertagesstätten von den Trägern anfordern und diese prüfen. Die Anforderung der Unterlagen darf nicht pauschal erfolgen, sondern nur stichprobenartig.

4.5.5 Unsicheres internetbasiertes Dokumentenmanagement

Anfang November 2011 wurde bekannt, dass im Internet etwa 3.600 Dokumente der Brücke Rendsburg-Eckernförde e. V. und von anderen Hilfsorganisationen für psychisch Kranke mit sensiblen Angaben zu Patientinnen und Patienten im Internet technisch ungeschützt abgerufen werden konnten. Die Dokumente waren in einem für interne Zwecke genutzten System abgelegt, das über das Internet betrieben wurde. Die Dokumentenverzeichnisse waren nicht gegen einen Zugriff von außen gesichert. Dienstleister für diesen Datendienst war die RebuS gGmbH, eine hundertprozentige Tochter der Brücke Rendsburg-Eckernförde e. V. Nach Einschaltung des ULD wurde der Dienst abgestellt und das ULD begann die Ermittlungen, wie es zu diesem Datenleck kommen konnte.

Dabei ist das ULD auf verschiedene Partner gestoßen, die in unübersichtlicher Weise an der Entwicklung und dem Betrieb des Dienstes beteiligt waren. Wer in dem Zusammenspiel dieser Stellen welche Aufgaben, Pflichten und Befugnisse hatte, war nicht geregelt. Mangels Dokumentation konnten wesentliche Schritte der Administration des Dienstes nicht mehr nachvollzogen werden. So konnten Brücke und RebuS nicht aufklären, ob für die Dokumentenablage in dem Dienst, der seit dem Jahr 2002 betrieben wurde, jemals ein wirksamer Zugriffsschutz bestanden hat.

Das ULD hat Bußgelder gegen die RebuS gGmbH und gegen die Brücke Rendsburg-Eckernförde e. V. in Höhe von insgesamt 18.000 Euro verhängt. Die Bußgeldbescheide sind rechtskräftig.

4.6 Schutz des Patientengeheimnisses

Der Schutz des Patientengeheimnisses ist anspruchsvoll und komplex. An ihm zerren unterschiedlichste, zumeist wirtschaftlich motivierte Interessen. Der Schutz ist bei der Normsetzung und in der Praxis gefordert, bei Behandlung, Betreuung, Abrechnung, Forschung, beim Einsatz modernster Informationstechnik. Verstöße können dramatische Folgen für den Patienten haben.

Eine Petentin berichtete uns von einer „missglückten“ Blasenspiegelung bei ihrem Urologen. Sie hatte große Angst vor der Untersuchung, aber Vertrauen zu dem Arzt. Die Untersuchung war schmerzhaft. Eine Arzthelferin hielt ihre Hand. Mitten in der Untersuchung verließ eine andere Arzthelferin den Behandlungsraum und ließ die Tür offen stehen. Vom Empfangstresen aus hatten die Wartenden so freien Blick auf das Behandlungsgeschehen und die Patientin. Diese verkrampfte. Die Situation führte für sie zu kaum ertragbaren körperlichen und seelischen Schmerzen. Wie in einer Schockstarre war es ihr nicht mehr möglich, etwas zu sagen, sich zu beschweren oder gar zu wehren. Sie empfand absolute Hilflosigkeit, verließ die Praxis wie in Trance. Noch Monate später durchlebt die Patientin diese erniedrigende Situation immer und immer wieder. Albträume, Panikattacken und Angstzustände quälen sie.

Derartige Schilderungen sind für das ULD Bestätigung und Ansporn, das Patientengeheimnis gegen die unterschiedlichsten Angriffe zu verteidigen, deren Hintergründe so unterschiedlich sein können: Gedankenlosigkeit, Technikverliebtheit, Profitstreben …

4.6.1 eHealth

eHealth – der Einsatz von Informationstechnik (IT) im Gesundheitswesen – ist allgegenwärtig und bestimmt oft die medizinische Praxis. Die normativen Grundlagen des Vertraulichkeitsschutzes blieben teilweise seit Jahrzehnten unverändert.

Anlässlich einer öffentlichen Anhörung des Bundestagsausschusses „Digitale Agenda“ zum Thema „eHealth“ machte das ULD unter dem Titel „Gesundheitsdaten bedürfen eines besonderen staatlichen Schutzes“ auf die gesetzgeberischen Defizite aufmerksam. Es besteht die Gefahr, dass die medizinischen Daten zur Beeinflussung des medizinischen Versorgungsgeschehens sowie für vorrangig kommerzielle Zwecke verwendet und hierdurch die Vertraulichkeit der Daten und damit das Vertrauen der Betroffenen beeinträchtigt werden. Folgende Trends sind dabei bestimmend:

- Die Arbeitsteilung im Medizinbereich und die Einschaltung von informationstechnischen Dienstleistern verunklart Verantwortlichkeiten und verstärkt über duplizierte Datenbestände das Risiko zweckwidriger Nutzungen.
- Durch biotechnologische (gentechnische) Verfahren fallen immer mehr Daten an, die für die Betroffenen schicksalhaft sind und von denen für diese ein hohes Diskriminierungsrisiko ausgeht.
- Die Einbindung des Internets bei der Informationsverarbeitung im Gesundheitswesen, z. B. durch Nutzung von Cloud-Diensten, sozialen Netzwerken und Big-Data-Technologien, erhöht das Risiko für die Vertraulichkeit und die Integrität der Daten.
- Angesichts des Kostendrucks im Gesundheitswesen und der Möglichkeit der zentralen Auswertung und Nutzung von Behandlungs- und Abrechnungsdaten drohen die Diskriminierung von bestimmten Personengruppen bei der Versorgung und eine unzulässige Beeinflussung des Behandlungsgeschehens.

Anforderungen

Die Potenziale der Informationsverarbeitung zur Verbesserung der Gesundheit in der Gesellschaft sowie individuell sollen genutzt werden. Zugleich sind dabei aber die damit einhergehenden Gefahren für Wahlfreiheit und Vertraulichkeit zu vermeiden. Der Gesetzgebung stellen sich so folgende Aufgaben:

- Die Telematikinfrastruktur ist zeitnah und funktionsfähig so zu realisieren, dass die medizinische Kommunikation zwischen den Gesundheitsdienstleistern vertraulich und zuverlässig ermöglicht wird und die Patientinnen und Patienten praktisch in die Lage versetzt werden, ihr Recht auf informationelle Selbstbestimmung wahrzunehmen.
- Da elektronische Kommunikation im gesamten Gesundheitssektor genutzt wird, dürfen sich zu schaffende datenschutzrechtliche Regelungen nicht auf einzelne Teilbereiche beschränken, sondern sollten den gesamten Gesundheitsbereich unter Einbeziehung u. a. der niedergelassenen Ärzteschaft, des Pflegewesens und anderer Gesundheitsberufe erfassen.
- Die Datenverarbeitung im gesetzlichen wie im privaten Versicherungsbereich ist so zu regeln und zu gestalten, dass dort Transparenz, Datensparsamkeit und eine wirksame Kontrolle gewährleistet werden.
- Ökonomische Veränderungen bei Leistungserbringern, z. B. Betriebswechsel, Forderungsabtretungen, Fusionen (z. B. zu bundesweiten Krankenhauskonzernen) und Abspaltungen, dürfen nicht zu einer Beeinträchtigung von Vertraulichkeit, Transparenz und Wahlfreiheit führen, wozu neue technische, organisatorische und rechtliche Vorkehrungen getroffen werden müssen. Änderungen in der Konzernstruktur dürfen nicht dazu führen, dass Datenzugriffe aus Drittstaaten ermöglicht werden. Gegen gesetzliche Zugriffsrechte aus Drittstaaten sind geeignete technische und organisatorische Schutzmaßnahmen vorzusehen.
- Die Abrechnung im Bereich der gesetzlichen Krankenversicherung ist auch aus Gründen des Datenschutzes vorrangig eine hoheitliche Aufgabe, die nur begrenzt und unter hohen Anforderungen an Private delegiert werden kann.
- Durch eine Verbesserung der Koordinierung und Intensivierung der Kontrolle von Informationsdienstleistern im Medizinbereich ist dafür zu sorgen, dass bei zweckändernder Weiternutzung der Daten deren Anonymität sichergestellt wird.
- Die Bereitstellung von aggregierten Gesundheitsdaten für Zwecke der Versorgungsplanung und zur Herstellung demokratischer Transparenz des Gesundheitswesens ist eine staatliche Aufgabe, die Bund

und Länder unter Einbeziehung der Krankenversicherungen und der Gesundheitsdienstleister zu erfüllen haben.

- Die Einschaltung von Dienstleistern im Bereich von Krankenhäusern und sonstigen heilberuflich Tätigen ist durch gesetzliche Regelungen so rechtssicher zu gestalten, dass sowohl die Funktionalität der Dienstleistungen als auch das Patientengeheimnis gewährleistet werden. Daten, die beim Behandelnden einer gesetzlichen Schweigepflicht unterliegen, müssen auch bei externen Dienstleistern dem gleichen Schutzniveau unterliegen, einschließlich eines umfassenden Beschlagnahmeschutzes.
- Die Krankheitsregistrierung für Zwecke der klinischen und epidemiologischen Forschung wie der Qualitätssicherung und Behandlungsunterstützung ist auf Bundes- und Landesebene möglichst einheitlich gesetzlich so zu regeln, dass Transparenz und Selbstbestimmung der Betroffenen gewahrt bleiben.
- Durch ein gesetzliches Forschungsgeheimnis sowie durch Anonymisierungs- und einheitliche Genehmigungserfordernisse kann die Bereitstellung der nötigen Datengrundlagen für die medizinische Forschung gesichert werden, ohne die Vertraulichkeit der Daten übermäßig zu beeinträchtigen.
- Die Bundesregierung soll sich dafür einsetzen, dass Standards für eine datenschutzkonforme Gestaltung von medizinischen IT-Produkten und -Verfahren erarbeitet und deren Einsatz z. B. durch gesetzlich regulierte Zertifizierungsangebote gefördert werden.

Nach Ansicht des ULD wird die Diskrepanz zwischen rechtlich geforderter Vertraulichkeit und informationstechnischer Praxis immer größer. Die – oft unzulässigen – Begehrlichkeiten an Gesundheitsdaten wachsen in den Himmel von Big Data, Cloud Computing & Co., wobei der Patient und seine Rechte oft auf der Strecke bleiben.

Referentenentwurf für ein eHealth-Gesetz

Ein vom Bundesgesundheitsministerium im Januar 2015 veröffentlichter Entwurf eines sogenannten eHealth-Gesetzes enttäuscht. Er wird seinem Anspruch, „für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen“ zu sorgen, nicht gerecht, indem er insbesondere das Ziel verfolgt, endlich die seit neun Jahren überfällige Telematikinfrastruktur (TI) und die elektronische Gesundheitskarte (eGK) mit finanziellen Sanktionen und Anreizen durchzusetzen. Diese TI ist eine zentrale und notwendige Grundvoraussetzung für sichere medizinische Kommunikation. Um allerdings die bisherigen Widerstände gegen die TI und die eGK zu überwinden, bedarf es weiterer Anstrengungen.

Der Vorschlag aus dem Bundesgesundheitsministerium befasst sich nur mit der ersten der oben genannten insgesamt elf zwingenden Voraussetzungen, um die elektronische Verarbeitung von Gesundheitsdaten auf eine sichere rechtliche Grundlage zu stellen, die technisch und faktisch auf der Höhe der Zeit ist. Nach Ansicht des ULD müssen die oft widersprüchlichen und aus vortechnischer Zeit stammenden Gesetze weiterentwickelt werden. Der vorliegende Entwurf adressiert einseitig die wirtschaftlichen Interessen von Ärzteschaft und Krankenhausbetreibern und verliert die Patienten mit ihren Bedürfnissen nach Transparenz und Vertraulichkeit aus dem Blick. Das ULD rät, den Entwurf – nach einigen Verbesserungen aus Datenschutzsicht – zur Etablierung einer medizinischen Telematikinfrastruktur weiterzuverfolgen. In einem zweiten Schritt muss versucht werden, das Patientengeheimnis und medizinische Funktionalitäten zusammenzubringen. Nur so kann der Gesetzgeber die Voraussetzungen dafür schaffen, dass die deutsche IT-Industrie im Gesundheitssektor nicht von halbseidenen Anbietern etwa aus Übersee ausmanövriert wird.

https://www.datenschutzzentrum.de/artikel/874-.html

4.6.2 Krebsregistergesetz Schleswig-Holstein

Durch Bundesgesetz sind die Länder gehalten, klinisch-epidemiologische Krebsregister einzurichten. In dem Register sind künftig alle Behandlungsvorgänge zu einer Krebserkrankung zu erfassen, sodass der Forschung auch Angaben über die Wirksamkeit bestimmter Behandlungsmethoden flächendeckend vorliegen. Durch epidemiologische Analysen soll auch künftig ein regionaler Überblick über Krebserkrankungen möglich sein. Der Regierungsentwurf sieht vor, die unter Mitwir-

kung des ULD für das epidemiologische Krebsregister entwickelte und bewährte Trennung von identifizierenden Daten und von pseudonymisierten klinisch-epidemiologischen Daten fortzuführen. Erstere sollen auch künftig in einer Vertrauensstelle, angesiedelt bei der Ärztekammer in Bad Segeberg, vorgehalten werden. Die zur Forschung erforderlichen medizinischen Daten stehen davon getrennt der Wissenschaft zur Verfügung.

Um die Vollständigkeit des Registers sicherzustellen, ist eine namentliche Meldepflicht für alle behandelnden Ärzte und Einrichtungen vorgesehen. Nur so können die Behandlungsverläufe einrichtungsübergreifend erfasst werden. Zum Schutz des Betroffenen sind die identifizierenden Angaben in der Vertrauensstelle zu löschen, wenn dieser widerspricht. Eine Zuordnung neuer Meldungen bleibt weiterhin über das Pseudonym möglich, aus dem jedoch nicht auf die Identität des Patienten geschlossen werden kann und darf. Der gefundene Kompromiss schränkt bei größtmöglichem Erhalt der informationellen Selbstbestimmung die Verwendung der Daten zu Forschungszwecken im geringstmöglichen Maß ein.

Im Vergleich zu Lösungen in anderen Bundesländern ist die geplante Umsetzung ausgesprochen datensparsam.

Was ist zu tun?

Nach Verabschiedung des Krebsregistergesetzes ist dieses gemäß den normativen Vorgaben sorgfältig umzusetzen.

4.6.3 Hackerangriff auf Pflegedokumentation – Patientendaten als Geiseln

Krankenhäuser, Arztpraxen, aber auch Pflegeheime und Pflegedienste speichern Patientendaten elektronisch. Die EDV muss sicher sein. Unbefugte sollen keinen Zugriff haben. Aber Sicherungsmaßnahmen sind aufwendig und kosten viel Geld.

Für Mitarbeiter eines kleinen Pflegedienstes begann ein Arbeitstag damit, dass sich die Computer nicht starten ließen. Die Rechner waren von einem Virus befallen, die Daten der Patientinnen und Patienten verschlüsselt und nicht mehr lesbar. Tourenpläne ließen sich nicht öffnen. Panik machte sich breit. Es kam noch schlimmer! Kurze Zeit später erhielt der Pflegedienst eine E-Mail. Die EDV wurde gezielt angegriffen, die Patientendaten wurden zu Geiseln gemacht. Die Täter drohten mit der Löschung der Daten, wenn nicht binnen 24 Stunden ein Lösegeld gezahlt würde. Dem Pflegedienst blieb nichts anderes übrig, als zu zahlen.

Der Pflegedienst reagierte professionell. Statt den Vorfall zu verschweigen, wurde das ULD um Hilfe gebeten. Es wurden Sofortmaßnahmen zum Schutz der Patientendaten ergriffen. Gemeinsam mit dem ULD wurden grundsätzliche Vorgaben zur sicheren Nutzung der EDV umgesetzt. Eine Strafanzeige gegen unbekannt wurde erstattet, die Ermittlungen laufen noch. Möglicherweise hat es der Pflegedienst den Angreifern zu einfach gemacht. Das ULD steht mit Rat und Tat zur Seite.

Was ist zu tun?

Daten verarbeitende Stellen müssen ausreichende Sicherungsmaßnahmen zum Schutz personenbezogener Daten ergreifen, insbesondere wenn diese sensibel sind.

4.6.4 Die Krankenhausrechnung von der fremden Firma

Darf ein privates Unternehmen die Krankenhausrechnungen erstellen? Ja, aber nur wenn der Patient ausreichend informiert wurde und schriftlich seine Einwilligung in die dafür nötige Datenübermittlung erklärt. Das Krankenhaus muss mit dem Abrechnungsunternehmen in einem schriftlichen Vertrag die Aufgabe und Befugnisse präzise festlegen. Welchen Inhalt die schriftliche Einwilligung, die Schweigepflichtentbindungserklärung, haben muss, wird unter Tz. 4.6.5 dargestellt. Fehlt die wirksame Einwilligung des Patienten, verstößt die Übermittlung von dessen Daten gegen die ärztliche Schweigepflicht. Der übermittelnde Arzt macht sich strafbar.

Selbst wenn ein Patient einverstanden ist, dürfen dem Abrechnungsunternehmen nicht unbegrenzt Patientendaten übermittelt werden. Für die Rechnung genügen grundsätzlich Angaben zu den durchgeführten Behandlungsleistungen einschließlich Datum, Name, Anschrift und Geburtsdatum des Patienten sowie Angaben zum Krankenversicherungsunternehmen. Daten zur Anamnese, Diagnosen und Untersuchungsergebnisse dürfen nicht übermittelt werden.

In einem aktuellen Fall bestand die Befürchtung, dass ein Krankenhaus dem Abrechnungsunternehmen die vollständigen Patientenakten überließ. Dies ist unzulässig. Die Krankenhausmitarbeiter müssen die benötigten Daten aus der Patientendokumentation heraussuchen und dem Abrechnungsunternehmen bereitstellen. In jedem Fall benötigt das Krankenhaus einen schriftlichen Vertrag mit dem Abrechnungsunternehmen. Diesem muss vorgegeben werden, „was es zu tun und was es zu lassen hat“. Der Auftraggeber trägt die Verantwortung für diese Datenverarbeitung im Auftrag. Verstöße des Auftragnehmers gehen stets zulasten des Auftraggebers. Diesem obliegen Kontrollbefugnisse und -verpflichtungen.

Was ist zu tun?

Bevor ein privates Abrechnungsunternehmen beauftragt wird, müssen die Patienten informiert werden und schriftlich in die Datenübermittlung einwilligen. Zwischen Krankenhaus und Abrechnungsfirma muss ein Vertrag geschlossen werden, der den gesetzlichen Anforderungen entspricht.

4.6.5 Muster einer Schweigepflichtentbindungserklärung

Nie ein Krankenhaus aufsuchen zu müssen, bleibt nur wenigen Menschen in ihrem Leben vergönnt. Der Ablauf eines Aufenthalts ist Routine: Aufnahme, Gespräch mit den Ärzten, Behandlung. Nur selten wird hinterfragt, welche Abläufe es im Hintergrund gibt. Damit der Betrieb eines Krankenhauses reibungslos vonstattengehen kann, arbeitet es mit externen Dienstleistern und Laboren zusammen. Die Liste der Kooperationspartner kann lang werden. Wer ist die Schwester, die gerade meine Akte zu sich genommen hat? Wer tippt das Protokoll meiner Behandlung ins EDV-System? Woher weiß die Essensversorgung, dass ich keine Laktose vertrage? Nicht immer ist klar, wer Mitarbeiter des Krankenhauses ist und wer zu einem externen Dienstleister gehört. Solche externen Unternehmen dürfen Patientendaten nur zur Kenntnis erhalten, wenn eine wirksame Schweigepflichtentbindung zur Zusammenarbeit vorliegt. Darin sind alle externen Dienstleister aufzulisten, an welche Patientendaten übermittelt werden, der genaue Datenumfang sowie eine explizite Zweckbeschreibung. Eine ausführliche Erklärung, die detailliert die datenschutzrechtlich vorgesehenen „Fünf-plus-zwei“-Punkte enthält, ist für viele Patienten unverständlich und lästig. Bei der Nutzung einer solchen ausführlichen Einverständniserklärung passiert es schnell, dass die Patienten einfach unterschreiben, ohne diese zu lesen.

„Fünf-plus-zwei"-Punkte bei einer Einwilligung:

1. Wer übermittelt? (Name des Senders)
2. Wessen Daten? (Name des Betroffenen)
3. Wem? (Name des Empfängers)
4. Welche Daten? (Datenumfang)
5. Wofür? (Zu welchem Zweck?)
6. Freiwilligkeit
7. Mit Wirkung für die Zukunft widerrufbar

Daher hat das ULD eine Mustereinwilligungserklärung entwickelt, die einen Mittelweg zwischen dem Zuviel und dem Zuwenig geht. Die mehrstufige Einwilligungserklärung besteht aus einem kurz gehaltenen Einverständnisbogen, auf dem die Einwilligung des Patienten durch Unterschrift erfolgt, und einem umfangreichen Aufklärungsblatt, auf welchem eine vollständige Auflistung aller Kooperationspartner des Krankenhauses und alle anderen ausführlichen Informationen aufgeführt sind. Das Aufklärungsblatt ist immer zusammen mit dem Einverständnisbogen auszugeben.

Die mehrstufige Einwilligungserklärung hat den Vorteil, dass die Patienten selbst entscheiden können, wie umfangreich sie sich über die Übermittlung ihrer Patientendaten informieren. Für diejenigen, die mit einer knappen Erläuterung, die jedoch in kurzer Form auch die „Fünf-plus-zwei"-Punkte enthält, zufrieden sind, genügt der Einverständnisbogen als Informationszugang. Für diejenigen, die das Verfahren hinterfragen, bietet das Aufklärungsblatt eine Möglichkeit zur Beantwortung der aufkommenden Fragen. Genannt werden müssen natürlich auch Ansprechpartner, der behandelnde Arzt oder geschultes Krankenhauspersonal, mit denen weitere Fragen im Gespräch erörtert werden können. Die Folgen bei einer Nichteinwilligung sind zu benennen. Wichtig ist zudem die Information, dass eine Notfallbehandlung in jedem Fall stattfindet.

Das Muster der mehrstufigen Einwilligungserklärung dient den Krankenhäusern als Orientierung. Der Aufbau und die Umsetzung der jeweiligen Schweigepflichtentbindungserklärung können abweichen. Das ULD empfiehlt den Krankenhäusern jedoch, anhand des veröffentlichten Musters zu prüfen, ob Wesentliches fehlt.

https://www.datenschutzzentrum.de/artikel/879-.html

Was ist zu tun?

Krankenhäuser dürfen Patientendaten an externe Dienstleistungsunternehmen und Labore übermitteln, wenn eine schriftliche Einwilligung der Patienten vorliegt, in der diese ausführlich über den Umfang der Datenübermittlungen unterrichtet werden. Das Muster der mehrstufigen Einverständniserklärung kann als Vorlage dienen.

4.6.6 Allergiepräparate auf Bestellung – Millionen Patientendatensätze

Gesundheitsfördernde Medikamente bekommt der Mensch in der Apotheke seines Vertrauens. Apotheker unterliegen der beruflichen Schweigepflicht, anderes gilt für Pharmaunternehmen.

Bei Allergien raten Ärzte oft zu einer spezifischen Immuntherapie und verschreiben entsprechende Präparate. Mit dem vom Arzt ausgestellten Rezept geht der Patient zu seiner Apotheke. Auf die Herstellung der Allergiepräparate haben sich wenige Pharmaunternehmen spezialisiert: Die benötigten Präparate müssen die Apotheken mittels eines Bestellbogens bei den Herstellern anfordern. Die Prüfergebnisse des ULD bezüglich der Bestellsysteme von zwei Pharmaunternehmen aus Schleswig-Holstein lösten „allergische" Reaktionen aus. Eine Firma hatte in den letzten 18 Jahren unbefugt beinahe 1.000.000 Datensätze von ca. 75.000 Patientinnen und Patienten erhoben und gespeichert.

Die verwendeten Bestellbögen sahen vor, dass bereits in der Arztpraxis angegeben wurde, welcher Patient welches Präparat benötigte. Auf

dem Bestellbogen wurden der Name, das Geburtsdatum, die Anschrift und die Kassenzugehörigkeit des Patienten vermerkt. In den Apotheken wurden die Bestellbögen an das Pharmaunternehmen gefaxt. Oft genug wurde zusätzlich das Rezept gefaxt. Die Pharmaunternehmen speicherten diese Daten und konnten so über Jahrzehnte nachvollziehen, welcher Patient von welchem Arzt wegen welcher Diagnose welches Präparat verschrieben und von welcher Apotheke ausgehändigt bekam.

Die Übermittlung von Patientendaten an ein Pharmaunternehmen ist nur zulässig, wenn die Patientinnen und Patienten zuvor ausreichend informiert werden und schriftlich ihre Einwilligung erklären (Tz. 4.6.5). Ohne eine derartige Befugnis machen sich die Apotheker strafbar.

Aber Vorsicht: Eine Einwilligung hilft nicht weiter, wenn das Pharmaunternehmen keinen legitimen Grund und Zweck angeben kann, weshalb es die konkreten Daten benötigt. Die Pharmaunternehmen begründeten ihre Begehrlichkeit mit dem damit ermöglichten Serviceangebot für die Patienten und Ärzte. Immuntherapien können sich über Jahre hinziehen. Die Dosierung und Zusammensetzung der Präparate ist vom Therapiestand abhängig. Eine falsche Medikation kann verheerende Folgen für den Patienten haben.

Wer behält den Überblick, wenn z. B. zwischendurch der Arzt gewechselt wird? Das Datensammeln wurde mit der Patientensicherheit gerechtfertigt.

Wir forderten die Pharmaunternehmen auf,

- ein Verfahren zu entwickeln, das sicherstellt, dass Patienten von ihren Ärzten bzw. Apothekern ausreichend über das „Serviceangebot“ und die beabsichtigte Datenübermittlung und -speicherung aufgeklärt werden,
- die Möglichkeit der anonymen Bestellung der benötigten Präparate anzubieten, wenn Patienten ihre Daten nicht übermittelt sehen wollen,
- für die dem Verfahren zustimmenden Patienten datenschutzgerecht gestaltete Einwilligungserklärungen zu erarbeiten und zu nutzen,
- den Umfang der übermittelten Patientendaten durch eine Neugestaltung der Bestellbögen zu minimieren,
- sicherzustellen, dass ausschließlich der Bestellbogen und nicht mehr Rezepte etc. von den Apotheken übermittelt werden,
- Patientendaten nur so lange zu speichern, wie dies wirklich für die Patientensicherheit erforderlich ist.

Ein Pharmaunternehmen erklärte sich bereit, die notwendigen Schritte zu gehen. Gemeinsam mit dem ULD werden datenschutzgerechte Lösungen erarbeitet. Es werden Aufklärungsbögen und Mustereinwilligungen gestaltet, sichere Übertragungswege geschaffen, Verfahrensvorgaben für die Apotheker erarbeitet und ein Löschkonzept erstellt. Aus einer Prüfung wurde eine Beratung. Allergiepatienten können sich freuen.

Was ist zu tun?

Apotheker dürfen die Daten von Patienten an Pharmaunternehmen nur übermitteln, wenn diese zuvor ausreichend informiert ihre Einwilligung erklärt haben.

4.6.7 Peer Review und Qualitätsmanagement in der Medizin

Die Ärztekammer Schleswig-Holstein ist mit einem geplanten Peer-Review-Verfahren an das ULD herangetreten. Danach besucht eine kleine Gruppe von Experten – leitende Ärzte von Intensivstationen und leitende Intensivpfleger – eine andere Einrichtung, um im gegenseitigen Diskurs die Qualität der Behandlung zu erhöhen und für alle Beteiligten neue Erkenntnisse zu erlangen. Die bettseitige Begehung der Station regt den Erfahrungsaustausch an und bietet Gelegenheit, Verbesserungsmöglichkeiten aufzuzeigen. Derartige Maßnahmen, bei denen patientenbezogene Daten

zur Kenntnis gelangen, sind grundsätzlich nur mit Einwilligung der Patienten durchzuführen. Bei Intensivstationen ist dabei weder die Belegung im Vorwege planbar noch auszuschließen, dass bewusstlose Patienten betroffen sind.

Lebenslanges Lernen und die Bestrebungen zur Verbesserung der Qualität im Gesundheitsbereich sollten nicht durch den Datenschutz blockiert werden. Das ULD schlug vor, das unter der Kontrolle der zuständigen Kammer eingerichtete und streng geregelte Verfahren unter enger Begleitung des ULD einzuführen. Die erforderlichen gesetzlichen Rechtsgrundlagen sollten in einem neuen Pflegekammergesetz eingeführt werden. Das ULD regt eine Übernahme solcher Normen auch für das Heilberufekammergesetz an.

Die Begrenzung auf öffentlich-rechtlich organisierte Kammern als Initiatoren und die Erfordernis einer Satzung soll ein Ausufern der Maßnahme verhindern. Allgemeine Maßnahmen zur Qualitätssicherung durch Externe und die Kontrolle durch Gutachter stehen weiterhin unter dem Vorbehalt einer Einwilligung aller betroffenen Patientinnen und Patienten oder einer gesetzlichen Regelung.

Was ist zu tun?

Der Gesetzgeber sollte die angeregten Ergänzungen übernehmen, um eine gesicherte gesetzliche Basis für Peer-Review-Verfahren zu schaffen.

4.6.8 Anonymisierung von Rezeptdaten

Ein Arzt teilte dem ULD mit, dass vor einigen Jahren Bluthochdruckpatienten bei ihm ein Anschreiben eines Unternehmens vorlegten, in dem sie aufgefordert wurden, sich von ihrem Arzt ein neues Hochdruckpräparat verschreiben zu lassen. Wie das Unternehmen an die hochsensiblen Gesundheitsdaten gelangt war, ließ sich nicht mehr aufklären. Aufgeklärt werden kann jedoch, wie mit Patientendaten in Deutschland systematisch umgegangen wird.

§ 300 Abs. 2 Satz 1, 2 SGB V

Die Apotheken […] können zur Erfüllung ihrer Verpflichtungen […] Rechenzentren in Anspruch nehmen. Die Rechenzentren dürfen die Daten für im Sozialgesetzbuch bestimmte Zwecke […] nur in einer auf diese Zwecke ausgerichteten Weise verarbeiten und nutzen, soweit sie dazu von einer berechtigten Stelle beauftragt worden sind; anonymisierte Daten dürfen auch für andere Zwecke verarbeitet und genutzt werden.

Im Sozialgesetzbuch (SGB) V wird den Apotheken erlaubt, für die Weiterleitung der Rezeptdaten an die Krankenkassen Apothekenrechenzentren zu beauftragen. Diese Daten sind für die Rechenzentren über die Dienstleistungsaufgabe hinausgehend von wirtschaftlichem Wert – lässt sich doch aus den Daten die Gesamtheit aller ärztlichen Verschreibungen in Deutschland ableiten. Die Daten unterliegen aber dem Patienten- und dem Sozialgeheimnis. Ziel ist der Schutz des Vertrauensverhältnisses der Apotheker zu ihren Kundinnen und Kunden. Um den bei den Rechenzentren als Auftragsdatenverarbeitern vorhandenen Datenschatz dennoch ökonomisch verwerten zu können, wurde ihnen im SGB V die Erlaubnis zugestanden, nach Anonymisierung der Daten diese weiterzugeben. Empfänger sind medizinische Informationsdienstleister, die mit ihren Auswertungen insbesondere die Pharmaindustrie, aber auch z. B. die Politik versorgen.

Über Jahre hinweg erfolgte durch die Rechenzentren vor der Datenweitergabe keine wirksame Anonymisierung. Vielmehr wurden die den Patienten identifizierenden Daten durch ein eindeutiges sogenanntes Patientenanonym ersetzt, über das die Verschreibungen zu einer Person zusammengefügt werden können. So wissen die Datenempfänger zwar nicht, wie der Patient heißt, doch können sie dessen Krankheitsgeschichte anhand der Verschreibungen präzise zuordnen und nach-

vollziehen. Es ist offensichtlich, dass damit keine Anonymisierung, sondern eine Pseudonymisierung erfolgt. Zumindest theoretisch ist es möglich, das Patientenanonym wieder zu reidentifizieren, etwa indem die Identifizierungsdaten mit demselben Verfahren umgewandelt und dann das erhaltene Pseudonym den vorhandenen Datensätzen zugeordnet wird oder indem bekannte Verschreibungsdaten zu einer Person mit den unter dem Patientenanonym abgelegten Daten abgeglichen werden.

Was damit offensichtlich ist, war und ist Rechenzentren und Datenempfängern nicht ersichtlich. Sie behaupten, eine Reidentifizierung sei dadurch ausgeschlossen, dass das Verfahren der Berechnung des Patientenanonyms nur wenigen Geheimnisträgern bekannt sei. Eine Reidentifizierung anhand der Verschreibungsmerkmale sei praktisch ausgeschlossen, da die Datenempfänger keinen Zugang zu solchen Merkmalen hätten. Während die Mehrheit der Datenschutzbehörden in Deutschland dieser Argumentation nicht folgte, wurde sie von zwei Stellen akzeptiert. Während ein Rechenzentrum seine Praxis der „Anonymisierung“ umstellte, praktizieren andere den Handel mit „patientenanonymisierten“ Rezeptdatensätzen weiter (Tz. 1.5).

Unabhängig von der umstrittenen Frage, wann von einer gesetzeskonformen Anonymisierung ausgegangen werden kann, ist diese Praxis eine große Gefahr für das Patientengeheimnis: Medizinische Informationsdienstleister, also Datenbroker, beschaffen sich nicht nur von Apothekenrechenzentren Patientendaten, sondern auch über informationstechnische Dienstleister, also Hard- und Softwareanbieter, und von Ärzten und Apotheken über das sogenannte Ärzte- und Apothekenpanel, z. B. gegen Preisnachlässe bei Datenverarbeitungsdienstleistungen. Apotheken in Schleswig-Holstein legten dem ULD entsprechende Angebote von Unternehmen vor. Es ist nicht auszuschließen, dass die Datenbroker die Daten aus den verschiedenen Quellen zusammenführen. Das ULD hat das Unternehmen sowie die zuständige Datenschutzaufsichtsbehörde diesbezüglich schon im Sommer 2013 um Aufklärung gebeten. Belastbare Erkenntnisse liegen bisher nicht vor.

Was ist zu tun?

Die Verarbeitung pseudonymisierter Medizindaten sollte umfassend aufgeklärt und einer rechtmäßigen Praxis zugeführt werden.

4.6.9 Kooperation von Hautarzt und Kosmetikinstitut

Eine Kooperation zwischen einem Hautarzt und einem Kosmetikinstitut scheint naheliegend. Manche dermatologische Erkrankung kann nur kosmetisch behandelt werden. Da erscheint es auf den ersten Blick sinnvoll, wenn ein Hautarzt und ein Kosmetikinstitut ein gemeinsames EDV-System nutzen, mit dem sie Patientendaten abgleichen und Termine planen. Eine solche Zusammenarbeit ist in Schleswig-Holstein nur erlaubt, wenn die Patientinnen und Patienten zuvor umfassend aufgeklärt werden und alle eine informierte Einwilligung unterzeichnet haben. Auch wenn viele Betroffene die Kooperation wünschen, muss dies nicht für alle gelten. Nicht alle Hautarztpatienten benötigen eine kosmetische Behandlung; manche möchten ihr Kosmetikinstitut selbst auswählen. Patientengeheimnis und Datenschutzrecht fordern – bei aller freundschaftlichen Kooperation – eine klare Trennung der Datenbestände.

Was ist zu tun?

Kooperieren Hautarztpraxen und Kosmetikinstitute, dürfen Patientendaten nur mit informierter Einwilligung übermittelt werden. Bei einer gemeinsamen Datenverarbeitung müssen die Zugriffsrechte klar definiert und die Datenbestände technisch getrennt sein.

4.6.10 Polizeianfragen in Kliniken zu Unfallopfern, Vermissten oder Straftätern

Beim ULD häuften sich Beratungsersuchen, inwieweit und unter welchen Voraussetzungen Kliniken auf Anfrage der Polizei Auskünfte über Patientinnen oder Patienten geben dürfen, möglicherweise sogar mit Angaben zu bestimmten Verletzungen. Derartige Anfragen wurden zumeist von den Kliniken zurückgewiesen. Das war ganz überwiegend korrekt. Bereits die bloße Information, dass eine Person Patient ist oder nicht, unterliegt der Schweigepflicht; eine Offenbarung wäre eine Straftat. Eine begrenzte und bei Kliniken bisher kaum bekannte Ausnahmeregelung findet sich im Melderecht. Vergleichbar mit Hotels müssen Kliniken und Heime ein Verzeichnis aller stationär aufgenommenen Personen führen und daraus gegenüber Ordnungsbehörden Auskunft erteilen. Diese beschränkt sich auf die Identität der Patienten sowie den Tag der Aufnahme und der Entlassung. Keinesfalls ist es zulässig, Personen über Angaben zur Gesundheit zu suchen, beispielsweise nach einer Person mit einer Schussverletzung. Im Dialog zwischen Vertretern der Polizei und Klinik-Datenschutzbeauftragten wurde unter Mitwirkung des ULD ein Text entworfen, in dem Voraussetzungen und Grenzen des Auskunftsanspruchs dargestellt werden. Die Position des ULD ist im Netz abrufbar.

https://www.datenschutzzentrum.de/artikel/46-.html

4.7 Wissenschaft und Bildung

4.7.1 WLAN in der Schule – vor dem Vergnügen kommt die Arbeit

Wenn Schulen beim Unterricht zunehmend Informationstechnik (IT) einsetzen, bleibt der Datenschutz oft leider außen vor. Vor einigen Jahren dominierten in den meisten Schulen Computerräume, in denen die Schülerinnen und Schüler unterrichtet wurden. In immer mehr Schulen gibt es jetzt WLAN-Architekturen, sodass die Computernutzung im Unterricht nicht auf bestimmte Räumlichkeiten konzentriert werden muss.

Vor dem Einsatz dieser Technik muss darüber nachgedacht werden, welche Regeln des Schulrechts, des Datenschutzes und der technischen Gestaltung zu beachten sind. Inhalt und Umfang solcher Regelungen sind von der einzusetzenden WLAN-Architektur abhängig. Setzt eine Schule schuleigene Geräte ein, die sich mit dem schuleigenen WLAN verbinden, kann sie technisch genau festlegen, in welcher Weise die Kommunikation mit dem Internet erfolgt; detaillierte organisatorische und technische Vorkehrungen sind möglich. In Schulen, in denen Schülerinnen und Schüler ihre eigenen Geräte – Notebooks, Tablets oder Smartphones – für unterrichtliche Zwecke nutzen dürfen – Stichwort „Bring Your Own Device“ – und sich darüber mit dem schuleigenen WLAN verbinden, müssen wesentlich weiter gehende technische Maßnahmen getroffen werden, um Missbrauch zu verhindern. Die nötigen organisatorischen und technischen Vorgaben zur WLAN-Nutzung sind dann umfassender.

Folgendes wird vom ULD empfohlen: Vor Inbetriebnahme einer WLAN-Architektur muss die Schulleitung eine Nutzungsordnung erstellen, die eindeutige Nutzungsvorgaben festlegt. Das WLAN sollte nur für schulische Zwecke zur Verfügung gestellt werden. Jedes Gerät mit Zugang zum

WLAN ist zu registrieren. Die Aktivitäten, die über das WLAN im Internet stattfinden, müssen protokolliert werden, um bei Missbrauchsverdacht den Verursacher feststellen zu können.

Für die Internetnutzung an Schulen, insbesondere für die Nutzung von schuleigenen WLAN-Architekturen, hat das Bildungsministerium im Jahr 2013 entsprechende Hinweise, die mit dem ULD abgestimmt worden sind, veröffentlicht. Darüber hinaus hat das Institut für Qualitätsentwicklung an Schulen Schleswig-Holstein (IQSH) IT-Ausstattungsempfehlungen für Schulen in Schleswig-Holstein zur Internetnutzung herausgegeben. Für die datenschutzrechtlichen Fragestellungen, insbesondere auch bezüglich der Datensicherheit von WLAN-Architekturen, steht das ULD den Schulen zur Beratung zur Verfügung.

http://www.schleswig-holstein.de/Bildung/DE/Zielgruppen/LehrerinnenLehrer/InternetNutzung/internetnutzung_node.html

http://www.schleswig-holstein.de/Bildung/DE/Service/Broschueren/Bildung/ItAusstattung__blob=publicationFile.pdf

Was ist zu tun?

Die Einrichtung von WLAN-Architekturen und deren Nutzung für schulische Zwecke ist sorgfältig vorzubereiten.

4.7.2 Einheitliche Schulverwaltungssoftware ist wünschenswert

Die Anforderungen an Schulverwaltungsprogramme sind in den letzten Jahren gestiegen. Wurden mit diesen Produkten zunächst lediglich die Daten der Schülerinnen und Schüler gespeichert und damit der Schulalltag organisiert, so sollen sie heute komplexe Verwaltungs- und Kommunikationsprozesse ermöglichen. Es geht nicht nur darum, Daten für die jährliche Schulstatistik schnell und korrekt zusammenzustellen und auf sicherem Weg über das Landesnetz dem Statistischen Amt zur Verfügung zu stellen. Schulverwaltungssoftware soll auch Daten für die offene Ganztagsschule, für Mensasysteme oder vom Schulträger gewünschte Informationen möglichst auf Knopfdruck zur Verfügung stellen. Die Daten müssen dabei valide sein. Zu achten ist aber auch auf die datenschutzrechtlichen Vorschriften.

Unterschiedlichste Produkte verschiedener Hersteller sind in den Schulen im Einsatz. Lediglich bei den berufsbildenden Schulen wird das Programm eines Herstellers genutzt. Die Datenschutzkonformität der Schulverwaltungsprogramme ist unterschiedlich. Lediglich ein Produkt, welches in vielen Schulen im Einsatz ist, verfügt über ein Datenschutz-Gütesiegel. Das ULD unterstützt die Forderung des Landesrechnungshofes nach der Einführung einer einheitlichen Schulverwaltungssoftware für alle Schulen Schleswig-Holsteins. Geht es dem Landesrechnungshof dabei vorrangig um Aspekte der Wirtschaftlichkeit, so sieht das ULD hierin die Chance, das Verfahren rundum datenschutzkonform auszugestalten. Das ULD hat sich sofort zur aktiven Teilnahme an den Planungen zur Einführung einer einheitlichen Schulverwaltungssoftware bereit erklärt.

4.7.3 Lernplattformen – Vorteile, Risiken und Nebenwirkungen

Das ULD fordert schon seit Langem, dass das Bildungsministerium Regelungen für den Einsatz elektronischer Lernplattformen trifft (33. TB, Tz. 4.7.2). Leider ist dies bis heute nicht geschehen. Im Rahmen einer umfangreichen datenschutzrechtlichen Beratung eines Schulträgers bei der Einführung einer Lern- und Kommunikationsplattform hat das ULD weitere Erkenntnisse gewonnen, die die Notwendigkeit von klaren Rahmenbedingungen vollumfänglich bestätigen.

Die Datenschutzfragen bei der begutachteten Lern- und Kommunikationsplattform erwiesen sich als hoch komplex. Das ULD steht selbstverständlich Schulleitungen im Einzelfall im Interesse einer datenschutzkonformen Einführung von Lernplattformen beratend zur Seite. Zumindest die Rahmenbedingungen sollten aber vom Ministerium verbindlich für alle Schulen in Schleswig-Holstein vorgegeben werden. Es ist ausdrücklich festzulegen, dass solche Verfahren nicht zur Bearbeitung personenbezogener Daten für Schulverwaltungszwecke eingesetzt werden. Die Erreichbarkeit über das Internet macht solche EDV-Anwendungen attraktiv für die Speicherung von personenbezogenen Schülerdaten, die Lehrkräfte sonst in der Regel auf ihren häuslichen privaten EDV-Geräten speichern. Die Datenschutzverordnung Schule fordert jedoch eine strikte Trennung zwischen Schulverwaltungs-EDV und pädagogischen Netzwerken, zu denen auch solche Lern- und Kommunikationsplattformen gehören. Notenlisten, Klassenlisten oder andere Informationen, die Lehrkräfte für ihre Arbeit benötigen, dienen Schulverwaltungszwecken und haben in Lern- und Kommunikationsplattformen nichts verloren.

Was ist zu tun?

Das Bildungsministerium sollte verbindliche Rahmenbedingungen für den Einsatz von Lern- und Kommunikationsplattformen festlegen.

4.7.4 Schuldaten in der Cloud

Schulen nutzten für unterrichtliche Zwecke sogenannte Cloud-Dienste verschiedener Anbieter. Die Erkenntnisse aus den Enthüllungen von Edward Snowden veranlassten das Bildungsministerium – unterstützt vom ULD – im Jahr 2013, den Schulen die Nutzung solcher Cloud-Dienste für unterrichtliche Zwecke generell zu untersagen. Das ULD stellte jedoch fest, dass Lehrkräfte Cloud-Dienste, z. B. Dropbox, auch nutzen, um dienstlich personenbezogene Daten von Schülerinnen und Schülern mit anderen Lehrkräften auszutauschen. Selbst in Bearbeitung befindliche sonderpädagogische Gutachten mit besonders schützenswerten Angaben zu medizinischen Befunden und Behinderungen werden mittels Cloud-Diensten ausgetauscht und bearbeitet. Diese Vorgehensweise stellt einen erheblichen Verstoß gegen datenschutzrechtliche Vorschriften dar. Ebenso inakzeptabel ist im Grundsatz die Nutzung von Cloud-Diensten für unterrichtliche Zwecke, etwa zum Austausch von Unterrichtsmaterial zwischen Lehrkräften und Schülerinnen und Schülern.

Rechtlich ist die Cloud-Nutzung eine Datenverarbeitung im Auftrag, die unter Bedingungen gemäß dem Landesdatenschutzgesetz zulässig sein kann. Die Entscheidungshoheit über das Ob und das Wie muss aber beim Auftraggeber – hier also der Schule – liegen. Anbieter von Cloud-Diensten legen aber in der Regel Geschäftsbedingungen fest, die diesen Anforderungen nicht genügen. So hat der Auftraggeber in der Regel keinen Einfluss auf den Ort der physikalischen Speicherung seiner Daten. Er ist auch nicht in der Lage, die ordnungsgemäße Datenverarbeitung zu kontrollieren.

Allerdings ist anzuerkennen, dass die Kommunikation und der Austausch personenbezogener Daten der Schülerinnen und Schüler zwischen Lehrkräften untereinander oder mit der Schulverwaltung über internetbasierte Cloud-Dienste zu einer Arbeitserleichterung führen kann. Die Nutzung solcher Dienste für unterrichtliche Zwecke, etwa in Form einer Lern- und Kommunikationsplattform (Tz. 4.7.3), vereinfacht die Kommunikation und bringt möglicherweise einen Mehrwert für den Unterricht. Deshalb arbeiten das Bildungsministerium, das IQSH und das ULD an datenschutzkonformen Lösungen für Cloud-Dienste für Zwecke der Schulverwaltung und des Unterrichts.

Das ULD hat eine Änderung des Schulgesetzes vorgeschlagen, um die datenschutzkonforme Verarbeitung personenbezogener Daten von Schülerinnen, Schülern und Eltern auf Geräten zu ermöglichen, die nicht dem Schulträger gehören. Dies wurde anlässlich der Novellierung des Schulgesetzes im Jahr 2014 umgesetzt. Damit öffnet sich der Weg für eine Datenverarbeitung auch außerhalb des Landesnetzes. Externen Dienst-

leistern kann nun auch die Auftragsdatenverarbeitung von Teilen der Schulverwaltung übertragen werden. Lehrkräfte können hierüber aus dem häuslichen Bereich auf Schulverwaltungsdaten zugreifen. Die Einführung und Nutzung z. B. eines elektronischen Klassenbuches ist nun rechtskonform machbar, vorausgesetzt, die Kontrolle über die Schuldaten wird bewahrt. Das ULD begleitet intensiv einen entsprechenden Pilotversuch. Auch die Nutzung einer vom IQSH favorisierten internetbasierten Kommunikationsplattform für Lehrkräfte ist nun grundsätzlich möglich. Um sicherzustellen, dass die Nutzung solcher Dienste datenschutzkonform erfolgt, enthält das neu gefasste Schulgesetz einen Genehmigungsvorbehalt für die Auftragsdatenverarbeitung.

Was ist zu tun?

Das Bildungsministerium sollte den gesetzlichen Genehmigungsvorbehalt als Steuerungsinstrument nutzen, um die Zwecke und den Umfang des zulässigen Cloud-Einsatzes einheitlich festzulegen.

4.7.5 Dienstliche E-Mail-Adressen für Lehrkräfte

Lehrkräfte kommunizieren seit Jahren mit Schülerinnen, Schülern und Eltern aus dem häuslichen Bereich heraus mit privaten E-Mail-Adressen. Diese dienstliche Kommunikation über private E-Mail-Adressen hat sich etabliert, ohne dass Schulleitungen oder das Bildungsministerium diesen Kommunikationsweg zugelassen oder irgendwie reglementiert haben. Sie wird schweigend hingenommen – trotz datenschutzrechtlicher Risiken.

E-Mail-Kommunikation der Lehrkräfte mit ihren Schülerinnen und Schülern und gegebenenfalls den Eltern ist heute ein wichtiges Instrument zum schulischen Informationsaustausch. Wenn die Lehrkräfte aus ihrem häuslichen Bereich heraus aus schulischen Gründen elektronischen Kontakt herstellen, erfolgt dies im Kontext mit ihrer dienstlichen Aufgabenwahrnehmung. Sie vertreten mit ihrer E-Mail-Kommunikation ihre Schule nach außen. Dies muss für die Empfänger auch in der Absenderadresse erkennbar sein. Wenn Lehrkräfte mit teilweise pseudonymen E-Mail-Adressen über unterschiedlichste E-Mail-Provider kommunizieren, verliert sich der „amtliche“ Charakter. Die Schulverwaltungen kommunizieren mit Landesnetzadressen, sodass die Empfänger eindeutig feststellen können, mit welcher Schule sie es zu tun haben. Bei Lehrkräften ist dies nicht ohne Weiteres möglich. Zudem können die Schulleitungen im Bedarfsfall nicht prüfen, welche personenbezogenen Daten im Zusammenhang mit der E-Mail-Kommunikation verarbeitet werden.

Die Fragestellung rückte für das ULD in den Fokus, als eine ehemalige Lehrerin – oder besser, eine Lehrkraft im Ruhestand – vor der Bundestagswahl 2013 per E-Mail-Verteiler Wahlwerbung verschickte. Die E-Mail-Adressen von Schülerinnen, Schülern, anderen Lehrkräften und auch Eltern stammten aus dem privaten E-Mail-Account der Lehrkraft. Der Vorfall war für das ULD Anlass, die Notwendigkeit der Vergabe dienstlicher E-Mail-Adressen für Lehrkräfte aus Datenschutzsicht gegenüber dem Bildungsministerium und der zentralen IT des Landes deutlich zu machen.

Allen Lehrkräften sollte eine dienstliche E-Mail-Adresse zur Verfügung gestellt werden. Die Erreichbarkeit sollte auch im häuslichen Bereich gewährleistet werden. Im Interesse des Datenschutzes sollten einheitliche Vorgaben etwa in Bezug auf Speicherungsdauer und Nutzungsumfang gemacht werden. Im Bedarfsfall sollten die Schulleitungen, die oberen und obersten Fachaufsichtsbehörden sowie das ULD die Einhaltung dieser Vorgaben überprüfen.

Was ist zu tun?

Die Bereitstellung von dienstlichen E-Mail-Adressen für Lehrkräfte sollte umgehend auf ihre Realisierbarkeit hin geprüft und dann umgesetzt werden.

4.7.6 Wenn die Lehrkraft eigentlich nur Taschenrechner bestellen will

Im Mathematikunterricht sollen die Schülerinnen und Schüler in den Schulen möglichst mit einheitlichen Taschenrechnermodellen arbeiten. Da diese Taschenrechner von den Eltern selbst bezahlt werden müssen, hat sich in vielen Schulen die Praxis herausgebildet, dass sie per Sammelbestellung beschafft werden. Lieferfirmen gewähren dann gerne Rabatte. Üblicherweise fällt die Aufgabe des Kontakts mit der Firma den Lehrkräften zu. In diesem Zusammenhang wurden von diesen häufig auch personenbezogene Daten der Schülerinnen und Schüler an die Firma übermittelt.

Die Zulässigkeit dieser Datenübermittlungen wurde zuerst von einem Rundfunksender hinterfragt und beschäftigte danach auch den Landtag. Das ULD schrieb eine größere Anzahl von Schulleitungen an und fragte nach der dortigen Praxis. Die Antworten der Schulen zeigten, dass die Bestellungen tatsächlich üblicherweise von Lehrkräften vorgenommen werden. Die Schulleitungen hatten für das Prozedere keinerlei Regelungen getroffen, auch nicht wenn dabei Schülerdaten übermittelt wurden.

Das Schulgesetz sieht bei der Übermittlung personenbezogener Daten an private Stellen explizit die schriftliche Einwilligung der Eltern vor. In fast keinem Fall war eine solche Einwilligung tatsächlich vorher eingeholt worden. In den seltensten Fällen erfolgte die Bestellung in schriftlicher Form mit Briefkopf der Schule; meist erfolgte die Abwicklung durch die Lehrkräfte über deren private E-Mail-Accounts.

Nach Auswertung der Antworten empfahl das ULD dem Bildungsministerium, den Schulen Hinweise zu geben, wie sie bei Datenübermittlungen an andere Stellen vorzugehen haben. Der Vorgang bestätigt anschaulich die Notwendigkeit der Beratung und Weiterbildung der Schulleiterinnen und Schulleiter, wie der Datenschutz innerhalb der Schule optimiert werden kann.

4.7.7 Medienkompetenzvermittlung

Um Schülerinnen und Schüler, Eltern und Lehrkräfte für Datenschutzfragen im Internet und in der realen Welt zu sensibilisieren, arbeitet das ULD mit der Polizei, Verbraucherschützern und (Medien-)Pädagogen zusammen.

Beim ULD-Beitrag bei Medienkompetenztagen an Schulen, die vom IQSH organisiert werden, liegt ein Schwerpunkt in der Vermittlung der Risiken, die sich bei der Nutzung von sozialen Netzwerken und neuen Kommunikationsformen wie WhatsApp ergeben. Zielgruppe waren insbesondere 7. und 8. Klassen. Die Schülerinnen und Schüler werden jeweils in die Präsentationen einbezogen.

Ein weiterer Schwerpunkt liegt in der Information der Lehrkräfte als Multiplikatoren. Als heikel erweist sich oft die digitale Kommunikation zwischen Lehrern und einzelnen Schülern. Auf Elternabenden zeigte sich, dass oft wenig Sensibilität hinsichtlich der Datenschutzrisiken besteht, die sich bei der Nutzung von Smartphones und bei sonstigen Internetaktivitäten ergeben. Hinsichtlich ihrer Einwirkungsmöglichkeiten auf ihre Kinder sind Eltern oft stark verunsichert. Bei Jugendlichen wandeln sich das Kommunikationsverhalten und die Nutzung etwa von bestimmten Apps oft schnell und stark, weshalb die aktuellen Entwicklungen dauernd im Blick bleiben müssen.

Was ist zu tun?

Eltern, Schüler- und Lehrerschaft sind weiterhin über den Datenschutz im und außerhalb des Internets zu informieren.

4.8 Steuerverwaltung

4.8.1 Einsicht in Steuerakten durch Insolvenzverwalter

Die Frage der Einsicht in Steuerakten bleibt aktuell (34. TB, Tz. 12.4). Eine besondere Note erhält die Frage, wenn ein Insolvenzverwalter in die Steuerakte einer Insolvenzschuldnerin Einsicht nehmen will. Insolvenzverwalter haben gegenüber Gläubigern den Anspruch auf Rückzahlung bereits erfüllter Verbindlichkeiten, um die Insolvenzmasse zur gleichmäßigen Befriedigung aller Gläubiger anzureichern. Die Steuerbehörden sind attraktives Ziel für Anfechtungen. Sie erfahren oft frühzeitig über Zahlungsschwierigkeiten, dürfen selbst Vollstreckungstitel erstellen und können so rechtzeitig vor der Insolvenz Steuerforderungen vollstrecken. Dürfte das Finanzamt die Auskunft über bereits gezahlte Steuern gegenüber dem Insolvenzverwalter verweigern, würden diese Einnahmen unter Verletzung der Gleichbehandlung der Gläubiger oftmals dem Fiskus verbleiben. Eine Ausnahme vom Auskunftsanspruch nach dem Informationszugangsgesetz (IZG), wie sie in anderen Bundesländern besteht, ist im IZG nicht enthalten und kann vom ULD nicht befürwortet werden. Das IZG besteht unabhängig von den Regelungen der AO. Der Schutz des Fiskus vor Insolvenzanfechtungen ist ein durchaus nachvollziehbares Anliegen. Über das Informationszugangsrecht wird mit Landesrecht in das Regelungsgefüge des Insolvenzrechts eingegriffen. Die Frage sollte nach Auffassung des ULD einheitlich im Insolvenzrecht geregelt werden.

Das VG Schleswig entschied, wie zuvor schon andere Gerichte, im Oktober 2014, dass die Regelungen der Abgabenordnung das IZG nicht verdrängen, sondern nebeneinander anzuwenden sind. Der vom Bundesfinanzministerium ergangene Anwendungserlass zur Abgabenordnung aus dem Jahr 1998 ist lediglich eine Handreichung zur Ermessensausübung nach der Abgabenordnung und hat keinen Einfluss auf Ansprüche nach dem IZG. Das Urteil ist noch nicht rechtskräftig.

Was ist zu tun?

Finanzämter haben nach dem IZG beantragte Auskünfte zu erteilen, sofern keine spezifischen Ausschlussgründe des IZG dagegensprechen.

4.8.2 Druckaufträge in Steuersachen – nicht bei privaten Dritten

Der Versand von Unterlagen in Besteuerungsverfahren ist ein Massengeschäft. Der Wunsch, Druck, Kuvertieren und Versand auszulagern, ist nachvollziehbar. Entsprechende Angebote für hybride Versandmethoden sind auf dem Markt vorhanden. Diese können aber bei Steuerangelegenheiten nicht genutzt werden. Im Bereich des Steuerwesens gilt aufgrund des Steuergeheim-

nisses ein besonderer Vertrauensschutz. Für die elektronische Kommunikation im Steuerverfahren ist eine durchgängige Verschlüsselung von Mitteilungen der Finanzbehörden vorgesehen. Bei hybriden Versandverfahren mit Druck durch Dritte müssen zumindest für den Druckvorgang die Daten entschlüsselt werden. Die Daten genießen nicht mehr den hohen Schutz des Telekommunikationsgesetzes, dem sie während der digitalen Übermittlung unterliegen; der Geheimnisschutz des Postgesetzes beginnt erst mit dem Einsammeln der Briefe, also nach Druck und Kuvertieren. Der Druck darf auch nicht im Rahmen einer Auftragsdatenverarbeitung erfolgen, weil mit der Verarbeitung von Daten, die dem Steuergeheimnis unterliegen, nur öffentliche Stellen betraut werden dürfen.

Damit fehlt es an einer Rechtsgrundlage zur Übermittlung und Offenbarung von Steuergeheimnissen bei hybriden Versandverfahren. Eine gesetzgeberische Regelung, dass das temporäre Entschlüsseln rechtlich unschädlich sei, fehlt für hybride Verfahren. Eine solche Klarstellung durch den Gesetzgeber ist in Kenntnis des konkreten Regelungsbedarfs ausgeblieben.

Was ist zu tun?

Auf externe Anbieter darf für Druck und Versand von Unterlagen in Steuerangelegenheiten nicht zurückgegriffen werden.

4.8.3 Die nacheheliche Indiskretion des Finanzamtes

Ein Petent wurde vor mehreren Jahren von seiner Frau geschieden und hatte dies mehrfach den Finanzbehörden mitgeteilt. Dies hinderte das zuständige Finanzamt nicht, auch der geschiedenen Ehefrau Mitteilungen über die Eigenheimzulage ihres Ex zu machen. Es zeigte sich, dass die automatische Versendung des Schreibens anlässlich eines Zuständigkeitswechsels der Finanzämter auf einem Programmfehler beruhte. Die mitgeteilte Steuernummer galt noch für die Ehezeiten und war nicht mehr aktiv. Das Finanzamt sicherte zu, das Problem zu lösen, sodass künftig keine Schreiben mehr an die Ehefrau gehen. Nach der Scheidung werden neue Steuernummern vergeben, womit verhindert werden soll, dass Informationen dem jeweils anderen bekannt werden.

05

KERNPUNKTE

Verbraucherdatenschutz

Geodaten

Videoüberwachung

5 Datenschutz in der Privatwirtschaft

Die gemäß dem Bundesdatenschutzgesetz im nicht öffentlichen Bereich tätigen Aufsichtsbehörden kooperieren seit 1977 im „Düsseldorfer Kreis". Immer mehr Datenschutzbeauftragte der Länder wurden zugleich Aufsichtsbehörden. Nur in Bayern blieb die Datenschutzaufsicht zweigeteilt. Es liegt nahe, innerhalb der Dienststellen nicht mehr streng zwischen öffentlichem und nicht öffentlichem Bereich zu trennen. Um auch auf Bundesebene Synergien zu erreichen, wurde der Düsseldorfer Kreis in die Strukturen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder integriert. Das Bayerische Landesamt für Datenschutzaufsicht nimmt seitdem an der Konferenz teil.

5.1 Datenschutz in der Versicherungswirtschaft

Im Düsseldorfer Kreis bestehen zu einzelnen Wirtschaftsbereichen Arbeitsgruppen, die von einer Aufsichtsbehörde geleitet werden; das ULD nimmt die Leitung der AG Versicherungswirtschaft wahr.

5.1.1 Warndatei – auch für private Krankenversicherungen

Das Hinweis- und Informationssystem der Versicherungswirtschaft (HIS) wurde nach langer Diskussion mit dem ULD und den anderen Aufsichtsbehörden im April 2011 in Betrieb genommen. Seitdem speichert und verarbeitet es Daten von Personen zu Zwecken der Risikoprüfung für die teilnehmenden Versicherungsunternehmen (34. TB, Tz. 5.1.1).

Die privaten Krankenversicherungen sind bisher nicht in das HIS integriert, sondern betreiben seit Jahrzehnten ein papier- bzw. faxbasiertes System zur Betrugsbekämpfung, die sogenannte Versicherungsumfrage. Im Rahmen dieses Systems senden einzelne private Krankenversicherer einen Datensatz als Anfrage an den Verband der Privaten Krankenversicherung (PKV e. V.). Dieser sammelt die Anfragen und schickt sie an die Mitgliedsunternehmen. Stellt ein Mitgliedsunternehmen eine Personenidentität mit einem Meldefall über Auffälligkeiten oder Risiken fest, nimmt es Kontakt mit dem einmeldenden Unternehmen auf.

Dieses System ist mit geltendem Datenschutzrecht nicht vereinbar, da keine wirksamen Einwilligungen der Betroffenen eingeholt werden, eine Vorratsübermittlung an die anderen Unternehmen erfolgt und keine klaren Kriterien für die Meldungen und die Rückmeldungen gelten.

Das bisher praktizierte System der Versicherungsumfrage ist rechtswidrig und soll ersetzt werden. Geplant wird die Anbindung der privaten Krankenkassen an das HIS.

Zwecks Beendigung des rechtswidrigen Verfahrens wird derzeit die Anbindung der privaten Krankenkassen an das HIS geprüft. Dazu finden seit 2013 konkrete Gespräche zwischen Vertretern der AG Versicherungswirtschaft und Vertretern der privaten Krankenkassen statt. Ziel der Prüfung ist es, das Interesse der betroffenen Versicherten und Versicherungsnehmer an der Wahrung ihres Rechts auf informationelle Selbstbestimmung mit dem Interesse der privaten Krankenversicherungen an einem geeigneten System zur Erkennung von betrügerischem Verhalten zusammenzubringen. Dazu hat der PKV e. V. Kategorien von Auffälligkeiten formuliert, mit denen Meldefälle beschrieben werden. Anknüpfungspunkte sind folgende Sachverhalte:

- Verletzung vorvertraglicher Informationspflichten,
- Verletzung von Meldepflichten des Versicherungsnehmers,
- betrügerische Inanspruchnahme von Leistungen der Versicherung.

Die Konkretisierung dieser Kategorien wird derzeit von der AG Versicherungswirtschaft geprüft. Es besteht die Gefahr, redliche Versicherungsnehmer und Versicherte vorschnell einzumelden. Kern der Prüfung ist deshalb die Abwägung, welche Merkmale ausreichend konkret sind, welches Maß an Verdacht erforderlich und wann eine Löschung der eingemeldeten Person vorzunehmen ist. An den übrigen datenschutzrechtlichen Vorgaben zum HIS, also insbesondere der strengen Erforderlichkeitsprüfung, der Protokollierungspflicht und der Informationspflicht gegenüber den Betroffenen, sollen keine Änderungen vorgenommen werden. Die Einbindung der privaten Krankenversicherungen wird vielmehr zum Anlass genommen, die vergangenen drei Jahre der Praxis mit dem HIS kritisch zu überprüfen.

Was ist zu tun?

Die Aufsichtsbehörden müssen prüfen, unter welchen datenschutzrechtlichen Voraussetzungen die privaten Krankenversicherungen Daten ihrer Versicherten und Versicherungsnehmer in das HIS einmelden können.

5.1.2 Kfz-Schadenklassendatei

Seit dem Jahr 2012 finden Gespräche mit dem Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV) über dessen geplante Einführung einer sogenannten Schadensklassendatei statt. Zweck einer solchen Datei ist die verbesserte Erkennung von missbräuchlichen Handlungen im Zusammenhang mit der Neuversicherung von Kraftfahrzeugen (Kfz). In gewissen Fallgestaltungen erfährt eine Kfz-Versicherung bei der Antragstellung zu einem Vertrag nicht, wo der Versicherungsnehmer zuvor versichert war. In diesen Fällen erhält ein Versicherungsnehmer die für ihn ungünstigste Einstufung für Neuverträge. Diese Einstufung ist in der Regel aber günstiger als diejenige, die bei seiner Einordnung in eine sogenannte Schadensklasse durch die Vorversicherung wegen Schadensfällen erfolgen würde.

Um zu verhindern, dass durch das Verschweigen der Vorversicherung eine versicherungsvertragliche Besserstellung erreicht wird, plant der GDV die Einführung einer Schadensklassendatei. Die Daten sollen das bestehende Verfahren zur Meldung von Schadensfreiheitsklassen ergänzen, das mit den Verhaltensregeln der Versicherungswirtschaft (Code of Conduct; 31. TB, Tz. 5.5.1) eingeführt wurde. Die AG Versicherungswirtschaft hat in einer Stellungnahme eine Anpassung des Code of Conduct sowie der Allgemeinen Bedingungen für die Kfz-Versicherung (AKB 2008) angeregt. Gefordert wird darin eine ausreichende Information der Betroffenen sowie die klare Bezeichnung der erfassten Daten, Verarbeitungszwecke und Datenempfänger.

Die Schadensklassendatei soll die existierende Übermittlung von Schadenfreiheitsklassen ergänzen und betrügerische Handlungen im Zusammenhang mit Kfz-Versicherungen bekämpfen.

5.1.3 BaFin-Rundschreiben zur Zusammenarbeit mit Versicherungsvermittlern

Das Rundschreiben der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) „Hinweise zur Zusammenarbeit mit Versicherungsvermittlern“ enthält Vorgaben zu den Prüfungspflichten von Versicherungsunternehmen, wenn diese mit Versicherungsmaklern und Vermittlern zusammenarbeiten. Aus Datenschutzsicht ist die Erhebung von Bonitätsauskünften oder die Einsichtnahme in Führungszeugnisse von großer Bedeutung.

Das Rundschreiben datiert in seiner aktuellen Fassung vom September 2007 und wird aktuell überarbeitet. Das ULD hat in Abstimmung mit der AG Versicherungswirtschaft eine Stellungnahme abgegeben und hat insbesondere auf folgende zwei Punkte hingewiesen:

- Soweit die Vorlage eines Führungszeugnisses verlangt wird, ist die bereits mit der BaFin abgesprochene Compliance-Regelung anzuwenden. Es muss sichergestellt werden, dass der Inhalt des Führungszeugnisses nur dem für die Zuverlässigkeitsprüfung zuständigen Personal zur Kenntnis gegeben wird. Nicht erforderliche Informationen dürfen nicht dauerhaft gespeichert werden, sondern sind unverzüglich zu löschen. Entsprechende Hinweise sollten in das Rundschreiben aufgenommen werden.
- Der aktuelle Entwurf enthält Hinweise zur Erforderlichkeit von Bonitätsabfragen über den Vermittler. Danach sollen Auskünfte von privaten Auskunfteien nicht mehr in jedem Fall genügen. Das ULD stellt infrage, inwiefern derartige Auskünfte überhaupt erforderlich sind. Es ist klarzustellen, in welchen Situationen auf private Auskunfteien zurückgegriffen wird. Zudem muss geklärt werden, wie unnötige Bagatellauskünfte unterhalb der für die Zuverlässigkeit relevanten Wertschwelle vermieden würden.

5.2 Verbraucherklagerecht bei Datenschutzverstößen

Nach dem Willen der Bundesregierung sollen künftig bestimmte qualifizierte Einrichtungen, wie etwa die Verbraucherzentralen, die gesetzliche Befugnis erhalten, gegen datenschutzrechtliche Verstöße im Wege einer gerichtlichen Unterlassungsklage vorzugehen. Unterlassungsklagen sind für entsprechende Einrichtungen nach bisheriger Gesetzeslage nur zulässig, wenn die allgemeinen Geschäftsbedingungen des jeweiligen Unternehmens Datenschutzvorschriften verletzen. Der Entwurf klärt die alte Streitfrage, ob gesetzliche Vorschriften des Datenschutzrechts verbraucherschützende Wirkung entfalten. Das ULD begrüßt den Gesetzentwurf sowie eine beabsichtigte Änderung, wonach neben den Unterlassungsanspruch auch ein Anspruch auf Beseitigung treten soll, um den bestehenden Störungszustand wirksam zu beenden.

Im Rahmen einer Anhörung hat das ULD folgenden Ergänzungsbedarf angemeldet:

- Sind Gegenstand einer Unterlassungsklage allgemeine Versicherungsbedingungen, welche der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zur Genehmigung vorzulegen sind, muss das Gericht die BaFin hierzu anhören. Zum gesetzlichen Aufgabenbereich der Datenschutzaufsichtsbehörden zählt zwar nicht die Genehmigung von entsprechenden Vertragswerken. Die Interessenlage ist aber vergleichbar, wenn mit den Vertragsbedingungen von Unternehmensseite aus Festlegungen zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten getroffen und so die Zuständigkeit der Datenschutzaufsichtsbehörden berührt werden. Das Gericht sollte sich dann im Rahmen einer Anhörung den Sachverstand der Datenschutzaufsichtsbehörden zunutze machen, was über eine gesetzliche Verpflichtung zur Anhörung sichergestellt werden kann.
- Unterlassungs- und Beseitigungsansprüche sollten nicht nur für Verstöße gegen materielle Datenschutzregelungen, sondern auch bei Verstößen gegen gesetzliche Vorgaben des technisch-organisatorischen Datenschutzes gelten. Auch in dieser Hinsicht sollten die Gerichte über eine gesetzlich verpflichtende Anhörung der Datenschutzaufsichtsbehörden deren besonderes Fachwissen nutzen.

Was ist zu tun?

Mit dem geplanten Gesetz wird ein großer Gewinn für den Datenschutz einhergehen, insbesondere wenn die ergänzenden Vorschläge des ULD berücksichtigt werden.

5.3 Ein „Code of Conduct" der Geoinformationswirtschaft?

Das ULD hat den Vorsitz der Unterarbeitsgruppe (UAG) Geodaten der Konferenz der Datenschutzbeauftragten des Bundes und der Länder inne. Die UAG Geodaten erörtert mit der 2004 gegründeten Kommission für Geoinformationswirtschaft des Bundesministeriums für Wirtschaft und Energie (GIW-Kommission) geplante Verhaltensregeln (Code of Conduct – CoC) für die Geoinformationswirtschaft.

In der GIW-Kommission sind über 20 Spitzenverbände der deutschen Wirtschaft vertreten, deren Mitgliedsunternehmen Geodaten für ihre wirtschaftliche Tätigkeit benötigen. Ziel der Geoinformationswirtschaft sowie des Vereins Selbstregulierung Informationswirtschaft e. V. (SRIW) ist die Anerkennung ihres CoC als Verhaltensregeln nach dem Bundesdatenschutzgesetz (BDSG). Durch Vorlage einer durch den CoC regulierten Selbstverpflichtungserklärung soll es Geodaten haltenden staatlichen Stellen erleichtert werden, über Informationsersuchen zu entscheiden. Mit den Selbstverpflichtungen soll bezüglich der Verarbeitung der Geodaten ein valides Datenschutzmanagement gewährleistet werden. Der CoC soll nach Billigung durch die Datenschutzaufsichtsbehörden vom zuständigen Berliner Beauftragten für den Datenschutz und die Informationsfreiheit gemäß dem BDSG anerkannt werden (34. TB, Tz. 4.1.3).

Vorangegangen sind der Unterstützung bei der Formulierung einer Selbsterklärung drei Studien, die das ULD im Auftrag der GIW-Kommission ausgeführt hat:

- „Datenschutz und Geoinformationen" (März 2007),
- „Datenschutzrechtliche Rahmenbedingungen für die Bereitstellung von Geodaten für die Wirtschaft – ‚Ampelstudie' " (Juli 2008),
- „Bereitstellung von Geodaten unter Berücksichtigung datenschutzrechtlicher Aspekte anhand des Datenclusters ‚Denkmalschutz' der öffentlichen Verwaltung für die Wirtschaft" (Mai 2010).

http://www.geobusiness.org

Geoinformationen können für die Wirtschaft von erheblicher Bedeutung sein. Der Nutzen der Daten ist vielfältig: Wirtschaftsunternehmen nutzen Geodaten zur Planung von Bedarfen und Angeboten. Neben zahlreichen sinnvollen Nutzungsmöglichkeiten bestehen aber auch solche mit kritischem Personenbezug. Vielfach werden Geodaten, z. B. der Aufenthaltsort, als Anknüpfungspunkt zur Anreicherung mit weiteren Informationen oder zur Kategorisierung nach Wohnung und Wohnungsumfeld sowie nach lokalisierten Angaben zum Eigentum und dessen Nutzung verwendet.

Artikel 3 Richtlinie 2007/2/EG des Europäischen Parlamentes und Rates vom 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE-Richtlinie)

Geodaten [sind] alle Daten mit direktem oder indirektem Bezug zu einem bestimmten Standort oder geografischen Gebiet […].

Derzeit wird der Personenbezug bei georeferenzierten Informationen noch uneinheitlich bewertet. Eine zentrale Frage für die Beteiligten ist: Wann wird in welcher Kombination welche Geoinformation zu einem datenschutzrechtlich relevanten Datum? Der GeoBusiness-CoC „Verhaltensregeln GeoBusiness und Datenschutz" soll Rahmenbedingungen für eine einheitliche und datenschutzkonforme Verarbeitung und Nutzung von Geodaten in Deutschland schaffen. Mit der Akkreditierung verpflichten sich die Teilnehmer freiwillig zum Einsatz eines Datenschutzmanagementsystems und technisch-organisatorischer Maßnahmen und tragen damit zur Erhöhung des Daten-

schutzniveaus bei. Die Verhaltensregeln und deren Erläuterungen sollen den Unternehmen zudem helfen, die bestehenden gesetzlichen Regelungen für den Bereich der personenbezogenen Geodaten umzusetzen.

Was ist zu tun?

Es ist sicherzustellen, dass die Selbstverpflichtung inhaltlich nicht hinter den gesetzlichen Vorgaben zurückbleibt und das Verfahren eine angemessene Prüfung und Kontrolle der Zusicherungen ermöglicht.

5.4 Orientierungshilfe „Selbstauskünfte von Mietinteressenten“

Das ULD hat eine Orientierungshilfe erarbeitet, die sich mit der Einholung von Selbstauskünften bei Mietinteressenten durch Vermieter befasst. Die Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich haben im Düsseldorfer Kreis der Orientierungshilfe zugestimmt.

Vor der Vermietung von Wohnraum erheben Vermieter bei den Mietinteressenten persönliche Angaben, auf deren Basis eine Entscheidung über den Vertragsabschluss getroffen wird. Der Vermieter darf nur solche Daten erheben, die zur Durchführung des Mietvertrags erforderlich sind und an denen er deshalb ein berechtigtes Interesse hat. Die Verwendung von Einwilligungserklärungen gegenüber Mietinteressenten in Formularen zur Selbstauskunft ist nicht das richtige Mittel zur Datenerhebung. Denn eine wirksame Einwilligung erfordert die Freiwilligkeit der Erklärung, setzt also ein Wahlrecht voraus, ob dem Vermieter die gewünschten Angaben zur Verfügung gestellt werden oder nicht. Diese Wahlfreiheit fehlt, wenn der Abschluss des Mietvertrags von der Erhebung bestimmter Angaben des Mietinteressenten abhängig gemacht wird, da in der dann bestehenden Drucksituation keine freiwillige Erklärung abgegeben wird.

Die Zulässigkeit einer Datenerhebung durch den Vermieter muss daher direkt an den gesetzlichen Anforderungen gemessen werden. Im Kern ist die Frage zu beantworten, ob ein konkretes Datum im jeweiligen Verfahrensstadium erforderlich ist. Es kann zwischen drei Zeitpunkten differenziert werden, nämlich dem Besichtigungstermin, der vorvertraglichen Phase, in welcher der Mietinteressent dem künftigen Vermieter mitteilt, eine bestimmte Wohnung anmieten zu wollen, und dem Stadium, in welchem die Entscheidung über den auszuwählenden Mietinteressenten fallen soll.

Im Rahmen des Besichtigungstermins gilt u. a. das Folgende:

- Angaben zur Identifikation (z. B. Name, Vorname und Anschrift) dürfen erfragt werden. Der Vermieter ist befugt, im Falle der Besichtigung allein die Angaben des Mietinteressenten durch Vorzeigen eines Personalausweises zu überprüfen und den Umstand der Überprüfung zu dokumentieren. Die Anfertigung einer Ausweiskopie ist nicht erforderlich und damit unzulässig.
- Die Erhebung von Angaben zum Wohnberechtigungsschein ist statthaft. Der künftige Vermieter darf eine Wohnung, die im Rahmen eines Programms zur sozialen Wohnraumförderung errichtet wurde, nur einem Wohnungssuchenden zum Gebrauch überlassen, wenn dieser ihm vorher seine Wohnberechtigung durch Übergabe eines Wohnberechtigungsscheins nachweist.
- Fragen des Vermieters nach dem beabsichtigten Einbringen von Haustieren sind zulässig, soweit die Tierhaltung nicht zum vertragsgemäßen Gebrauch der Mietsache zählt und folglich zustimmungsbedürftig ist. Entsprechende Fragen sind zulässig, soweit dies nicht Kleintiere betrifft (z. B. Zierfische, Mäuse, Hamster).

Ab der Erklärung des Mietinteressenten, eine bestimmte Wohnung anmieten zu wollen, gilt u. a. Folgendes:

- Angaben zum Familienstand des Mietinteressenten werden oft im Hinblick auf die gesamtschuldnerische Haftung von Ehegatten gefordert. Allein deshalb wird aber kein berechtigtes Vermieterinteresse be-

gründet, da Ehegatten nicht zwangsläufig gemeinsam Mietvertragsparteien sein müssen.

- Die Frage nach einem eröffneten Verbraucherinsolvenzverfahren ist zulässig, da den Mietinteressenten eine Offenbarungspflicht trifft. Das Insolvenzverfahren führt dazu, dass das gesamte pfändbare Vermögen zur Insolvenzmasse gehört und dem Mietinteressenten nur die nicht pfändbaren Vermögensteile zur Verfügung stehen.
- Fragen nach Räumungstiteln wegen Mietzinsrückständen sind dann zulässig, wenn diese aufgrund der zeitlichen Nähe noch Auskunft darüber geben können, ob künftige Mietzinsansprüche gefährdet wären. Dies kann der Fall sein, wenn bezüglich eines bestehenden Wohnraummietverhältnisses mit einem anderen Vermieter die Zwangsräumung wegen Mietzinsrückständen droht.
- Die Erhebung von Angaben zu Vorstrafen ist grundsätzlich nicht erforderlich und damit unzulässig. Gegen die Erhebung von Informationen zu laufenden strafrechtlichen Ermittlungsverfahren spricht schon die verfassungsrechtlich verankerte Unschuldsvermutung.
- Angaben zu Heiratsabsichten, bestehenden Schwangerschaften und zum Kinderwunsch zählen zum Kernbereich privater Lebensgestaltung. Fragen hierzu sind unzulässig.
- Es besteht keine Verpflichtung, über die Zugehörigkeit zu Parteien oder Mietervereinen Auskunft zu geben. Mit den Angaben wird zudem noch keine Aussage zur Bonität des Mietinteressenten bzw. zu dessen Zahlungsfähigkeit und Zahlungswilligkeit getroffen.
- Für die Entscheidung über den Abschluss eines Mietvertrags darf nach dem Beruf und dem Arbeitgeber als Kriterium zur Beurteilung der Bonität des Mietinteressenten gefragt werden. Die Dauer einer Beschäftigung bietet in einer mobilen Gesellschaft hingegen keine Gewissheit über die Fortdauer und Beständigkeit des Beschäftigungsverhältnisses und ist daher ungeeignet, das Sicherungsbedürfnis des Vermieters zu erfüllen. Fragen nach der Dauer der Beschäftigung sind damit unzulässig.

Ab der Entscheidung des Vermieters, mit einem bestimmten Mietinteressenten über Wohnraum einen Mietvertrag abzuschließen, gilt das Folgende:

- Der künftige Vermieter möchte nun mit dem einzigen Mietinteressenten für eine konkrete Wohnung einen Mietvertrag schließen. Haben sich zwei oder mehrere Mietinteressenten für eine konkrete Wohnung entschieden, so trifft der künftige Vermieter die Entscheidung für einen bestimmten Mietinteressenten (Erstplatzierten). Nach dieser Entscheidung kann die Einholung weiterer Informationen beim Erstplatzierten erforderlich sein.
- Nachweise zu den Einkommensverhältnissen dürfen erfragt werden.
- Der Vermieter fordert Informationen zu den wirtschaftlichen Verhältnissen des Mietinteressenten an, um dessen Zahlungsfähigkeit bezüglich des Mietzinses beurteilen zu können. Selbstauskünfte, die Mietinteressenten bei Auskunfteien, z. B. der Schufa, selbst einholen können, enthalten wesentlich mehr Angaben über deren wirtschaftliche Verhältnisse, als für eine solche Beurteilung erforderlich sind. Schon aus diesem Grund wäre die pauschale Forderung des künftigen Vermieters an den Mietinteressenten, eine solche Selbstauskunft vorzulegen, unzulässig.

Die Orientierungshilfe „Einholung von Selbstauskünften bei Mietinteressenten“ ist abrufbar unter:

http://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OH_SelbstauskunftMietinteressenten.pdf

Was ist zu tun?

Der Vermieter darf nur diejenigen Angaben vom Mietinteressenten erheben, die in der jeweiligen Verfahrensphase zwingend erforderlich sind. Formulare zur Selbstauskunft müssen den obigen Vorgaben genügen.

5.5 Orientierungshilfe „Cloud Computing 2.0“

Das ULD hat an einer erweiterten Fassung einer Orientierungshilfe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und des Düsseldorfer Kreises zum „Cloud Computing“ mitgewirkt. Das Papier wendet sich an öffentliche und nicht öffentliche Stellen und gibt Hinweise zur Handhabung einer Datenverarbeitung in der Cloud.

Cloud Computing beschreibt bekanntlich eine über Netze angeschlossene Rechnerlandschaft, in welche die eigene Datenverarbeitung ausgelagert wird. Es geht um eine Form der bedarfsgerechten und flexiblen Anwendung von IT-Dienstleistungen, indem diese in Echtzeit als Service über das Internet bereitgestellt werden. Die Abrechnung erfolgt zumeist nach dem Umfang der Nutzung.

Aus Datenschutzsicht ist von Bedeutung, welche Datenverarbeitungen zwischen den Beteiligten (Cloud-Anwender und Cloud-Anbieter) stattfinden, wer die datenschutzrechtliche Verantwortung trägt, wie die Rechte von betroffenen Bürgern und Bürgerinnen auf Auskunft, Löschung, Sperrung, Berichtigung, Benachrichtigung und Widerspruch gewahrt werden, wie eine Kontrolle der teilweise weltweit tätigen Auftragnehmer und Unterauftragnehmer erfolgt, welche technisch-organisatorischen Maßnahmen getroffen sind und welche Regeln bei grenzüberschreitendem Datenverkehr bestehen.

Die Orientierungshilfe „Cloud Computing 2.0“ knüpft an die Ausführungen der Vorgängerfassung (34. TB, Tz. 5.7) an und beleuchtet zusätzlich vor allem folgende Themenbereiche:

- Bei Nichteinhaltung der Datenschutzbestimmungen drohen dem Cloud-Anwender haftungsrechtliche Konsequenzen. Gegenüber den Betroffenen kann er zum Schadensersatz verpflichtet werden; gegen ihn können Bußgelder verhängt oder aufsichtsbehördliche Anordnungen verfügt werden. Bei unrechtmäßiger Kenntniserlangung von Daten entstehen Informationspflichten. Der Cloud-Anwender muss einen Mechanismus vorsehen, wonach Datenpannen, die gesetzliche Meldepflichten auslösen, unverzüglich der zuständigen Aufsichtsbehörde und den Betroffenen mitgeteilt werden.
- Sofern der Cloud-Anbieter seinen Sitz nicht in einem Drittstaat ohne angemessenes Datenschutzniveau hat, sondern vielmehr in der EU bzw. im EWR oder in einem Drittstaat mit angemessenem Datenschutzniveau, sind die Standardvertragsklauseln gemäß Kommissionsbeschluss 2010/87/EU für Auftragsdatenverarbeitung vom 05.02.2010 nicht direkt anwendbar. Die Vergabe von Unteraufträgen stellt die beteiligten Stellen in dieser Konstellation vor besondere Herausforderungen. Denn in dieser Konstellation ist die Vergabe von Unteraufträgen nicht durch den Hauptauftragsdatenverarbeiter (d. h. den Cloud-Anbieter) im eigenen Namen möglich, jedenfalls nicht im Wege einer genehmigungsfreien Lösung. Die Orientierungshilfe definiert die Voraussetzungen für die Einschaltung von Unteranbietern.
- US-Behörden, wie etwa das Federal Bureau of Investigation (FBI), die National Security Agency (NSA) oder die Central Intelligence Agency (CIA), sind auf der Grundlage von US-amerikanischem Recht ermächtigt, auf personenbezogene Daten in Europa zuzugreifen, was bezüglich einer Datenverarbeitung in der Cloud eine besondere Relevanz aufweist. Darüber hinaus wurde bekannt, dass staatliche Behörden in EU-Mitgliedstaaten, wie das Government Communications Headquarters (GCHQ – britischer Nachrichten- und Sicherheitsdienst) und die Direction Générale de la Sécurité Extérieure (DGSE – französischer Nachrichtendienst), umfassend und manchmal ohne jede Rechtsgrundlage auf personenbezogene Daten von EU-Bürgern, Verbindungs- wie Inhaltsdaten (Telekommunikationsverbindungsdaten, E-Mails, SMS, Chats) zugreifen. Entsprechende Maßnahmen verletzen europäisches Datenschutzrecht. Bei der Prüfung der Aufsichtsbehörden, ob ein Datentransfer in die USA den datensicherheitsrechtlichen Anforderungen entspricht, ist etwa von Bedeutung, ob der Cloud-Anbieter sowie die Unteranbieter dem Cloud-Anwender zu Prüfzwecken einen Zugriff auf die Protokolldaten ermöglichen. Dem Cloud-Anwender muss eine auswertbare Protokollierung zur Verfügung gestellt werden. Die Berechtigung zur Einsichtnahme in die Protokolldaten sollte explizit an den Cloud-Anwender vergeben werden können. Das Durchführen einer Auswertung muss zu einem eigenen Protokolleintrag führen. Die Aufbewahrungszeit der Protokolldaten muss durch den Cloud-Anwender konfigurierbar sein.

- Weitgehende Verschlüsselungen wie eine Transport- und Inhaltsverschlüsselung bilden einen Teilaspekt. Sie können aber keine vollständige Datensicherheit gewährleisten, da der Cloud-Anwender im Rahmen der Verarbeitung der Daten eine Entschlüsselung vornehmen muss und der Cloud-Anbieter sowie die Unteranbieter möglicherweise auf die entschlüsselten Daten Zugriff nehmen können. Eine Inhaltsverschlüsselung unter Verwendung eigener Schlüssel, d. h. welche, auf die der Cloud-Anbieter keinen Zugriff hat und sich auch nicht verschaffen kann, ist dann zu empfehlen, wenn es sich um bloße Storage-Dienste handelt, bei denen über die Datenspeicherung in der Cloud hinaus keine weitere Verarbeitung erfolgt. Durch die geeignete Wahl von Algorithmen und Schlüssellängen kann man hier einen lange währenden Schutz erreichen.

Die Orientierungshilfe „Cloud Computing 2.0“ ist abrufbar unter:

https://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf

Was ist zu tun?

Neben den gesetzlichen Anforderungen an den Vertrag, die beim Cloud Computing gestellt werden, müssen angemessene technisch-organisatorische Maßnahmen gewährleistet werden. Der Dienstleister muss dem Cloud-Anwender nachweisen, dass er in der Lage ist, die datenschutzrechtlichen Bestimmungen einzuhalten. Kann er dies nicht, so sollte von einer Beauftragung dringend Abstand genommen werden.

5.6 Videoüberwachung

Im Dezember 2014 entschied der Europäische Gerichtshof (EuGH), dass private Videoüberwachung durch das Datenschutzrecht begrenzt ist, wenn sie sich „auch nur teilweise auf den öffentlichen Raum erstreckt“. Privatpersonen können sich nicht damit herausreden, es handele sich dabei ausschließlich um eine „persönliche oder familiäre Tätigkeit“. Mit dem Urteil bestätigte der EuGH die Praxis der deutschen Datenschutzbehörden, den Einsatz von Videokameras kritisch zu hinterfragen. Es gibt viele Beschwerden, zumeist von Nachbarn und Mitbewohnern, zunehmend auch über Wildkameras im Wald oder über mobile Kameras, etwa als sogenannte Dashcams in Autos oder als fliegendes Auge in Drohnen. Der EuGH bestätigte auch, dass ein Kameraeinsatz aus Sicherheitsgründen gerechtfertigt sein kann. Ein gesteigertes Sicherheitsbedürfnis des Betreibers genügt aber nicht. Vielmehr müssen bezüglich Grund, Speicherdauer, Übermittlungen und technischer Sicherungen die berechtigten Sicherheitsbelange gegenüber den Schutzinteressen von Betroffenen überwiegen. Hochproblematisch wird es, wenn eine Privatperson die Bilder von Verdächtigen zur Privatfahndung ins Internet stellt. Für die Strafverfolgung muss ausschließlich die Polizei zuständig bleiben.

In einer aktuellen Orientierungshilfe „Videoüberwachung durch nicht öffentliche Stellen“ erhalten Betroffene und Stellen weitere Hinweise:

http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2014/03/OH-V%C3%9C-durch-nicht-%C3%B6ffentliche-Stellen.pdf

5.6.1 Umgang mit Wildkameras

Das ULD wird häufig mit der Frage konfrontiert, inwieweit Jagdausübungsberechtigte in öffentlich zugänglichen Waldbereichen Wildkameras verwenden dürfen. Waldflächen und -wege, in deren Bereich Holz eingeschlagen, aufbereitet, gerückt oder gelagert wird oder Wegebaumaßnahmen durchgeführt werden, sowie Forstkulturen, Pflanzgärten, Wildäcker und sonstige forstwirtschaftliche, fischereiwirtschaftliche oder jagdliche Einrichtungen und Anlagen zählen zu den öffentlich zugänglichen Räumen, wenn ein entgegenstehender Wille aus den Umständen, z. B. über Verbotsschilder oder Eingrenzungen, nicht erkennbar ist.

Jagdausübungsberechtigte können an der Verwendung von Wildkameras ein berechtigtes Interesse haben, da die Kontrolle des Wildbestandes zu den jagdrechtlichen Aufgaben gehört. Die Jagd dient auch der Vermeidung von Überpopulationen, Wildschäden und -seuchen. Zur Einhaltung von Abschussplänen müssen effiziente Jagdstrategien entwickelt werden. Hierzu nutzen Jagdausübungsberechtigte zunehmend Kameras, um z. B. zu dokumentieren, dass Schwarzwild einen bestimmten Futterplatz aufgesucht hat. Diesem berechtigten Interesse stehen die schutzwürdigen Belange von Waldbesuchern, Spaziergängern und Pilzsammlern entgegen, die sich einer Erfassung mittels Videokamera nicht ohne Weiteres entziehen können. Ein Einsatz von Wildkameras in öffentlich zugänglichen Waldbereichen ist daher im Grundsatz unzulässig.

Ausnahmen hiervon sind nur denkbar, wenn die Wildkamera so eingestellt wird, dass einzelne Personen nicht identifizierbar sind. Eine Erfassung von Wanderwegen oder anderen von Personen frequentierten Bereichen ist nicht statthaft. Der Einsatz von Wildkameras im öffentlich zugänglichen Wald ist zulässig, wenn ausschließlich die Futterstelle, die Kirrung, erfasst wird und die Kameraeinstellung so gewählt wird, dass ein Betreten des Bereichs durch Personen mit vernünftigen Erwägungen ausgeschlossen werden kann. Auf den Umstand der Überwachung ist mit geeigneten Mitteln, z. B. mit Schildern, hinzuweisen. Das ULD hat hierzu eine Stellungnahme veröffentlicht.

https://www.datenschutzzentrum.de/artikel/527-.html

Was ist zu tun?

Es ist von allen Beteiligten darauf zu achten, dass der Wald ein überwachungsfreier Erholungsraum bleibt.

5.6.2 Videoüberwachung in Fitnessstudios

Durch mehrere Beschwerden von Betroffenen wurde das ULD auf die umfangreiche Videoüberwachung einer Fitnessstudiokette aufmerksam. Kameraüberwacht werden neben den Eingangs- und Kassenbereichen auch die Trainingsräume sowie die Umkleiden. Über Prüfungen in mehreren Filialen vor Ort verschaffte sich das ULD einen Eindruck von der eingesetzten Technik sowie den jeweils konkret erfassten Bildbereichen und prüfte die jeweiligen Zwecke der einzelnen Kameras.

Die Sicherheit der Kunden, der Trainierenden und der Mitarbeiter sowie das zu schützende Eigentum des Studiobetreibers sind Schutzgüter, die grundsätzlich auch mit Videotechnik geschützt werden dürfen. Die Überwachung muss jedoch stets im Verhältnis zu den dadurch entstehenden Folgen für die Überwachten stehen. Das ULD beanstandete insbesondere die Überwachung in den Umkleiden. Selbst wenn die Gefahren für Spindaufbrüche und der Verlust von Wertsachen nicht unerheblich sind, stellt der Umkleidebereich eine Tabuzone dar, in der im Hinblick auf die Intimsphäre der Kunden eine Videoüberwachung unverhältnismäßig ist. Zum Schutz der Sachwerte ist die verantwortliche Stelle auf alternative Maßnahmen zu verweisen, wie etwa verstärkte Kontrollgänge oder Wertschließfächer.

Auch die Überwachung der Trainingsräume musste das ULD beanstanden. Der großflächigen und umfassenden Überwachung können sich die Kunden nicht entziehen. Während des Trainings werden unweigerlich das gesamte Sozialverhalten der Trainierenden und ihre Interaktion miteinander aufgezeichnet. Für die Kunden gibt es keinen Rückzugsraum. Die Überwachung kann sich über einen langen Zeitraum erstrecken. Das Interesse des Studiobetreibers an der Aufklärung von etwaigen Straftaten, die auf der öffentlichen Trainingsfläche begangen werden, muss zurücktreten im Verhältnis zu der Privatsphäre der überwiegend unauffälligen Kunden. Einige Störfälle pro Jahr rechtfertigen keine dauerhafte und lückenlose Überwachung der Trainingsflächen.

5.7 Einzelfälle

5.7.1 SCHUFA-FraudPool zur Betrugsbekämpfung in der Kreditwirtschaft

Die SCHUFA Holding AG nahm im Juli 2014 eine neue Datenbank zur Bekämpfung von Betrugsfällen und zur Erkennung von Terrorismusfinanzierung und Geldwäsche im Banken-und Kreditwesen in Betrieb, den sogenannten FraudPool. Das ULD war als Mitglied der AG Auskunfteien und der AG Kreditwirtschaft im Vorfeld an Beratungen über die rechtliche Bewertung dieser neuen Datenbank beteiligt und hat starke Bedenken an der Rechtmäßigkeit.

Die Datenbank dürfte als Auskunfteidatenbank bereits deshalb unzulässig sein, weil die gesetzliche Grundlage, auf die die Schufa den Betrieb der Datenbank stützt, nicht anwendbar ist. Der Datenpool soll ebenso wie die bekannte Bonitätsdatenbank auf eine Regelung im BDSG gestützt werden. Das ULD sieht dies kritisch, da für den Bereich der Terrorismusfinanzierung und Geldwäschebekämpfung das Kreditwesengesetz eine Sonderregelung enthält. Danach dürfen Banken und Kreditinstitute zwar Daten untereinander austauschen. Dies soll nach den gesetzlichen Bestimmungen im Kreditwesengesetz aber nur im Einzelfall und nur untereinander erfolgen. Nach Auffassung des ULD legt diese Rechtslage nahe, dass die Einbeziehung einer Auskunftei in den Austauschprozess unzulässig ist.

Die Übermittlung personenbezogener Daten an die Schufa zum Zweck der Teilnahme an einem solchen FraudPool ist damit nach aktueller Auffassung des ULD rechtswidrig. Stellen im Zuständigkeitsbereich des ULD müssen damit rechnen, dass die Übermittlung an einen solchen FraudPool durch Anordnungen untersagt wird.

Unabhängig von der Sperrwirkung des Kreditwesengesetzes ergeben sich weitere Bedenken gegen die Datenverarbeitung.

§ 25 h Abs. 3 Satz 3 Kreditwesengesetz

Institute dürfen im Einzelfall einander Informationen im Rahmen der Erfüllung ihrer Untersuchungspflicht nach Satz 1 übermitteln, wenn es sich um einen in Bezug auf Geldwäsche, Terrorismusfinanzierung oder einer sonstigen Straftat auffälligen oder ungewöhnlichen Sachverhalt handelt und tatsächliche Anhaltspunkte dafür vorliegen, dass der Empfänger der Informationen diese für die Beurteilung der Frage benötigt, ob der Sachverhalt gemäß § 11 des Geldwäschegesetzes anzuzeigen oder eine Strafanzeige gemäß § 158 der Strafprozessordnung zu erstatten ist.

So ist nach Einschätzung des ULD bisher nicht ausreichend geklärt, welche Daten unter welchen Umständen zu einer Meldung an den FraudPool übermittelt werden. Es bestehen zudem große Zweifel daran, ob die aktuell eingesetzte Schufa-Klausel auch die Übermittlung zu Zwecken der Terrorismus- und Geldwäschebekämpfung rechtfertigt. Vor allem aber wird durch den FraudPool eine Datensammlung geschaffen, die in großem Umfang auch strafrechtlich relevante Vorfälle speichert. Die Auslagerung solcher Straftatdatenbanken auf private Unternehmen operiert in einem Raum, der originär zu den staatlichen Aufgaben zählt. Während staatliche Straftatenmeldesysteme und Fahndungsdatenbanken einer strengen Kontrolle unterliegen, gelten für die Schufa keine vergleichbaren Regelungen. Mit Blick auf die bestehenden Probleme der Auskunfteien hinsichtlich der Zuverlässigkeit der dort gespeicherten Daten (Tz. 8.7.2) befürchtet das ULD, dass

die jetzt hinzukommende Speicherung von Straftatverdachtsmeldungen die Betroffenen zusätzlich belastet. Vor dem Hintergrund der Unschuldsvermutung, die bis zum Abschluss eines strafrechtlichen Verfahrens jeden Betroffenen als unschuldig ansieht, droht mit dem FraudPool ein System der Generalverdächtigungen.

Was ist zu tun?

Das ULD muss prüfen, ob und inwiefern aufsichtsrechtliche Anordnungen gegen verantwortliche Stellen in Schleswig-Holstein erlassen werden müssen, die Daten an den FraudPool der Schufa übermitteln.

5.7.2 Schülerdaten zur Bestellung von Schultaschenrechnern

Medien berichteten, dass ein Anbieter von Schultaschenrechnern Lehrkräfte aufgefordert habe, bei Sammelbestellungen ganze Klassenlisten zu übermitteln. Eine Befragung von Schulen ergab, dass die Initiativen für die Sammelbestellungen überwiegend von den Schulen selbst oder einzelnen Lehrern ausgegangen und nur die Namen interessierter Schülerinnen und Schüler von den Schulen übermittelt worden sind. Teilweise wurden die Eltern von den Schulen über einen Elternbrief über die Bestellmöglichkeiten für Schultaschenrechner informiert (Tz. 4.7.6).

Dokumentierte Einwilligungserklärungen der Eltern bezüglich der Übermittlung der Schülernamen zwecks Vornahme einer Taschenrechnerbestellung konnten die Schulen nicht vorlegen. Weder die zur Stellungnahme aufgeforderten Schulen noch der Anbieter der Schultaschenrechner konnten nachvollziehbar begründen, warum in Einzelfällen die Namen aller Schüler übermittelt wurden, obwohl einige der Schüler keine Taschenrechner bestellen wollten. Das ULD hat die Beteiligten zur künftigen Einhaltung der schul- und datenschutzrechtlichen Vorgaben aufgefordert.

Was ist zu tun?

Die Schule und die Lehrkräfte müssen bei Sammelbestellungen vor der Weitergabe der Schülerdaten an das Unternehmen, welches ein Produkt vertreibt, die Einwilligung der Eltern einholen.

5.7.3 Unwirksame Einwilligungserklärung für Werbezusendungen

Im Frühjahr 2013 wollte ein Bürger wissen, ob eine bestimmte Datenschutzerklärung eines großen norddeutschen Kreditinstituts rechtlich zulässig sei. In der Datenschutzerklärung wurde dem Kunden gegenüber behauptet, dass der Gesetzgeber die Abgabe einer Datenschutzerklärung fordere und diese vom Kunden unterschrieben zurückzusenden sei. Bei der Prüfung der Einwilligungserklärung in diesem Institut ging es dem ULD insbesondere darum, ob den Kundinnen und Kunden ausreichend erkennbar gemacht wird, dass die Abgabe der Einwilligung freiwillig erfolgt und diese Einwilligung in keinem Zusammenhang mit dem eigentlichen Vertrag über das Bankkonto steht. In Einwilligungen muss ausreichend konkret benannt werden, zu welchen Zwecken die Daten genutzt werden sollen und infolgedessen auch, worauf sich die Einwilligung bezieht. Die Prüfung des ULD ergab, dass die Einwilligungserklärung nicht ausreichend konkret war. Das Kreditinstitut

unterschied nicht genügend zwischen den vertraglichen und den darüber hinausgehenden Zwecken, für die zumeist eine Einwilligung notwendig ist.

§ 28 Abs. 1 Satz 1 Nr. 1 BDSG

Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

Das ULD wird durch Eingaben von Betroffenen immer wieder auf Fälle aufmerksam, in denen ein Kreditinstitut suggeriert, eine bestimmte datenschutzrechtliche Einwilligung sei notwendig, um seine grundlegenden Vertragszwecke gegenüber dem Kunden erfüllen zu können. Diese nicht zutreffende Behauptung wurde auch im konkreten Verfahren durch das ULD bemängelt. Alle erforderlichen Datenverarbeitungen, die zwischen Kunde und Bank, etwa bezüglich eines Giro- oder Sparkontos, notwendig sind, werden bereits gesetzlich durch das BDSG legitimiert.

Nur wenn ein Kreditinstitut weitere Zwecke verfolgt, etwa das Anbieten von Werbung oder die Durchführung von Marktforschung, ist dazu eine Einwilligung der Kunden erforderlich. Einwilligungen müssen freiwillig sein und dürfen die Datenverarbeitung in Bezug auf den zugrunde liegenden Vertrag nicht beeinflussen. Sie sind auch jederzeit widerruflich, ohne dass der zugrunde liegende Vertrag im Ansatz infrage gestellt würde. Das ULD erreichte im konkreten Fall eine Anpassung der verwendeten Mustervorgaben für datenschutzrechtliche Einwilligungen.

Was ist zu tun?

Unternehmen müssen prüfen, ob eine eingeforderte Einwilligung der Kunden notwendig ist oder die bezweckte Datenverarbeitung durch den Vertragszweck gerechtfertigt wird. Zulässig ist stets nur die unbedingt erforderliche Datenverarbeitung.

5.7.4 Das private Interesse an E-Mail-Adressen von Genussrechtsscheininhabern

Durch Beschwerden vieler Betroffener wurde das ULD auf einen Fall aufmerksam, in dem der ehemalige Geschäftsführer eines Unternehmens die Daten der Genussrechtsscheininhaber weiternutzte, obwohl er als Geschäftsführer abberufen wurde.

Das Unternehmen war in die Insolvenz geraten und stand unter Insolvenzverwaltung. Um die Entscheidungen in den Gläubigerversammlungen zu beeinflussen, griff der ehemalige Geschäftsführer auf die E-Mail und Postadressen der Gläubiger des Unternehmens zurück und verschickte tausendfach Schreiben, in denen er um die Stimmenabgabe auf einer Gläubigerversammlung für eine bestimmte Person bzw. für bestimmte inhaltliche Positionen warb. Die Gläubiger und Genussrechtsscheininhaber hatten zumeist dieser Weiternutzung ihrer Daten durch den ehemaligen Geschäftsführer nicht zugestimmt.

Das ULD kam zu dem Ergebnis, dass der ehemalige Geschäftsführer keine Berechtigung hatte, die Adressdaten zu diesen Zwecken zu nutzen. Die Genussrechtsscheininhaber hatten die Daten nur dem Unternehmen zur Verfügung gestellt, um die Rechte und Pflichten aus der Beteiligung an dem Unternehmen ausüben zu können. Ab dem Zeitpunkt, ab dem das Unternehmen unter der Verwaltung des Insolvenzverwalters stand und der ehemalige Geschäftsführer von seinen Aufgaben entbunden wurde, endete auch dessen Zugriffsbefugnis auf die Daten des Unternehmens.

§ 28 Abs. 1 Satz 2 BDSG

Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

Die spätere Nutzung der Daten durch den ehemaligen Geschäftsführer geschah in getrennter Verantwortung und stand in keinem Zusammenhang zu den ursprünglichen Zwecken, sondern erfolgte im Eigeninteresse des Geschäftsführers. Dieser neue Zweck war weder durch die ursprüngliche Übermittlung an das Unternehmen noch durch die Einwilligung der Betroffenen gedeckt. Das ULD hat deshalb ein Ordnungswidrigkeitenverfahren eingeleitet.

5.7.5 E-Mail-Umleitung bei gleichzeitiger dienstlicher und privater Nutzung

Anlässlich eines Vertretungsfalls in einem Unternehmen wurden sämtliche E-Mails der vertretenen Person zur Geschäftsleitung umgeleitet. Das Unternehmen hatte keine Festlegungen über die Zulassung von privater E-Mail-, Internet- und Telefonnutzung vorgenommen. Seit Jahren wurde offen die private Nutzung dieser dienstlichen Kommunikationsmittel geduldet. So landete eine Vielzahl privater E-Mails durch die Umleitung im Zugriffsbereich des Geschäftsführers.

Ein Unternehmen ist als Telekommunikationsanbieter anzusehen, wenn Mitarbeiter dienstliche Kommunikationsmittel zu privaten Zwecken nutzen dürfen. Dies gilt im Fall einer ausdrücklichen Genehmigung wie auch im Fall der offensichtlichen Duldung. Damit ist das Unternehmen an das Fernmeldegeheimnis gebunden. Es darf sich ohne Einwilligung des Mitarbeiters keine Kenntnis des Inhalts der privaten E-Mails verschaffen. Diese Rechtsauffassung wird zwar durch aktuelle einzelne Urteile infrage gestellt, das ULD vertritt aber nach wie vor diese Position. Auch in der datenschutzrechtlichen Literatur wird auf die entscheidende Rolle des Unternehmens an der Erbringung der Kommunikationsleistung hingewiesen. Der Inhalt der Kommunikation ist damit in gleicher Weise vor dem Zugriff zu schützen wie gegenüber jedem anderen Erbringer von Telekommunikationsleistungen.

Das ULD empfahl dem Unternehmen für die Zukunft beim dienstlichen und privaten Gebrauch der unternehmerischen Kommunikationsmittel das vom ULD entwickelte und etablierte Stufenmodell. In dessen Hinweisblatt finden sich weitere technische Empfehlungen, um einen Konflikt zwischen der privaten Internetnutzung der Mitarbeiter und den berechtigten Kontrollbedürfnissen der Unternehmen zu vermeiden. Über die Nutzung von Webmail-Diensten kann das betriebliche E-Mail-Postfach von privater Korrespondenz freigehalten werden.

https://www.datenschutzzentrum.de/uploads/privatwirtschaft/private-und-dienstliche-internetnutzung.pdf

5.7.6 Veröffentlichte Krankheitsabwesenheitszeiten zur Motivationsförderung

Mit einer besonderen Aktion warb ein Arbeitgeber um Verständnis für die schlechte wirtschaftliche Situation seines Betriebes. Die von den Beschäftigten erfassten Arbeitszeiten wurden vom Arbeitgeber nach sogenannten produktiven und unproduktiven Arbeitszeiten sowie Fehlzeiten wegen Krankheit ausgewertet. Die ermittelten Daten wurden monatlich unter Namensnennung und Ermittlung der jeweils konkreten finanziellen Belastung für den Arbeitgeber durch Aushang bekannt gegeben. Die Zahlen sollten den Beschäftigten die Hintergründe für die bereits erfolgte Einstellung der Weihnachtsgeldzahlung sowie für anstehende betriebsbedingte Kündigungen verdeutlichen.

Unsere Nachfrage führte umgehend zum Entfernen des Aushangs. Man räumte blauäugiges Handeln ein. Das Ziel sei jedoch erreicht worden: Die wirtschaftliche Lage des Betriebes habe sich verbessert. Nach der kritischen Hinterfragung des Vorgehens durch das ULD beabsichtigt das Unternehmen, künftig weiterhin entsprechende Listen – jedoch ohne dass ein Personenbezug möglich ist – zur Motivation der Beschäftigten zu veröffentlichen.

06

KERNPUNKTE

Sichere IT-Infrastrukturen

Standard-Datenschutzmodell

Verfahrensdokumentation

6 Systemdatenschutz

6.1 Zusammenarbeit auf Landesebene

Der Chief Information Officer (CIO) und das zentrale IT-Management der Staatskanzlei, die Abteilung ZIT, organisieren maßgeblich den IT-Betrieb der Landesregierung. Dazu zählen neben den Ministerien auch die nachgeordneten Behörden des Landes. Darüber hinaus nutzen weitere Institutionen wie die Landtagsverwaltung und der Landesrechnungshof Teile der technischen Infrastruktur der Landesregierung, etwa den Standard der Bürokommunikation oder das Landesnetz. Im Bereich der IT gibt es zahlreiche Schnittstellen und gemeinsame IT-Projekte von Land und Kommunen, etwa die Anschlüsse von Kreisen an das Landesnetz oder ein E-Mail-Austausch zwischen Land und Kommunen bei Dataport auf der Plattform „Mailland“. Zur Koordination gibt es verschiedene Gremien, die teils operativen, teils strategischen Charakter haben:

Die IT-Beauftragten-Konferenz (ITBK) ist die monatliche Besprechung der Abteilung ZIT mit den IT-Leitungen der Ressorts und einiger nachgeordneter Behörden. Häufig sind Mitarbeiterinnen oder Mitarbeiter von Dataport zu Gast, die zu aktuellen Entwicklungen bei Dataport mit allgemeiner Bedeutung vortragen, etwa zur Umzugsplanung in die neuen Rechenzentren RZ^2 oder zum Vertragsmanagement.

Der (Bundes-)IT-Planungsrat, in dem Bund und Länder die bundesweite IT-Planung vorantreiben, hat ein Spiegelgremium in Schleswig-Holstein: Der vierteljährlich tagende Landes-IT-Rat dient der Information und dem Meinungsaustausch zwischen den Vertretern Schleswig-Holsteins im IT-Planungsrat (CIO und Staatskanzlei) und den mit IT-Themen befassten Institutionen des Landes (u. a. Landesregierung, Ressorts, Landtag, Landesrechnungshof) und der Kommunen, vertreten durch das KOMFIT (Kommunales Forum für Informationstechnik).

Ein spezielles Gremium für das Thema „IT-Sicherheit“ ist das Integrierte Sicherheitsmanagementsystem (ISMS) des Landes. Die IT-Sicherheitsbeauftragte des Landes ist im ZIT angesiedelt. Parallel gibt es in den Ressorts und vielen nachgeordneten Behörden IT-Sicherheitsbeauftragte. Vertreten ist auch der kommunale Bereich durch das KOMFIT sowie Dataport. In zweimonatlichen Arbeitstreffen werden dort Rahmenrichtlinien sowie das strategische und operative Sicherheitsmanagement abgestimmt.

In allen drei Gremien ist auch das ULD vertreten, wird dort frühzeitig über neue Entwicklungen und Planungen informiert und kann sich kommentierend oder beratend für Datenschutzbelange einsetzen.

Was ist zu tun?

Die konstruktive Zusammenarbeit auf Landesebene sollte weiter fortgesetzt werden.

6.2 Länderübergreifende Zusammenarbeit der Datenschutzbeauftragten

Die Zusammenarbeit der Datenschutzbeauftragten zu technisch-organisatorischen Fragen erfolgt insbesondere über den Arbeitskreis Technik, der diesbezüglich auch allen Facharbeitskreisen und -arbeitsgruppen zuarbeitet. Daneben gibt es regionale und Ad-hoc-Kooperationen sowie eine Vertretung der Datenschutzbeauftragten in externen Gremien, die sich mit Datenschutz und Datensicherheit in der Verwaltung und der Wirtschaft befassen.

6.2.1 Themen aus dem AK Technik

Im Arbeitskreis Technik (AK Technik) treffen sich Vertreter der Technikabteilungen bzw. Technikreferate der Datenschutzbeauftragten der Länder und des Bundes. Der Arbeitskreis bereitet Kommentare, Orientierungshilfen (z. B. Tz. 5.5) und Entschließungen zu technischen Themen für die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSBK) vor. Die DSBK trifft sich im Halbjahresabstand, um Dokumente aus diesem und anderen Arbeitskreisen zu verabschieden, auf die sie sich deutschlandweit geeinigt haben. Im Berichtszeitraum haben vier Sitzungen des AK Technik stattgefunden.

Dabei ragten die folgenden Themen in den vergangenen zwei Jahren heraus:

- die Entwicklung eines Standard-Datenschutzmodells (SDM) zur Standardisierung technisch-organisatorischer Schutzmaßnahmen des Datenschutzes (siehe Tz. 6.2.3),
- soziale Netzwerke und öffentliche Fahndung (siehe Tz. 4.3.3),
- die Sicherheit von Cloud Computing (siehe Tz. 5.5, 8.3),
- die von Geldinstituten vorgelegten Privacy Impact Assessments (Technikfolgenabschätzung) unter Einsatz von Near Field Communication (NFC) bei Geldkarten,
- die Sicherheit von Verwaltungsnetzen,
- die Sicherheit von De-Mail.

Nachfolgend werden die Themen angesprochen, für die kein eigener Beitrag im Tätigkeitsbericht vorgesehen ist.

Geldkarten

Dem AK Technik wurden von den Anbietern sogenannte Privacy Impact Assessments (PIA) – offizielle datenschutzrechtliche Bewertungen – der Geldkarte „girogo“ der Deutschen Kreditwirtschaft sowie der kontaktlosen Zahlungsverfahren „PayWave“ von VISA und „PayPass“ von MasterCard vorgelegt.

Den Datenschutzbehörden vorgelegte PIAs orientieren sich regelmäßig an den methodischen Vorgaben der International Organization for Standardization (ISO) und genügen diesen durchaus. Ein Vorbild ist der Entwurf „Privacy and Data Protection Impact Assessment Framework for RFID Applications“ des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) vom Januar 2011, der auch in die Arbeit der ISO eingespeist wurde. Ein Erfüllen dieser Anforderungen bedeutet aber nicht zwangsläufig, dass das in Deutschland geltende Datenschutzrecht beachtet wird. Aus Sicht des ULD ist insbesondere das genutzte Angreifermodell mangelhaft. Dieses konzentriert sich einseitig auf von Hackern ausgehende Risiken und übersieht die Risiken für die Betroffenen, die von den die Geldkarte nutzenden Unternehmen selbst ausgehen. Außerdem wurde der Prüfgegenstand zu eng definiert, indem ausschließlich die drahtlose Schnittstelle NFC – Near Field Communication – der girogo-Karte betrachtet wurde; andere wichtige Systemteile, z. B. die Backend-Kommunikation der Systeme von Händlern, blieb außen vor. Das Auslesen der Daten ist ohne besondere Authentisierung möglich und kann auch durch Dritte erfolgen, die ein Lesegerät in die Nähe der Karte bringen. So können z. B. Geldkarten in Portemonnaies im Gedränge in öffentlichen Verkehrsmitteln mit versteckten NFC-fähigen Smartphones ausgelesen werden. Datenschutzaufsichtsbehörden monierten zudem die unverschlüsselte Datenübertragung zwischen Karte und Terminal, die mit einem gewissen – leistbaren – Aufwand mitgelesen werden kann.

Auf solchen Karten können auch Dritten, z. B. Fitnessklubs, Lese- und Speichermöglichkeiten zur Verfügung gestellt werden, die die ausgebenden Stellen, also die Banken, VISA oder MasterCard, nicht im Einzelnen beeinflussen können. Dies begründet die Gefahr, dass dort personenbezogene Informationen gespeichert werden, die beim unbefugten Mitlesen mit Daten aus dem Bereich der Geldkarte kombiniert werden können, und dass Nutzeraktivitäten anwendungsübergreifend zusammengeführt werden. Für das ULD ist das vorgelegte PIA somit nicht mehr als eine Art Herstellererklärung, die methodisch-wissenschaftlichen Maßstäben nicht genügt und weder den Anforderungen des Datenschutzrechts noch den Aspekten der IT-Sicherheit gerecht wird.

Als Schutzmaßnahmen wurde von den Aufsichtsbehörden die Ausgabe von Schutzhüllen an die Kunden verlangt, die die drahtlose Kommunikation blockieren. Eine Möglichkeit für Kundinnen und Kunden, die NFC-Kommunikationsfähigkeit ihrer Karte auszuschalten, besteht derzeit nicht; sie ist aber sinnvoll. Weiterer Inhalt des Forderungskatalogs ist die Verpflichtung der Unternehmen, nur solche Daten zu speichern, die das Pseudonymisierungskonzept der Karte nicht unterlaufen,

und dass Zufallszahlen als Kartennummern genutzt werden.

Die Anforderungen an ein PIA aus Sicht der Datenschutzaufsichtsbehörden wurden im November 2013 in einem Papier abgestimmt:

https://www.datenschutz-mv.de/datenschutz/publikationen/informat/pia/pia.pdf

Was ist zu tun?

Bei der Durchführung sind die Anforderungen der Datenschutzaufsichtsbehörden zur Grundlage zu nehmen.

Sicherheit von Verwaltungsnetzen

Nach dem Bekanntwerden der Aktivitäten insbesondere US-amerikanischer und britischer Geheimdienste stellt sich verstärkt die Frage nach der Sicherheit und dem Datenschutz in deutschen Verwaltungsnetzen. Der AK Technik plant deshalb – unter Berücksichtigung auch der Aktivitäten des IT-Planungsrates, wonach sich die Geltung der IT-Sicherheitsleitlinie für den Bund und die Länder auch auf den kommunalen Bereich erstrecken soll – per Fragebogen flächendeckend die Sicherheitsaspekte der Landesnetze, die von Kommunen und von der Landesebene genutzt werden, zu erheben. Die Notwendigkeit für Kommunen in Schleswig-Holstein, eine sichere IT-Infrastruktur zu betreiben, ergibt sich nicht erst aus der IT-Sicherheitsleitlinie des IT-Planungsrates, sondern unmittelbar aus den Anforderungen des Landesdatenschutzgesetzes (LDSG) in Verbindung mit der Datenschutzverordnung des Landes (DSVO). Das ist keine Frage der Konnexität.

Was ist zu tun?

Angesichts zunehmender Relevanz und Sensibilität der Kommunikation in Verwaltungsnetzen sind verstärkte Anforderungen an Vertraulichkeit und Integrität zu stellen.

De-Mail

Das Thema „De-Mail“ begleitet den AK Technik seit Jahren. Ein dauernd wiederkehrender besonderer Aspekt ist die Verschlüsselung.

Die gesetzlich vorgesehene Ver- und Entschlüsselung bei De-Mail ist eine Transportsicherung, die nicht unter der Kontrolle der Nutzerinnen und Nutzer steht. Sie sichert den Transport zwischen verschiedenen De-Mail-Servern. Auch der Weg zwischen De-Mail-Server und dem Mail-Client des Benutzers, meist ein Webbrowser, ist transportgeschützt durch eine https-Verschlüsselung bei den Browsern. Doch den verwendeten Schlüssel kennt auch der De-Mail-Anbieter.

Gleichwohl ist es möglich, De-Mail-Kommunikation Ende-zu-Ende zu verschlüsseln. De-Mail erlaubt auch die Verwaltung solcher Schlüssel. Idealerweise erfolgt die Verschlüsselung unter der alleinigen Hoheit des Absenders und liegt die Entschlüsselung in der alleinigen Hoheit des Empfängers. Dies gilt für die Nutzung von Webmail zumeist nicht, da ein Webmail-Client nur einen Fernzugriff auf die Server des Betreibers zulässt. Die Ver- und Entschlüsselung erfolgt auf den Servern des Betreibers und nicht in der alleinigen Hoheit von Absender und Empfänger. Dennoch wird das Mitlesen durch einzelne Mitarbeiter der Betreiber und unbefugte Empfänger erschwert, da die Ver- und Entschlüsselungen stärker gekapselt sind als bei der Transportverschlüsselung.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) empfiehlt Berufsgeheimnisträgern, zur Übertragung von Informationen bei Nutzung von De-Mail und ePost eine Ende-zu-Ende-Verschlüsselung vorzunehmen. Aus Sicht des ULD gilt diese Empfehlung auch für

Amtsgeheimnisträger, wenn De-Mail für die bundesländerübergreifende Behördenkommunikation eingesetzt wird. Es stellt sich aber die Frage, wie sinnvoll die Nutzung von De-Mail dann ist, zumal die bewährte OSCI-Transport-Technik jeder Behörde zur Verfügung steht – sei es unmittelbar in den Anwendungsprogrammen eingebunden oder vermittelt durch eine Clearingstelle, deren Nutzung, wie im Falle des Melderechts, möglicherweise sogar gesetzlich vorgeschrieben ist.

Was ist zu tun?

Wenn sich aus einer Schutzbedarfsanalyse die Anforderung nach Ende-zu-Ende-Sicherheit ergibt, darf De-Mail nicht ohne zusätzliche Sicherheitsvorkehrungen genutzt werden.

6.2.2 Standard-Datenschutzmodell (SDM)

Die 85. Datenschutzbeauftragtenkonferenz (DSBK) hat im März 2013 eine Arbeitsgruppe mit der Entwicklung eines Standard-Datenschutzmodells (SDM) beauftragt. Diese Arbeitsgruppe ist mit Vertretern verschiedener Bundesländer besetzt. Unter dem Vorsitz Schleswig-Holsteins konnte der 88. Datenschutzkonferenz im Oktober 2014 ein erster vollständiger Entwurf des Modells zur Abstimmung vorgelegt werden. Der Modellentwurf fand in der DSBK breite Zustimmung. Die Arbeitsgruppe wurde damit beauftragt, auf der Grundlage dieses akzeptierten Modells einen Referenzkatalog mit Standard-Datenschutzmaßnahmen zu entwickeln.

Ein solcher Katalog kann als Grundlage für Datenschutzprüfungen und -beratungen im Hinblick auf technisch-organisatorische Maßnahmen genutzt werden, ohne dass dadurch die Unterschiede in den Datenschutzgesetzen der Länder und des Bundes eingeebnet werden und die Unabhängigkeit der Datenschutzaufsicht aufgehoben wird.

Die Bemühungen der deutschen Aufsichtsbehörden um ein Standard-Datenschutzmodell stehen im Einklang mit den Standardisierungsaktivitäten des nationalen IT-Planungsrates (ITPR) als auch mit denen auf europäischer Ebene. Der ITPR bemüht sich, die Funktionalität, die Interoperabilität, die Kosten, die Sicherheit und Ordnungsmäßigkeit des IT-Betriebs in der öffentlichen Verwaltung zu verbessern. Das Modell hilft ebenso Unternehmen, die gesetzlichen Anforderungen zu operationalisieren und dabei die Kosten für die konkreten Datenschutz- und IT-Sicherheitsmaßnahmen zu kalkulieren. Nicht zuletzt erlaubt es, bei der Planung von neuen Projekten etwa mit wissenschaftlichem Anspruch die bestehenden operativen Anforderungen zu erfüllen. Das Modell verbessert generell die Erwartungssicherheit darüber, welche technischen und organisatorischen Schutzmaßnahmen in welchem Maße Datenschützer bei Verfahren mit Personenbezug vorzufinden erwarten. Das hilft den behördlichen und betrieblichen Datenschutzbeauftragten, mit Verweis auf den Maßnahmenkatalog bestimmte Schutzmaßnahmen des Datenschutzes einzufordern.

Das Standard-Datenschutzmodell verfolgt methodisch einen ähnlichen Ansatz wie der inzwischen gut verstandene IT-Grundschutz des BSI. Außerdem enthält das Modell Aspekte des IT-Security Managements nach ISO 27001. Anders als diese Methoden, die ausschließlich der Gewährleistung von IT-Sicherheit dienen, zielt das SDM auch auf die wirkungsvolle Umsetzung der Rechte der Betroffenen ab. Ein wesentlicher Aspekt ist, dass die dreistufigen Schutzbedarfsfeststellungen, wie man sie vom Grundschutz kennt, explizit aus der Sicht der Betroffenen formuliert und dass die zu betrachtenden Risiken nicht nur anhand von drei, sondern von sechs Schutzzielen – Verfügbarkeit, Integrität, Vertraulichkeit sowie Transparenz, Nichtverkettbarkeit und Intervenierbarkeit – analysiert werden. Neben den Risiken der konkreten personenbezogenen Datenverarbeitung werden auch die Risiken der IT-Systeme und -Prozesse betrachtet.

Schutzziele sind in vielen Landesdatenschutzgesetzen aufgeführt, insbesondere in den Daten-

schutzgesetzen neueren Datums. Schleswig-Holstein hat die sechs Schutzziele bislang als einziges Bundesland seit 2012 vollständig im LDSG verankert.

Was ist zu tun?

Bei der methodisch angeleiteten Gestaltung von Verfahren mit Personenbezug sind a) die Schutzziele aus § 5 LDSG heranzuziehen, ist b) eine Schutzbedarfsanalyse anhand der sechs Schutzziele aus der Sicht von Betroffenen anzufertigen und sind c) entsprechende Schutzmaßnahmen vorzusehen, die für Daten, IT-Systeme und -Prozesse gesondert zu treffen sind.

6.2.3 Arbeitsgruppe der Datenschutzbeauftragten der Dataport-Trägerländer

Mit dem Land Sachsen-Anhalt, das im Januar 2014 dem Staatsvertrag zur Gründung von Dataport beigetreten ist, hat Dataport insgesamt sechs Trägerländer: Schleswig-Holstein, Hamburg, Bremen, Niedersachsen, Mecklenburg-Vorpommern und Sachsen-Anhalt. Für diese führt die Anstalt insbesondere Auftragsdatenverarbeitungen durch, wobei sie die verschiedenen Datenschutzregeln der jeweiligen Länder zu beachten hat, also das für die Auftraggeber jeweils geltende Recht. Dataport verarbeitet zudem Daten in bestimmten Fällen eigenverantwortlich, wie z. B. die Personaldatenverarbeitung für Dataport-Mitarbeiterinnen und -Mitarbeiter. Dies richtet sich gemäß dem Staatsvertrag nach dem LDSG Schleswig-Holstein; die zuständige Aufsichtsbehörde ist das ULD. Bei der Datenverarbeitung im Auftrag für die jeweiligen Trägerländer oder deren Kommunen muss Dataport für einzelne Verfahren bis zu sechs verschiedene Regelungen beachten und wird durch bis zu sechs Datenschutzaufsichtsbehörden kontrolliert.

Erklärtes Ziel der Gründung von Dataport war, durch Zusammenarbeit der Bundesländer Synergieeffekte zu nutzen. Dies gelingt, wenn Dataport Verfahren länderübergreifend oder zumindest möglichst einheitlich, z. B. durch Nutzung der gleichen Software, betreiben kann. Die Grenzen der übergreifenden Zusammenarbeit bilden die jeweiligen landesrechtlichen Regelungen.

Im technischen Bereich sind die Landesregelungen zur Datensicherheit weitgehend vergleichbar. Unterschiede gibt es im materiellen Recht: Setzen die Länder Bundesrecht um, etwa im Bereich des Pass- und Personenstandswesens, sind die Rechtsgrundlagen identisch. Ergänzende Festlegungen und Weisungen bei der Ausführung von Bundesrecht sind zwischen den Trägerländern mitunter unterschiedlich.

Ein weiterer Unterschied ist die Anzahl der Daten verarbeitenden Stellen: In den Stadtstaaten Hamburg und Bremen gibt es oft nur einen zentralen Auftraggeber für ein Verfahren. Im Flächenland Schleswig-Holstein mit vielen Kommunen haben diese mitunter verschiedene Anforderungen an „ihr" Verfahren. Dies erfordert eine mandantenfähige Anwendung. Beim Betrieb von manchem Verfahren ist die Überraschung bei den Beteiligten groß, wenn dieses aus Hamburg von Schleswig-Holstein übernommen werden soll und hierzulande deutlich mehr und differenzierte Zugriffsberechtigungen vergeben werden müssen. Folge ist, dass mitunter die Software angepasst bzw. erweitert werden muss, um den Unterschieden gerecht zu werden.

Da bis zu sechs Aufsichtsbehörden zuständig sind, ist deren Absprache, etwa bei den Prüfungsmaßstäben oder über eine Zusammenarbeit bei Prüfungen und Beratungen, geboten. Zu diesem Zweck gibt es regelmäßige Treffen der Datenschutzaufsichtsbehörden auf Arbeits- und Leitungsebene, in denen gemeinsam Strategien festgelegt werden. So wird Doppelarbeit vermieden, Know-how gebündelt und Prüfungsmaßstäbe, soweit möglich, angeglichen.

Was ist zu tun?

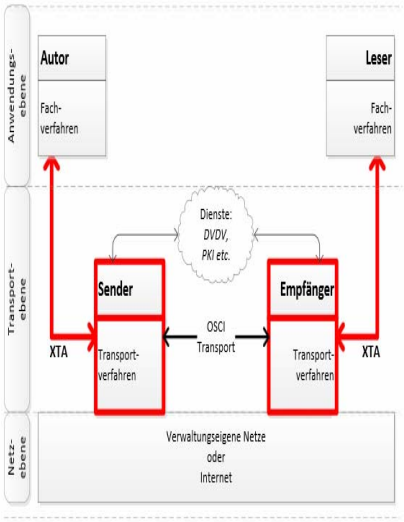
Dataport und seine Auftraggeber sollten die Datenschutzbeauftragten frühzeitig einbinden, damit auf gegebenenfalls abweichende landesrechtliche Regelungen schon in der Planungsphase reagiert werden kann.

6.2.4 Standardisierung von Datentransport im E-Government (XTA)

Das ULD berät eine Arbeitsgruppe des IT-Planungsrates bei der Erstellung der Spezifikation eines standardisierten Transportadapters für die öffentliche Verwaltung (XTA).

Der XTA ist ein Programmbestandteil zwischen einem Fachverfahren, mit dem die Sachbearbeitung in einer öffentlichen Verwaltung durchgeführt wird, und dessen Transportschnittstelle, über welche die Daten zu einem anderen Fachverfahren einer anderen Verwaltungseinheit geschickt werden. Wesentlich dabei ist, dass der Betreiber einer Transportschnittstelle – zumeist sind mit dieser Aufgabe Rechenzentren betraut – nachweisbar keinen Zugriff auf die Inhaltsdaten des Fachverfahrens nehmen kann und jederzeit vollständige Transparenz darüber herstellbar ist, welches System an den Transaktionen in welcher Form beteiligt war. Der Hintergrund zur Notwendigkeit der Standardisierung sowie der Begleitung der XTA-Entwicklung durch den Datenschutz wurden bereits im letzten Tätigkeitsbericht (34. TB, Tz. 6.3.3) ausführlich dargestellt.

Die funktionale Spezifikation des XTA ist inzwischen abgeschlossen. Im Jahr 2014 wurde ein Testkonzept für XTA-Nachrichten entwickelt. Mit dem Testkonzept soll die Implementation von XTA mit der Spezifikation gemäß den Vorgaben der Datensicherheit und des Datenschutzes aktiv anhand von Testnachrichten kontrolliert werden können. Dafür wurde eine Vielzahl von Testnachrichten entwickelt. Darunter sind Testnachrichten, mit denen die Wirksamkeit aller Maßnahmen zur Gewährleistung der sechs Datenschutz-Schutzziele (vgl. Tz. 6.2.2) überprüft werden können. Konkret sind Testnachrichten spezifiziert, die die Systemeigenschaften bezüglich der Protokollierung, der Verschlüsselung, des Integritätsschutzes sowie der Zustellung bzw. des Abrufs von Nachrichten über die gesamte Transportkette, die aus mehreren XTA-Servern bestehen kann, kontrollieren.



Darstellung des Regelungsgegenstandes von XTA bei der Vereinheitlichung der Schnittstellen zwischen IT-Fachverfahren (Autor bzw. Leser einer Nachricht) und den Transporteuren (Sender bzw. Empfänger einer Nachricht)

Aus: KoSIT: „XTA in der E-Government-Infrastruktur des IT-Planungsrates", S. 4

http://www.xoev.de/sixcms/media.php/13/Anlage%201%20XTA-Infrastruktur_Ziele.pdf

Es zeigt sich, dass eine aktive Teilnahme schon bei der Spezifikation eines Verfahrens dazu führen kann, dass IT-Sicherheit und Datenschutz ganzheitlich berücksichtigt werden. Mehr noch: Es können bislang wenig erprobte, aber absehbar wirksame Instrumente des Datenschutzes, wie die Formulierung von Testnachrichten zum Test der Maßnahmenumsetzung, fortentwickelt werden. Damit wurde ein weiterer Schritt zur Automatisierung auch von Datenschutzprüfungen getan.

Der gesamte Zuschnitt des XTA-Projekts ist ein Vorbild zur Erarbeitung von Standards für die öffentliche Verwaltung in Deutschland. Der Pro-

jektzuschnitt erfüllt viel besser als andere IT-Projekte vergleichbarer Art die Anforderungen der Schutzziele, insbesondere nach Transparenz, Intervenierbarkeit und Integrität, die man an das Projektmanagement selbst stellen kann und muss. Das Konzept der aktiven Kontrolle der Datenschutzeigenschaften von Verfahren befindet sich noch am Anfang der Entwicklung.

Was ist zu tun?

Die guten Erfahrungen in der Zusammenarbeit mit der Arbeitsgruppe des IT-Planungsrates sollte als Vorbild für die Begleitung weiterer strategisch zentraler Projekte zur Standardisierung von Verwaltungsverfahren in Deutschland genommen werden.

6.3 Ausgewählte Ergebnisse aus Vorabkontrollen und Prüfungen

6.3.1 Dokumentation von Abrufverfahren und gemeinsamen Verfahren

Die Rechtslage nach der Datenschutzverordnung (DSVO) ist eindeutig: „Automatisierte Verfahren sind zu dokumentieren." Für die Verwaltung des Landes beschreibt die DSVO die Einzelheiten, was genau dokumentiert werden muss, schreibt aber nicht die Form der Dokumentation vor.

Zur Erinnerung: Automatisierte Verfahren sind Arbeitsabläufe zur Verarbeitung personenbezogener Daten mithilfe von informationstechnischen Geräten (Hardware), Programmen (Arbeitsanweisungen für die Hardware) und automatisierten Dateien (elektronisch gespeicherte Daten).

Schon die Dokumentation eines automatisierten Verfahrens, das personenbezogene Daten nur innerhalb einer öffentlichen Stelle verarbeitet, stellt einen gewissen koordinativen Arbeitsaufwand dar, an dem idealerweise die Administration, die Fachbereiche und – sofern vorhanden – auch die oder der Datenschutzbeauftragte beteiligt sein sollten. Für diese Dokumentation stellt das ULD auf seiner Webseite Handreichungen und Vorlagen als Hilfestellung zur Verfügung.

https://www.datenschutzzentrum.de/dsvo/

Schwieriger sind Dokumentationen, wenn es um Abrufverfahren oder gemeinsame Verfahren geht, an denen mehrere öffentliche Stellen beteiligt sind:

Abrufverfahren

Ein Abrufverfahren ermöglicht die Übermittlung definierter personenbezogener Daten per Online-Abruf durch andere Daten verarbeitende Stellen. Es ist zwischen der speichernden Stelle und der abrufenden Stelle zu unterscheiden. Die abrufende Stelle trägt die Verantwortung für die Zulässigkeit des einzelnen Abrufs. Die speichernde Stelle ist sowohl verantwortlich für die Ordnungsmäßigkeit der Datenverarbeitung, also die Sicherstellung der technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit, als auch für die Richtigkeit der verarbeiteten Daten. Sie muss demnach auch die vollständige Verfahrensdokumentation des automatisierten Verfahrens erstellen. Die nachfolgend aufgeführten Punkte sind in Verbindung mit den Regelungen in der DSVO für die speichernde Stelle bei der Dokumentation besonders relevant:

- Die generelle Zulässigkeit der Übermittlung an eine abrufende Stelle einschließlich der Zulässigkeit des Abrufverfahrens als solches (§ 8 Abs. 1 LDSG) muss vor dem ersten Abruf geprüft und dokumentiert werden (§ 3 Abs. 2 Nr. 1 DSVO).
- Die Schnittstellen zu den abrufenden Stellen müssen in Form eines Datenflussdiagramms (§ 3 Abs. 2 Nr. 4 DSVO) dargestellt werden.

- Die Dokumentation muss einen Überblick darüber geben, wer mit welcher Berechtigung welche Daten abrufen darf (§ 3 Abs. 2 Nr. 5 DSVO).
- Die Zulässigkeit von Abrufen ist durch die speichernde Stelle nicht einzeln zu prüfen (§ 8 Abs. 5 LDSG). Eine anlassbezogene Prüfung im Einzelfall muss jedoch möglich sein. Um das zu gewährleisten, muss ein entsprechender Protokollierungsprozess eingeführt und dokumentiert werden (unter Berücksichtigung von § 4 Abs. 5 DSVO).
- Im Datenschutzmanagement muss ein geeigneter Prozess definiert werden, um sicherzustellen, dass Betroffene ihre Rechte ausüben können, die sie gemäß § 8 Abs. 3 LDSG sowohl bei der speichernden als auch bei der abrufenden Stelle einfordern können. Das bedeutet, dass alle beteiligten Stellen einen einheitlichen Prozess definieren und dokumentieren müssen (§ 4 Abs. 6 DSVO).
- Das Verfahrensverzeichnis muss um eine Kategorie erweitert werden, in der die Verantwortungsbereiche beschrieben werden, die die speichernde Stelle übernimmt.

Der Umstand, dass die speichernde Stelle für die vollständige Verfahrensdokumentation verantwortlich ist, entbindet im Umkehrschluss die abrufende Stelle jedoch nicht von ihrer Verantwortung für die Zulässigkeit der einzelnen Abrufe. Sie muss deshalb in einer geeigneten Form sowohl einen Abrufprozess festlegen – d. h., sie muss festlegen, wer welche Daten zu welchem Zweck abrufen darf und wie lange diese Abrufe dokumentiert werden – als auch die Protokolldaten für den definierten Zeitraum vorhalten, um den tatsächlichen Abruf nachvollziehen zu können. Auch die Verfahrensbestandteile, wie z. B. Hard- und Software, die benötigt werden, um den Abrufprozess durchzuführen, als auch die Sicherstellung der Betroffenenrechte sind bei der abrufenden Stelle zu dokumentieren. Im Grundsatz obliegen der speichernden Stelle und allen abrufenden Stellen entsprechende Dokumentationspflichten. Das ULD erarbeitet zurzeit in Zusammenarbeit mit betroffenen Behörden die Dokumentationsbestandteile, die abrufende Stellen vorhalten müssen. Die erarbeiteten Ergebnisse werden dann auf der Webseite veröffentlicht.

Gemeinsames Verfahren

Im Gegensatz zu Abrufverfahren, bei denen die abrufenden Stellen auf „fremde“ Datenbestände zugreifen, verarbeiten zwei oder mehrere Daten verarbeitende Stellen bei einem gemeinsamen Verfahren mit einem automatisierten Verfahren (eventuell teilweise) einen gemeinsamen Datenbestand, d. h., sie können unmittelbar dieselben Daten verarbeiten. Unabhängig davon, dass es bei den gemeinsamen Verfahren mehrere Möglichkeiten der Verteilung von Aufgaben und Verantwortung gibt, gilt auch hier der Grundsatz, dass alle beteiligten Stellen das gemeinsame Verfahren als ein automatisiertes Verfahren nach LDSG und DSVO dokumentieren müssen. Je nach Umfang der Verantwortung, welche die beteiligten Stellen am gemeinsamen Verfahren übernehmen, fallen die Dokumentationsbestandteile mehr oder weniger umfangreich aus.

Nachfolgende Punkte müssen in Verbindung mit den Regelungen in der DSVO bei gemeinsamen Verfahren besonders sorgfältig dokumentiert werden:

- Die Schnittstellen zu den beteiligten Stellen müssen in Form eines Datenflussdiagramms (§ 3 Abs. 2 Nr. 4 DSVO) dargestellt werden.
- Die Dokumentation muss einen Überblick darüber geben, wer mit welcher Berechtigung welche Daten im gemeinsamen Verfahren verarbeiten darf (§ 3 Abs. 2 Nr. 5 DSVO).
- Im Datenschutzmanagement muss ein geeigneter Prozess definiert werden, um sicherzustellen, dass Betroffene ihre Rechte ausüben können, die sie gemäß § 8 Abs. 3 LDSG bei allen beteiligten Stellen einfordern können. Das bedeutet, dass alle beteiligten Stellen einen einheitlichen Prozess definieren und dokumentieren müssen (§ 4 Abs. 6 DSVO).
- Das Verfahrensverzeichnis muss um eine Kategorie erweitert werden, in der die Verantwortungsbereiche beschrieben werden, die die beteiligten Stellen übernehmen.

Wie kann eine Dokumentation bei einem gemeinsamen Verfahren praktisch aussehen? Aus rechtlicher Sicht können bei gemeinsamen Verfahren grob drei Konstellationen unterschieden werden:

- Alle beteiligten Stellen sind selbst verantwortlich sowohl für die Ordnungsmäßigkeit der Datenverarbeitung als auch für die Richtigkeit der gespeicherten Daten.
- Die Verantwortung für die Gewährleistung der Ordnungsmäßigkeit der Datenverarbeitung wird von der Verantwortung für die Richtigkeit der gespeicherten Daten abgetrennt und auf eine zentrale Stelle übertra-

gen (z. B. per Rechtsverordnung gemäß § 8 Abs. 2 LDSG oder durch einen öffentlich-rechtlichen Vertrag als partielle Aufgabenübertragung gemäß dem Gesetz über kommunale Zusammenarbeit, 34. TB, Tz. 4.1.7).

- Die Verantwortung für die Gewährleistung der Ordnungsmäßigkeit der Datenverarbeitung und die Verantwortung für die Richtigkeit der gespeicherten Daten werden durch einen öffentlich-rechtlichen Vertrag auf eine zentrale Stelle übertragen (§ 18 Abs. 1 des Gesetzes über die kommunale Zusammenarbeit).

Im ersten Fall ist jede Daten verarbeitende Stelle sowohl für die Ordnungsmäßigkeit der Datenverarbeitung als auch für die Richtigkeit der verarbeiteten Daten verantwortlich und erstellt demgemäß die vollständige Verfahrensdokumentation des automatisierten Verfahrens.

Im zweiten Fall wird die Verantwortung der Ordnungsmäßigkeit der Datenverarbeitung auf eine zentrale Stelle übertragen. Die beteiligten Stellen müssen für ihre Verantwortungsbereiche jeweils eine Verfahrensdokumentation erstellen.

Im dritten Fall obliegt die Erstellung der Verfahrensdokumentation derjenigen Stelle, der die Verantwortung für die Ordnungsmäßigkeit der Datenverarbeitung und für die gespeicherten Daten im Wege einer Funktionsübertragung durch einen öffentlich-rechtlichen Vertrag übertragen wurde. Für die übertragende Stelle können bezüglich der Erstellung der Verfahrensdokumentation Mitwirkungspflichten bestehen, die vertraglich festgehalten werden können.

Das ULD erarbeitet zurzeit am Beispiel des automatisierten Verfahrens „KoPers-Kommunen“ die Inhalte einer Verfahrensdokumentation für die beteiligten Stellen (Tz. 4.1.6). Die erarbeiteten Ergebnisse werden veröffentlicht.

Was ist zu tun?

Alle beteiligten Stellen müssen – neben dem Verfahrensverzeichnis – bei dokumentationspflichtigen automatisierten Verfahren nach LDSG und DSVO die Verfahrensbestandteile ihres Verantwortungsbereichs dokumentieren.

6.3.2 pBON

Das Verfahren „pBON“ des Ministeriums für Schule und Berufsbildung ist ein über das Schleswig-Holstein-Gateway zugängliches internetbasiertes Bewerbungsportal. Es dient als zentrale Bewerbungsplattform für den Schuldienst.

Schulleitungen, Schulaufsicht in den Schulämtern sowie das Ministerium für Schule und Berufsbildung können Stellenausschreibungen erstellen, die nach einer Qualitätskontrolle durch die Schulaufsicht oder das Ministerium freigegeben werden und im Portal einzusehen sind. Bewerbungen können zentral über das Portal in elektronischer Form eingereicht werden. Nach einer Qualitätskontrolle durch das Ministerium werden die Bewerbungen innerhalb des Bewerbungsportals freigegeben und können dann dezentral durch Schulleitungen, Schulämter und das Ministerium eingesehen werden. Sind inhaltliche Nachlieferungen erforderlich oder Fragen offen, so wird die sich bewerbende Person informiert und kann ihre Bewerbungsunterlagen online vervollständigen und zur erneuten Qualitätskontrolle einreichen.

Je nach Art der Bewerbung – schulgenau, regional begrenzt oder landesweit – bestehen in die freigegebenen Bewerbungen schulgenaue, regional begrenzte oder landessweite Einsichtsmöglichkeiten durch die Schulleitungen und die Schulämter. Eine Differenzierung der Einsichtsrechte nach Schularten ist nicht vorgesehen, da Bewerbungen, insbesondere im Bereich der Vertretungen, auch schulartübergreifend erfolgen.

Mithilfe des Verfahrens können Schulleitungen auch Einladungsschreiben und Einstellungsverfü-

gungen erstellen, die dann in Papierform weiterbearbeitet werden. Es besteht die Möglichkeit eines eingeschränkten Datenexports für die Schulleitungen, um beispielsweise Serienbriefe erstellen zu können.

Das Verfahren pBON wird bei Dataport betrieben. Für die Bewerberinnen und Bewerber gibt es einen sogenannten Frontend-Bereich, der über das Internet erreichbar ist. Die Schulen, Schulverwaltungen und das Ministerium kommunizieren hingegen über das Landesnetz mit den Verfahrenskomponenten. Die Rechtesteuerung für diese Nutzer erfolgt innerhalb von pBON, das dazu Nutzerkonten aus dem Active Directory des Landes kopiert und um die pBON-interne Rechteverwaltung ergänzt.

Im Rahmen einer Vorabkontrolle untersuchte das ULD, inwieweit die Einsichtsrechte der Schulen und die Exportfunktion dazu führen, dass das Verfahren als gemeinsames Verfahren von Schulen, Schulämtern und dem Ministerium zu betrachten ist. Angesichts des vergleichsweise geringen Funktionsumfangs für Schulleitungen innerhalb des Verfahrens pBON und der ausschließlichen Steuerung des Verfahrens durch das Ministerium kann man nicht von einem gemeinsamen Verfahren sprechen. Die vollständige Verantwortung für die Ordnungsmäßigkeit des Verfahrens liegt also beim Ministerium für Schule und Berufsbildung.

Was ist zu tun?

Das Ministerium für Schule und Berufsbildung muss die Dokumentation des Verfahrens vervollständigen.

07

KERNPUNKTE

Internetdienstleister

Internetfernsehen

7 Neue Medien

7.1 Verantwortlichkeit für Facebook-Fanpages

Der Konflikt um die datenschutzrechtliche Verantwortlichkeit der Betreiber von Facebook-Fanpages für die bei Facebook in den USA erfolgende Verarbeitung von Nutzungsdaten (34. TB, Tz. 7.1.1) geht in die nächste Runde. Das Verwaltungsgericht Schleswig hat Klagen von Webseitenbetreibern im Oktober 2013 gegen Untersagungsverfügungen des ULD stattgegeben. Im September 2014 bestätigte das Schleswig-Holsteinische Oberverwaltungsgericht (OVG) in einem Musterverfahren diese Urteile und entschied, dass allein Facebook als verantwortliche Stelle anzusehen sei. Das ULD hat gegen die Entscheidung des OVG beim Bundesverwaltungsgericht (BVerwG) Revision eingelegt. Bei der von diesem Gericht zu klärenden Rechtsfrage sind aus Sicht des ULD folgende Punkte von Bedeutung:

- Das OVG ignoriert, dass die von Facebook auf den Rechnern der Seitenbesucher gesetzten Cookies, mit denen die Nutzungsdaten erhoben werden, eine zentrale Rolle im Geschäftskonzept Facebooks spielen. Insbesondere die langfristig gespeicherten Cookies (datr- und fr-Cookie) liefern Facebook personalisierbare Daten über die Internetnutzung. Wenn die Nutzer durch ihre Browsereinstellungen die Annahme von Cookies nicht verweigern oder diese löschen, bleiben die Cookies bis zu zwei Jahren auf den Computern, Smartphones oder Tablets erhalten. Über diesen Zeitraum kann Facebook die markierten Systeme umfassend und weit über die eigene Plattform hinaus wiedererkennen und so das Verhalten der betroffenen Nutzer im Internet detailgenau erfassen.
- Indem die Instanzgerichte zwischen der Bereitstellung von Webinhalten durch die Betreiber der Fanpages und der Verarbeitung der Nutzungsdaten durch Facebook sowie der Übermittlung der durch Facebook anonymisierten Nutzungsstatistik differenzieren, übersehen sie, dass darin ein einheitlicher technischer Vorgang liegt, auf den sich Fanpage-Betreiber und Facebook vertraglich geeinigt haben. Ohne die Inhalte der Fanpage würden die Nutzenden keine Nutzungsdaten hinterlassen, die Facebook zur Profilbildung und Werbeeinblendung verwendet.
- Die datenschutzrechtlichen Regelungen zur Verantwortlichkeit gelten einheitlich für öffentliche und nicht öffentliche Stellen. Das OVG berücksichtigt nicht ausreichend die Bindung öffentlicher Stellen an die Grundrechte der Nutzer. Auch öffentliche Stellen, welche entsprechende Fanpages betreiben, tragen eine Verantwortlichkeit dafür, dass Facebook beim Seitenbesuch durch Nutzer deren Daten erhebt und verarbeitet. Dies gilt besonders für sensible Bereiche, etwa Schulen, wo Kinder angesprochen werden, oder die Polizei, wo fahndungsrelevante Daten ausgetauscht werden. Auch in diesen Fällen entstehen Kommunikations- und Nutzungsdaten bei der US-amerikanischen Firma Facebook. Wegen ihrer Grundrechtsbindung müssen öffentliche Stellen von einer Nutzung von Facebook absehen (34. TB, Tz. 1.5).
- Beide Instanzen leugneten entgegen den realen Verhältnissen, dass die Fanpage-Betreiber und Facebook gemeinsam über die Zwecke und Mittel der Datenverarbeitung entscheiden und ihnen deshalb nach den europarechtlichen Vorgaben eine gemeinsame Verantwortlichkeit für die Nutzerdatenverarbeitung zukommt. Die Fanpage-Betreiber verfolgen mit der Ansprache der Nutzer über ihren Webauftritt Werbezwecke. Zum anderen möchten sie ihr Webangebot den Bedürfnissen der Seitenbesucher anpassen und optimieren, wozu die von Facebook abgelieferte anonymisierte Nutzungsstatistik „Insights“ einen wesentlichen Beitrag leistet. Mit dem Anlegen der Fanpage steuern und initiieren sie die Erhebung und Verarbeitung der Nutzungsdaten durch Facebook, wodurch ein zentrales Mittel in den Verarbeitungsprozess eingeführt wird.
- Fanpage-Betreiber haben als Diensteanbieter durch technisch-organisatorische Vorkehrungen sicherzustellen, dass die personenbezogenen Daten über die Nutzung verschiedener Telemedien durch denselben Nutzer nicht zusammengeführt werden.

Damit will das deutsche Telemediengesetz die Zusammenführung von Daten zu Nutzungsprofilen verhindern. Individualisierte Nutzungsdaten dürfen nur für Abrechnungszwecke verwendet werden. Die Fanpage-Betreiber verfolgen keine Abrechnungszwecke, sondern allenfalls den Zweck der Werbung und den Zweck der bedarfsgerechten Gestaltung ihres Webauftritts. Gleichwohl lassen sie eine Verbindung der Nutzungsdaten, z. B. IP-Adresse und Cookie-Informationen, mit den Anmeldedaten der Nutzer, also z. B. Vorname, Familienname, Geburtsdatum, Geschlecht, durch Facebook zu und verletzen damit die Anforderungen zum technisch-organisatorischen Datenschutz.

- Für Facebook gilt deutsches Datenschutzrecht. Dieser Schluss ergibt sich aus den Ausführungen, die der Europäische Gerichtshof (EuGH) in einem im Mai 2014 ergangenen Urteil zu Google gemacht hat. Die Facebook Inc. muss deutsches Datenschutzrecht beachten, denn sie betreibt in Deutschland mit der Facebook Germany GmbH, Großer Burstah 50-52, 20457 Hamburg, eine Niederlassung. Die Facebook Germany GmbH wurde nach den Angaben von Facebook im Jahr 2009 in Hamburg eröffnet, um die Zusammenarbeit von Marken und Unternehmen mit Kunden oder Fans auf Facebook zu verbessern. Die Facebook Germany GmbH unterstützt durch Werbe- und Marketingmaßnahmen die Nutzung der Facebook-Dienste. Diese Tätigkeit genügt, um die Facebook Germany GmbH als Niederlassung zu qualifizieren. Es ist hierfür nicht notwendig, dass die Facebook Germany GmbH selbst personenbezogene Daten verarbeitet, so wie dies noch das Schleswig-Holsteinische OVG in einer Entscheidung vom April 2013 angenommen hatte.

Die Umsetzung des Facebook-Fanpage-Urteils des OVG führt zu der absurden Konsequenz, dass Webseitenbetreiber generell – egal ob diese öffentlich oder privatwirtschaftlich organisiert sind – auf vertraglicher Basis von einer offenkundig rechtswidrigen Datenverarbeitung profitieren können, ohne dass ihnen hierfür ein datenschutzrechtlicher Vorwurf gemacht werden kann. Zu der zugrunde liegenden Rechtsfrage wird nun das BVerwG entscheiden.

Die Entscheidung des OVG Schleswig und die hierzu veröffentlichte Presseerklärung des ULD sind abrufbar unter:

https://www.datenschutzzentrum.de/artikel/770-.html

Die Entscheidung des VG Schleswig und die hierzu veröffentlichte Presseerklärung des ULD sind abrufbar unter:

https://www.datenschutzzentrum.de/artikel/769-.html

Was ist zu tun?

Es ist zu hoffen, dass bald Rechtsklarheit in der Form hergestellt wird, dass deutsche Stellen sich ihrer datenschutzrechtlichen Verantwortlichkeit nicht dadurch entledigen können, dass sie ausländische Portale nutzen.

7.2 Klarnamenpflicht bei Facebook

Nach mehreren Beschwerden von Facebook-Nutzenden, die sich bei dem sozialen Netzwerk nicht unter ihrem wirklichen Namen, dem Klarnamen, sondern unter einem Pseudonym angemeldet hatten, erließ das ULD sofort vollziehbare Verfügungen gegen Facebook Ltd. in Irland und Facebook Inc. in den USA, weil das Netzwerk deren Konten sperrte. Diese weltweite Praxis verstößt gegen deutsches Recht, das im Telemediengesetz (TMG) vorsieht, dass Diensteanbieter verpflichtet sind, die Nutzung „anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist“. Das von Facebook angerufene Verwaltungsgericht (VG) Schleswig gab den beiden Unternehmen recht mit der Behauptung, nicht deutsches, sondern irisches Recht sei anwendbar.

Es spiele keine Rolle, dass Facebook in Deutschland eine Niederlassung hat und den deutschen Markt anspricht (34. TB, Tz. 7.1.3). Mit Beschlüssen vom April 2013 wurden die Entscheidungen des VG Schleswig vom Schleswig-Holsteinischen Oberverwaltungsgericht (OVG) auf die Beschwerden des ULD hin voll bestätigt.

https://www.datenschutzzentrum.de/facebook/20130422-ovg-beschluss-facebook-inc.pdf

https://www.datenschutzzentrum.de/facebook/20130422-ovg-beschluss-facebook.pdf

Die Anwendung der nicht anfechtbaren Beschlüsse des OVG hätten zur Folge, dass keine deutsche Aufsichtsbehörde gegen US-Unternehmen, deren wesentliche Datenverarbeitung in den USA erfolgt und die in Irland ihre europäische Hauptniederlassung haben, nach deutschem Datenschutzrecht vorgehen könnte. Die Entscheidungen haben glücklicherweise nach dem Google-Urteil des Europäischen Gerichtshofes (EuGH) vom April 2014 keinen rechtlichen Bestand mehr. Während die Verwaltungsgerichtsbarkeit des Landes die vom ULD vorgetragene grundrechtliche Begründung seiner Bescheide nicht aufgegriffen hatte, entschied der EuGH, dass das Marktortprinzip gilt, also bei Bestehen einer Niederlassung in Deutschland deutsches Recht beachtet werden muss. Dies hat zur Folge, dass die weiterhin von Facebook praktizierte Klarnamenpflicht rechtswidrig ist. Tatsächlich sperrt das Unternehmen weiterhin Konten, die unter einem Pseudonym angemeldet sind.

Was ist zu tun?

Das ULD wird gemeinsam mit den anderen deutschen Aufsichtsbehörden eine Strategie entwickeln, um Facebook zu einem rechtmäßigen Handeln zu bewegen.

7.3 Microsoft Office 365 – eine Bürolösung mit fehlenden Antworten

Mit Microsoft Office 365 sollen dem Nutzer Cloud-basierte Dienste, vor allem fremde Serverkapazitäten zur Verfügung gestellt werden. Fragen zum technisch-organisatorischen Datenschutz blieben bis heute leider unbeantwortet.

Mithilfe von Office 365 kann der Nutzer auf seine Anwendungen und Dateien von jedem Standort aus mit beliebiger Hardware zugreifen, wobei die Anwendungen durch automatische Updates immer aktuell bleiben. E-Mail- und Kalenderfunktionen, ein großer Datenspeicher, die Möglichkeit, Videokonferenzen durchzuführen, und ein moderner Standard zur Bearbeitung von Office-Dokumenten gibt es inklusive. Für Privatnutzer, Studierende und Firmen unterschiedlicher Größe stehen verschiedene Lizenzvarianten zur Verfügung, die sich hinsichtlich des Funktionsumfangs der Software (z. B. nur online oder auch lokal installierbar), Zahlungsweise (Festpreis oder monatliche Kosten) und Integration in die bestehende Firmeninfrastruktur unterscheiden. Die bisher ausschließlich lokal installierte Office-Software wird jetzt unter Office 365 vermarktet, die automatisch Verbindung zum Internet aufnimmt.

Datenschutzrechtlich besonders relevant ist die Nutzung von Office-365-Varianten, die ihre Dateiablage auf Microsoft-Servern realisieren. Als vertragliche Grundlage für Geschäftskunden hat Microsoft die Standardvertragsklauseln 2010/87/EU der Europäischen Kommission verwendet, die bei Inanspruchnahme von Office 365 mit dem Nutzer vereinbart werden. Die Artikel-29-Datenschutzgruppe hat die verwendeten Standardvertragsklauseln geprüft und festgestellt, dass diese mit Ausnahme ihres Anhangs zu den technisch-organisatorischen Sicherheitsanforderungen den Vorgaben der Kommission entsprechen. Ausführungen in dem Anhang wurden von der Artikel-29-Datenschutzgruppe nicht geprüft und unterliegen der Kontrolle der zuständigen Aufsichtsbehörden.

Das ULD nahm mit Microsoft über das Produkt „Office 365“ den Dialog auf und bat um die Übersendung einer prüfbaren Verfahrensdokumentation einschließlich eines Sicherheitskonzepts und um nähere Informationen zu den vorgenommenen Protokollierungen, was das Unternehmen im Sommer 2013 zusagte. Dem ULD wurden seitdem trotz Nachfragen keine der erbetenen Dokumente

übersandt. Es kann deshalb keine Aussage getroffen werden, dass Office 365 beanstandungslos betrieben werden kann.

Das ULD kam im Rahmen seiner Prüfung zu folgenden Ergebnissen:

- Office 365 ist aktuell nicht geeignet, selbst personenbezogene Daten mit normalem Schutzbedarf datenschutzkonform zu verarbeiten. Das ULD müsste den Einsatz von Office 365 durch Stellen in Schleswig-Holstein in der aktuellen Form beanstanden. Für einen Einsatz bei öffentlichen und nicht öffentlichen Stellen in Schleswig-Holstein sind durch die verantwortlichen Daten verarbeitenden Stellen Pflichten abgefordert, denen sie mit dem Standardangebot von Microsoft genügen können.
- Das Produkt „Office 365“ muss, um datenschutzkonform eingesetzt werden zu können, durch eine vom Kunden auswertbare Protokollierung aller diesen betreffenden administrativen Änderungen und jeder Verarbeitung von durch diesen verwendeten Daten ergänzt werden. Die Protokollierung muss sowohl durch den Kunden veranlasste Veränderungen – direkt über das Webfrontend oder per Auftrag an Microsoft – als auch durch Microsoft durchgeführte Änderungen umfassen. Die Protokollierung sollte direkt am jeweiligen Objekt einsehbar sein, z. B. durch Rechtsklick auf eine Datei. Alternativ ist auch eine zentrale Protokollauswertung denkbar. Die Berechtigung zur Einsichtnahme in die Protokolldaten muss explizit an einzelne Personen vergeben werden können. Das Durchführen einer Auswertung muss wiederum zu einem Protokolleintrag führen.
- Die Aufbewahrungszeit der Protokolldaten muss durch den Kunden konfigurierbar sein. Der Mechanismus zur Protokollierung und Auswertung muss explizit Bestandteil einer unabhängigen, regelmäßigen Begutachtung sein, deren Ergebnisse den Anwendern bekannt gemacht werden müssen.
- Microsoft muss die für den Kunden wesentlichen Sicherheits- und Datenschutzmaßnahmen bei Office 365 und das bei Microsoft vorhandene Sicherheits- und Datenschutzmanagement so beschreiben, dass diesem und den Datenschutzaufsichtsbehörden eine eigene Prüfung und Bewertung des Sicherheits- und Datenschutzniveaus möglich ist. Die Dokumentation muss eine Vorstellung zu den für die Diensterbringung beteiligten Standorten, zu Personal, Systemen und Netzverbindungen geben sowie die diesbezüglich getroffenen Sicherheits- und Datenschutzmaßnahmen nachvollziehbar beschreiben.
- Für Daten mit erhöhtem Schutzbedarf, z. B. Daten mit Berufs- oder Amtsgeheimnissen, Personalaktendaten sowie Steuerdaten, muss Microsoft eine Lösung beschreiben, wie durch eine Verschlüsselung, z. B. auf Basis des Einsatzes der in den Microsoft Rights Management Services (RMS) vorhandenen Lösung, eine Kenntnisnahme dieser Daten durch Microsoft ausgeschlossen werden kann. In einzelnen Nutzungsszenarien lässt sich für die Daten verarbeitenden Stellen durch den Einsatz von Verschlüsselung und Pseudonymisierung der personenbezogenen Daten bei der Nutzung von Office 365 ein ausreichendes Sicherheits- und Datenschutzniveau erreichen. Dies muss jedoch im Einzelfall geprüft werden. Generell ist nicht von der Möglichkeit einer beanstandungsfreien Nutzung von Office 365 auszugehen.

Was ist zu tun?

Öffentliche und nicht öffentliche Stellen in Schleswig-Holstein müssen leider derzeit auf das wegen seiner Funktionalität zweifellos attraktive Angebot Office 365 von Microsoft verzichten.

7.4 Financial Blocking beim Online-Glücksspiel

Im Jahr 2013 wandten sich Internet- und Finanzdienstleister an das ULD mit der Frage, inwieweit die im Glücksspielstaatsvertrag vorgesehene Regelung zum Unterbinden von Zahlungen für unerlaubtes Online-Glücksspiel – das sogenannte Financial Blocking – mit Datenschutzrecht zu vereinbaren ist.

Schleswig-Holstein ist mit seinem Glücksspielgesetz in diesem Bereich zunächst einen eigenen Weg gegangen. Doch hat das Land im Frühjahr 2013 beschlossen, dem Glücksspielstaatsvertrag der anderen 15 Bundesländer beizutreten. Darin wird der Glücksspielaufsicht erlaubt, Beteiligten, insbesondere Kredit- und Finanzdienstleistungsinstituten, nach vorheriger Bekanntgabe unerlaubter Online-Glücksspielangebote die Mitwirkung durch Zahlungsabwicklung zu untersagen.

Voraussetzung für die wirksame Untersagung ist, dass bei den adressierten Finanz- und Internetdienstleistern die Daten vorliegen, mit denen sie effektiv zwischen unzulässigem und erlaubtem Online-Glücksspiel unterscheiden können. Da der Glücksspielmarkt nicht nur in Deutschland, sondern in Europa zersplittert ist und bei Online-Glücksspielen und den damit verbundenen Finanztransaktionen nationale Grenzen keine wesentliche Rolle spielen, können Spiele an einem Ort zulässig, an einem anderen verboten sein. Um das Financial Blocking rechtskonform durchführen zu können, müssen die Finanz- und Internetdienstleister wissen, wo sich der Spieler beim Spiel aufhält und dass die Zahlung sich auf ein verbotenes Glücksspiel bezieht. Dies ist aber Finanztransaktionen – egal ob sie über das Internet oder auf anderem Wege erfolgen – nicht anzusehen. Zwar kann bei Kreditkartenzahlungen erkannt werden, dass ein Empfänger Glücksspielanbieter ist. Weiter gehende Daten zur Erkennung eines unzulässigen Online-Glücksspiels liegen den Finanz- und Internetdienstleistern aber nicht vor.

Eine datenschutzrechtliche Untersuchung des Glücksspielstaatsvertrags ergab, dass Dienstleister die bei ihnen vorhandenen Daten für ein Financial Blocking verwenden dürfen. Darüber hinausgehende Befugnisse zur Datenverarbeitung, insbesondere die eigenständige Datenbeschaffung von Lokalisierungsdaten, können aber rechtlich nicht abgeleitet werden. Eine Vorratsdatenerhebung zu allen Internetnutzenden, um bei illegalen Glücksspielern die unzulässige Zahlungsaktion zu erkennen, wäre unverhältnismäßig. Ebenso wenig besteht eine Befugnis für Servicebetreiber, Identifizierungsdaten an Finanzdienstleister oder an andere Stellen weiterzugeben. Dies hat zur Folge, dass die im Staatsvertrag vorgesehene Maßnahme des Financial Blocking nicht effektiv umgesetzt werden kann. Die Stellungnahme des ULD ist im Internet abzurufen.

https://www.datenschutzzentrum.de/artikel/860-.html

Was ist zu tun?

Das Land Schleswig-Holstein sollte sich dafür einsetzen, dass der Glücksspielstaatsvertrag so geändert wird, dass unzulässiges Glücksspiel bekämpft werden kann, ohne gegen Datenschutzvorschriften zu verstoßen.

7.5 Smart-TV

Ende 2013 bat der Medienrat der Medienanstalt Hamburg-Schleswig-Holstein (MA HSH) das ULD um eine Beratung zum Thema „Internetfernsehen und Datenschutz“. Daraus entstand eine Kooperation, aus der das Positionspapier „Internet-TV und Datenschutz – ein Annäherungsversuch“ entstand. Das digitale, über das Netz erreichbare Fernsehgerät eröffnet die Möglichkeit einer zweidirektionalen Kommunikation, aus der Sender, Portal- und Diensteanbieter sowie TV-Hersteller in die Wohn- und Schlafzimmer eindringen und nicht nur die Sehgewohnheiten ausspionieren können, ohne dass die Betroffenen dies wissen, geschweige denn dies unterbinden können. Mit in den Bildschirm

eingebauten Mikrofonen und Kameras kann die Zuschauerüberwachung weiter perfektioniert werden.

https://www.datenschutzzentrum.de/artikel/619-.html

Dem Thema nahm sich der Düsseldorfer Kreis in Kooperation mit den Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten mit einer Entschließung an, die von der Konferenz der Direktoren der Medienanstalten unterstützt wird.

https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2014/Smartes_Fernsehen_nur_mit_smartem_Datenschutz/Beschluss_Smart_TV.pdf

Das Thema ist inzwischen allen Beteiligten bekannt. Ein öffentlich-rechtlicher Sender hat direkt reagiert und sein Nutzungstracking mithilfe von Google Analytics eingestellt. Viele Datenflüsse spielen sich aber weiterhin im Verborgenen ab; deren Zwecke sind unklar. Ein riesiges neues Feld tut sich für den Datenschutz auf, das nach einer umfassenden Bestandsaufnahme ruft.

Was ist zu tun?

Nach einer systematischen Sachverhaltsaufklärung bedarf es eines gemeinsamen Vorgehens von Datenschützern, Medienanstalten und Sendern zur Festlegung datenschutzkonformer Standards beim Internetfernsehen.

7.6 Rundfunkänderungsstaatsvertrag

Im 15. Rundfunkänderungsstaatsvertrag (RÄStV) wurde die bisherige Rundfunkgebühr durch einen Beitrag abgelöst. Die dabei getroffenen Regelungen ermöglichen ein Übermaß an Datenverarbeitung (34. TB, Tz. 7.4). Diese von sämtlichen Datenschutzbeauftragten geteilte Kritik stieß auf offene Ohren beim Landtag Schleswig-Holstein und veranlasste letztendlich die Rundfunkanstalten, die Praxis der Datenverarbeitung bei der Beitragserhebung durch untergesetzliche Festlegungen im Sinne der Datenschutzkritik zu begrenzen. Das ULD forderte im Einklang mit den anderen Datenschutzbeauftragten, bei der nächsten Rundfunkstaatsvertragsänderung die bestehenden ausufernden Regelungen auf das unbedingt Erforderliche zurückzuführen. Beim vorgelegten Entwurf eines 16. RÄStV wurde zwar das Beitragsrecht angefasst, doch die Forderung der Datenschützer ignoriert. Mit deren Umsetzung würde normativ dem Grundrechtsschutz entsprochen und zugleich das Recht der Praxis weitgehend angepasst. Nur so kann verhindert werden, dass künftig durch eine Änderung der Praxis eine übermäßige und damit grundrechtswidrige Datenverarbeitung im Rahmen der Beitragserhebung stattfindet.

08

KERNPUNKTE

Big Data und Scoring

Soziale Netzwerke

Innere Sicherheit

8 Modellprojekte und Studien

Neben seiner Prüf- und Beratungstätigkeit beteiligt sich das ULD an drittmittelfinanzierten Projekten und Studien mit besonderem Datenschutzbezug. Ziel ist es, über das gesetzlich notwendige Mindestmaß an Datenschutz hinauszugehen und besonders „datenschutzfördernde Technik" zu entwickeln, die den Bürgerinnen und Bürgern in Schleswig-Holstein zugutekommt. Durch diese Aktivitäten profitiert das Land finanziell und in Form von Kompetenzbündelung im Bereich Datenschutz (Tz. 8.1–8.7). Die vielfältigen Projektbeteiligungen zeigen, dass nationale und internationale Forschungseinrichtungen das Datenschutz-Know-how aus Schleswig-Holstein als einen wichtigen Bestandteil der technischen Entwicklung sehen.

Die Projekte werden im ULD durch das Innovationszentrum Datenschutz & Datensicherheit (ULD-i) koordiniert, das interessierten schleswig-holsteinischen Unternehmen und Hochschulen für die Integration von Datenschutz und Datensicherheit in ihre Projekte und Produkte zur Verfügung steht. Bei der Gestaltung von Systemen sollen Datenschutzanforderungen von Anfang an einbezogen werden; dieses Grundanliegen des ULD wird voraussichtlich mit der kommenden EU-DSGVO Pflicht für alle verantwortlichen Stellen (Tz. 2.2) und ist deshalb ein Schwerpunkt der Projektarbeit des ULD. Im Berichtszeitraum 2013-2014 hat das ULD sich an Projekten zu vielen aktuellen und wichtigen Themen beteiligt: Grundlagenforschung zu Privatheit (Tz. 8.1), Identitätenmanagement (Tz. 8.2), Cloud Computing (Tz. 8.3), Cybersicherheit (Tz. 8.4), Big Data (Tz. 8.5), Sicherheit (Tz. 8.6) und Betroffenenrechte (Tz. 8.7).

http://www.uld-i.de/

8.1 Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt

Das gemeinsame Erarbeiten von Lösungen in einem interdisziplinären Team bewährt sich in der Projektarbeit des ULD. Zwar prallen manchmal die Sichten von Recht, Informatik, Betriebswirtschaft und Sozialwissenschaften aufeinander, doch dann wird gemeinsam um tragfähige Lösungen gerungen, in denen die Grundrechte hochgehalten werden. Der interdisziplinäre Diskurs steht auch im Vordergrund in dem vom Bundesforschungsministerium geförderten „Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt" (kurz: Privacy-Forum).

Seit Ende 2013 ist das auf drei Jahre angelegte Privacy-Forum aktiv; das ULD kam im Herbst 2014 als Projektpartner hinzu. Wissenschaftler aus der Ethik, Informatik, Jura, Ökonomie, Politologie, Psychologie und Soziologie arbeiten interdisziplinär zum Thema „Privatheit in der digitalen Welt" an einem gemeinsamen Verständnis und Konzepten für eine (Neu-)Bestimmung und Gewährleistung der informationellen Selbstbestimmung. Die Projektpartner sind sowohl an gemeinsamen Themen als auch an individuellen Schwerpunkten tätig. Die „White Paper" zu Selbstdatenschutz und zum versteckten Internet, die über die Projekt-Webseite veröffentlicht sind, richten sich an interessierte Bürgerinnen und Bürger, können aber auch als Grundlage für politische Entscheidungen dienen. Weitere Ausarbeitungen mit unterschiedlichem Adressatenkreis werden folgen.

Das ULD wirkt an dem Forum als Schnittstelle zwischen der Praxis der Datenschutzaufsicht und der nationalen und europäischen Privacy-Forschung mit. Gerade angesichts der europäischen Datenschutzreform (Tz. 2.2) will sich das ULD gestaltend einbringen, um die Konzepte wie „Privacy by Design", „Privacy by Default" und Datenschutzfolgenabschätzung zu konkretisieren. Damit sollen Entwickler, einsetzende Stellen, betriebliche Datenschutzbeauftragte, Standardisierungsgremien und Datenschutzbehörden in ihrem Bestreben nach einem guten Privacy-Niveau unterstützt werden.

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

Was ist zu tun?

Der interdisziplinäre Diskurs zu Privacy-Themen muss lösungsorientiert geführt werden, um Wege für die Praxis zu finden.

8.2 eIDs, Identitätenmanagement und Datenschutz

Nutzergesteuertes Identitätenmanagement und vertrauenswürdige elektronische Ausweise (eIDs) sind von großer Bedeutung für die informationelle Selbstbestimmung in der digitalen Welt. Seit vielen Jahren engagiert sich das ULD für datenschutzfördernde Technik zum Identitätenmanagement, die mittlerweile Einsatzreife erlangt hat (Tz. 8.2.1). Trotz einer großen eID-Vielfalt in Europa gibt es leider wenig Datenschutz-Features. Vertrauenswürdige Identitätsvermittler zwischen verschiedenen technischen Systemen können bei geeigneter Gestaltung Nutzende in ihrem Datenschutz unterstützen (Tz. 8.2.2). Diese Forschungsarbeiten sind im größeren Kontext zu betrachten, da auf EU-Ebene im Sommer 2014 die Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt in Kraft getreten ist (Tz. 11.6): Bei der Umsetzung dieser Verordnung sollten die in den Projekten entwickelten Datenschutzkonzepte berücksichtigt werden.

8.2.1 ABC4Trust – vertrauenswürdige digitale Authentisierung im Pilotversuch

Von November 2010 bis Februar 2015 hat das von der Europäischen Kommission geförderte Projekt „ABC4Trust – Attribute-based Credentials for Trust“ unter Beweis gestellt, dass datensparsame Berechtigungsnachweise praxistauglich sind. Die sogenannten Privacy-ABCs ermöglichen eine Authentisierung auch ohne Vorzeigen der Identitätsdaten.

Schon in den EU-Projekten „PRIME – Privacy and Identity Management for Europe“ (26. TB, Tz. 8.5) und PrimeLife (30. TB, Tz. 8.2) hat das ULD zum nutzergesteuerten Identitätenmanagement geforscht, wie sich mit datensparsamen Berechtigungsnachweisen in der digitalen Welt ein Mehr an Datenschutz erreichen lässt. Diese kryptografischen Techniken sind mittlerweile unter dem Begriff „Privacy-ABCs“ bekannt.

Um für diese Datenschutztechniken den Weg von der Forschung in die Praxis zu ebnen, beteiligte sich das ULD am EU-Projekt ABC4Trust (34. TB, Tz. 8.2), in dem die Erprobung dieser Privacy-ABCs in zwei Pilotversuchen im Mittelpunkt stand: in einem Kommunikationsnetzwerk an einer schwedischen Schule und in einem Kursevaluierungssystem an einer griechischen Universität.

Privacy-ABCs

Privacy-ABCs ist die Kurzform von „privacy-enhancing attribute-based credentials“, also ins Deutsche übersetzt: „datenschutzfördernde attributbasierte Berechtigungsnachweise“. Diese Privacy-ABCs vereinigen verschiedene kryptografische Mechanismen, denen gemeinsam ist, dass

1. die Nutzenden bestimmte Eigenschaften nachweisen können, ohne dass sie ihre Identität offenlegen müssen, und

2. diese digitalen Nachweise jedes Mal verschieden aussehen, sodass sie keine Verkettung erlauben und dadurch ein Nachverfolgen der Nutzenden nicht möglich ist.

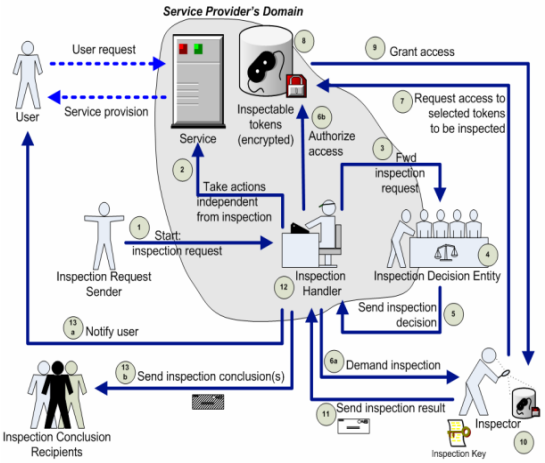
Man kann die Systeme so konfigurieren, dass ein Aufdecken hinterlegter verschlüsselter Daten für bestimmte vorab definierte (Missbrauchs-)Fälle unterstützt wird („Inspection“).

In den Pilotversuchen wurden die Nutzerinnen und Nutzer mit Chipkarten und Lesegeräten ausgestattet. So konnten sie ihre Privacy-ABCs, also ihre Berechtigungsnachweise, von einer Ausgabestelle herunterladen und lokal – auf der Chipkarte – speichern. Für eine Authentisierung zwischen Nutzer und einem Online-Service genügt ein direkter Datenaustausch ohne Einbindung einer weiteren Instanz; die Ausgabestelle ist an diesem Prozess unbeteiligt. Dies wirkt dem Erstellen von heimlichen Nutzungsprofilen entgegen. Je nach Realisierung verfügen die Privacy-ABCs über verschiedene Eigenschaften. Ähnlich dem elektronischen Personalausweis ermöglichen Privacy-ABCs den Nutzenden, nur solche Attribute auszuwählen und zu übertragen, deren Nachweis im Einzelfall erforderlich ist, um Zugang zu einem bestimmten Service zu erhalten. Die gesetzlichen Prinzipien der Datensparsamkeit und der Zweckbindung werden dadurch unterstützt.

An der griechischen Universität von Patras richtete das ABC4Trust-Projekt ein elektronisches Kursevaluierungssystem ein, das es den Studierenden ermöglichte, ihre Vorlesungen anonym zu bewerten. Das System stellte sicher, dass nur Studierende, die eine Mindestanzahl an Vorlesungen besucht hatten, an der Evaluierung teilnehmen konnten.

Mit dem zweiten Pilotversuch wurde erfolgreich ein Kommunikationsnetzwerk für die Schülerinnen und Schüler, Lehrkräfte und Eltern an der schwedischen Norrtullskolan in Söderhamn eingerichtet und betrieben. Die Nutzenden konnten pseudonym und zum Teil sogar anonym diskutieren, Kontakt zu Vertrauenslehrern aufnehmen und Dokumente austauschen.

Die Pseudonymität – statt vollständiger Anonymität – ergibt sich aus dem Umstand, dass in dieser Konfiguration der Privacy-ABCs die Identität der Nutzenden aufgedeckt werden kann, wenn die Inhalte ihrer Chats gegen im Vorfeld dargelegte Regeln verstoßen. Diese „Inspection"-Funktion lässt die Identifizierung der Nutzenden zu, wenn dies z. B. aufgrund gesetzlicher Bestimmungen möglich sein muss. Die Identität des Betroffenen bleibt – ganz im Sinne der Datensparsamkeit – geschützt, solange er sich regelkonform verhält. Weiterhin bietet dieses Vorgehen den Nutzenden Transparenz und Kontrolle über ihre Daten. Die rechtliche und technisch-organisatorische Ausgestaltung des „Inspection"-Prozesses mit definierten Verfahrensschritten (Überblick siehe Abbildung) gehörte neben der allgemeinen datenschutzrechtlichen Begleitung der Pilotentwicklung zu den Hauptaufgaben des ULD.



Quelle: ULD

http://www.abc4trust.eu/

Was ist zu tun?

Nachdem im Projekt ABC4Trust erfolgreich der Einsatz von Privacy-ABCs für zwei Szenarien getestet worden ist, müssen diese Erkenntnisse praktisch umgesetzt werden. Datenschutzfördernde Technik muss die Nutzenden erreichen. Es bedarf daher der gezielten Information von Politik und Wirtschaft über die Funktionsweise und Vorteile der Technologie sowie über geeignete Einsatzfelder. Insbesondere im Rahmen von Online-Abstimmungen, wie etwa Petitionen und Bürgerbegehren, können Privacy-ABCs ein adäquates Datenschutzniveau und die wünschenswerte Vertraulichkeit gewährleisten.

8.2.2 FutureID – vom Passwort zur anwendungsunabhängigen Chipkarte

Nach wie vor wirft die Verwendung sicherheitstechnisch unzureichender Authentisierungsverfahren, etwa mittels Benutzername und Passwort im Internet, große Probleme auf. Dabei sind sicherere Verfahren wie elektronische Ausweisdokumente bereits weitgehend verfügbar. Allerdings hapert es an der Unterstützung solcher elektronischen Identitätsnachweise, kurz eIDs.

Identity Brokerage (Identitätsvermittlung)

Die Verwendung sogenannter Identitätsvermittler (Identity Broker) ermöglicht es Nutzenden, ihre vorhandenen eIDs auch für Dienste zu nutzen, die diese eIDs nicht selbst ausgestellt haben. So könnte mithilfe passender Identitätsvermittler beispielsweise ein elektronischer Personalausweis dazu dienen, einem Arzt in Italien direkten Zugriff auf eine in Frankreich vorgehaltene Patientenakte zu ermöglichen. Zudem ließen sich datenschutzfreundliche attributbasierte Nachweise, z. B. über das Alter einer Person, direkt aus einem geeigneten eID-Ausweis ableiten und über passende Identitätsvermittler auch dann einsetzen, wenn der Diensteanbieter die direkte Verwendung des eID-Ausweises nicht unterstützt. Die Hauptaufgabe der Identitätsvermittler ist dabei die technische Konvertierung der Identitäts- bzw. Attributsnachweise (siehe auch Privacy-ABCs, Tz. 8.2.1) zwischen zwei oder mehr Beteiligten. Dies muss selbstverständlich unter Einhaltung der rechtlichen Rahmenbedingungen erfolgen.

Das Einführen von eID-Systemen ist für Diensteanbieter ein Kostenfaktor, zumal im europäischen Kontext nicht nur ein Verfahren existiert, sondern sich eine heterogene Landschaft von untereinander nicht kompatiblen eID-Systemen entwickelt hat, die einzelne Anbieter kaum vollständig unterstützen könnten. Dies ist der Ausgangspunkt für das von der Europäischen Kommission geförderte Forschungsprojekt „FutureID – Shaping the Future of Electronic Identity“: Seit dem Projektstart im November 2012 forscht das ULD im Verbund mit 18 weiteren Partnern aus ganz Europa daran, geeignete Konzepte und Architekturen zu entwickeln, um die Konvertierung von Identitätsinformationen zwischen verschiedenen eID-Systemen datenschutzgerecht zu ermöglichen.

Die Kernaufgabe des ULD besteht in diesem Projektkontext darin, die datenschutzrechtlichen Anforderungen an ein solches Identitätsvermittlungssystem zu erarbeiten und ihre Einhaltung in den Projektergebnissen zu überprüfen. Im letzten Projektjahr wird das ULD auf Basis der erarbeiteten Anforderungen die FutureID-Pilotanwendungen und die konzipierten Komponenten evaluieren. Die flexible Referenzarchitektur von FutureID ermöglicht eine datenschutzfreundliche Realisierung und kann auch Datenschutztechniken wie Privacy-ABCs (Tz. 8.2.1) unterstützen. Allerdings muss darauf geachtet werden, dass die Identitätsvermittler nicht selbst zu einem Datenschutzrisiko mutieren.

http://www.futureid.eu/

Was ist zu tun?

Datenschutzanforderungen müssen nicht nur national, sondern auch in der europäischen eID-Landschaft realisiert werden. Vertrauenswürdige Identitätsvermittler können hier eine wesentliche Rolle spielen, solange sich datenschutzfreundliche Standards, die ohne weitere Instanzen auskommen, nicht durchgesetzt haben.

8.3 Cloud Computing

Immer mehr Datenverarbeitung findet nicht mehr lokal auf Geräten der Nutzerinnen und Nutzer statt, sondern ausgelagert in der Cloud. Cloud Computing ermöglicht die bedarfsgerechte Verwendung von Ressourcen, die von Cloud-Anbietern zur Verfügung gestellt werden. Damit befinden sich Daten und Programme nicht mehr unmittelbar im Herrschaftsbereich derjenigen, die für die Verarbeitung verantwortlich sind. Das ULD beteiligt sich an mehreren Projekten für mehr Datenschutz in der Cloud, um einem Kontrollverlust über die personenbezogenen Daten entgegenzuwirken. Während im europäischen Kontext an Multi-Cloud-Lösungen geforscht wurde (Tz. 8.3.1), beteiligt sich das ULD national an einem Projekt, das die Einflussbereiche der verschiedenen Dienstleister auf das Minimum beschränken soll (Tz. 8.3.2). Zudem ist das ULD an einem Projekt zur Datenschutzzertifizierung des Cloud Computing beratend beteiligt (Tz. 9.1).

8.3.1 TClouds – Datenschutzfolgenanalyse und mehr Vertrauenswürdigkeit für Cloud-Umgebungen

Ende 2013 wurde das von der EU geförderte Projekt „TClouds – Trustworthy Clouds“ abgeschlossen, das sich mit sicherem und mit den europäischen Datenschutzanforderungen vereinbartem Cloud Computing beschäftigte. Das ULD arbeitet weiterhin daran mit, Cloud-Lösungen im Einklang mit den rechtlichen Vorgaben auf europäischer Ebene zu entwickeln.

Nachdem der Schwerpunkt in der Anfangsphase auf der Zusammenstellung der europäischen rechtlichen Vorgaben und der Entwicklung von Lösungen in Bezug auf Cloud Computing gelegen hatte (34. TB, Tz. 8.4), konzentrierte sich die Arbeit im dritten und letzten Projektjahr auf die Evaluation der entwickelten TClouds-Komponenten und Prototypen. Hierzu erstellte das ULD rechtliche Gutachten zum Einsatz vertrauenswürdiger Cloud-Umgebungen – sowohl in den beiden projektspezifischen Anwendungsgebieten (medizinische Daten und Energiedaten) als auch im Hinblick auf Fragen des internationalen Datenaustausches.

Zudem führte das ULD ein Data Protection Impact Assessment (kurz DPIA) für die Cloud-Lösungen, die im Projekt entstanden sind, durch. Dieses Verfahren ermöglicht es, eine methodisch fundierte Aussage über Auswirkungen der Nutzung von Cloud-Technologien auf den Datenschutz und die informationelle Selbstbestimmung zu treffen. Die Betrachtung umfasst aktuelle wie auch zu erwartende zukünftige Auswirkungen und bietet sich dafür an, die rechtliche Einordnung und Bewertung dieser neuartigen Technologien zu unterstützen.

Data Protection Impact Assessment (Datenschutzfolgenanalyse)

Das Verfahren eines Data Protection Impact Assessment (zu Deutsch etwa: Datenschutzfolgenanalyse) nutzt eine wissenschaftlich fundierte Methodik, um neuartige Technologien hinsichtlich ihrer Auswirkungen auf den Datenschutz und die informationelle Selbstbestimmung einzuordnen. Ausgehend vom zu betrachtenden Anwendungsszenario wird dabei überprüft, welche Konsequenzen sich aus dem Einsatz der jeweils analysierten neuen Technologie ergeben und wie diese zu bewerten sind.

Da die Methodik für ein DPIA nicht genormt ist, entwickelte das ULD nach Auswertung bisheriger Vorschläge ein Verfahren auf Basis der Schutzziele des Datenschutzes (Nichtverkettbarkeit, Transparenz, Intervenierbarkeit) und der IT-Sicherheit (Vertraulichkeit, Integrität, Verfügbarkeit). Diese Methodik ermöglicht es, Anforderungen je nach Anwendungskontext verschieden stark zu gewichten. Der Ansatz hat sich bereits in vielen Projekten bewährt, z. B. in einer Studie zu altersgerechten Assistenzsystemen (33. TB, Tz. 6.3). Ziel ist sowohl die Nachvollziehbarkeit des Vorgehens als auch eine Vergleichbarkeit zwischen DPIAs mit ähnlichem Evaluierungsgegenstand, z. B. über ein IT-System, das sich über die Zeit weiterentwickelt.

Im Projekt TClouds wurde der koordinierte, gleichzeitige Einsatz mehrerer Clouds (Multi-Cloud, Cloud of Clouds) beleuchtet, woraus Vorteile für IT-Sicherheit und Datenschutz resultieren können. Dieser Forschungsansatz sollte weiterverfolgt werden.

http://www.tclouds-project.eu/

Was ist zu tun?

Bei der Konzeption neuer IT-Systeme sollten Datenschutzfolgenanalysen standardmäßig durchgeführt werden. Dabei sind insbesondere die Anforderungen der Nichtverkettbarkeit, der Transparenz und der Intervenierbarkeit zu berücksichtigen.

8.3.2 SPLITCloud – teile und herrsche

„Teile und herrsche" – dieses bereits in der Antike bekannte Prinzip fördert die Beherrschbarkeit großer IT-Systeme und spielt in hochkomplexen Technologiefeldern wie dem Cloud Computing eine große Rolle. Denn hier greifen viele verschiedene Akteure mit jeweils ganz eigenen Interessen auf dasselbe Cloud-System zu.

Der Cloud-Anbieter betreibt etwa die Server-Hardware, die er seinen Kunden, den Cloud-Nutzern, bereitstellt, die wiederum selbst Dienstanbieter sind. Diese implementieren ihre anwendungsspezifischen Dienste auf diesen Rechnern und bedienen damit Anfragen ihrer Dienstnutzer. In diesem Spannungsfeld kommt es häufig zu unklaren Situationen hinsichtlich des Verschuldens und der Verantwortung. Die technische Administration eines solchen Cloud-Systems ist komplex. Sowohl der Cloud-Anbieter als auch der Dienstanbieter haben Interesse daran, administrative Tätigkeiten wie die Installation aktueller Sicherheitsupdates in ihren Systemen durchzuführen. Folglich bedarf es administrativer Zugriffsrechte für beide Parteien. Dies wiederum wirft viele rechtliche Fragestellungen auf, besonders bei Konstellationen mit Partnern aus verschiedenen Ländern und legislativen Domänen.

Im Rahmen des vom Bundesministerium für Bildung und Forschung geförderten Projekts „SPLITCloud" untersucht das ULD zusammen mit vier weiteren nationalen Partnern, wie sich dieses fundamentale Dilemma des sicheren und rechtskonformen Einsatzes von Cloud-Computing-Technologien lösen lässt. Im Fokus der Betrachtung steht dabei eine innovative Lösung zur Absicherung von Cloud-Systemen, die vertrauenswürdiges Rechnen (Trusted Computing) auf der Basis kryptografischer Protokolle realisiert.

Trusted Computing

Der Begriff „Trusted Computing" umfasst eine Reihe technischer Maßnahmen, die dazu dienen, die Ausführung von Software auf Computern derart abzusichern, dass nur spezifisch zur Verwendung vorgesehene Programme überhaupt zur Ausführung gebracht werden können. Dies wird über die Verwendung diverser kryptografischer Verfahren erreicht, die zumeist in einem Hardware-Baustein direkt in den betroffenen Computern installiert sind.

Im Kontext des Cloud Computing kann die Verwendung solcher Trusted-Computing-Bausteine gewährleisten, das Basissystem der Cloud-Server derart zu starten und zu betreiben, dass ein administrativer Zugriff auf die Cloud-Server ausschließlich über explizit vorgegebene, wohldefinierte Schnittstellen möglich ist. Im Rahmen des SPLITCloud-Projekts soll diese Technologie weiterentwickelt werden, um eine logische Trennung zwischen den verschiedenen Domänen der Administratoren zu erreichen.

Bei korrektem Einsatz kann diese Technologie es ermöglichen, die administrativen Domänen von

Cloud-Anbieter und Cloud-Nutzer bzw. Diensteanbieter derart zu trennen, dass eine rechtskonforme Unterscheidbarkeit erreicht wird. Ziel des Projekts ist es, diese Fragestellungen zu bearbeiten und ein Konzept zu entwickeln, nach dem die Daten der Nutzer künftig besser gegen Einsichtnahme durch Administratoren geschützt sind.

http://www.vdivde-it.de/KIS/sichere-ikt/sicheres-cloud-computing/splitcloud

Was ist zu tun?

Sofern Unternehmen und Privatpersonen sich entscheiden, ihre Daten in einem Cloud-System zu speichern, müssen sie prüfen, welche Akteure Zugriff darauf haben können. Dabei sollten sie entsprechende Garantien verlangen, die durch technische Maßnahmen abgesichert sind.

8.4 Cybersicherheit und Datenschutz

In der digitalen Welt spielt sich mittlerweile ein Großteil des Lebens ab: Die Nutzerinnen und Nutzer kaufen online ein, buchen Reisen, erledigen Bankgeschäfte, versteigern Waren, kommunizieren mit Freunden und Verwandten, spielen und lernen im Cyberspace, lesen E-Books, reichen die Steuererklärung online ein und nutzen Dienstleistungen des E-Government. Ebenso verlassen sich Firmen und Verwaltungen auf das korrekte Funktionieren der Netze. Cybersicherheit ist aber keinesfalls garantiert; die heutigen Systeme sind verwundbar, und ständig müssen Angriffe abgewehrt werden. Das Ende 2014 von der Bundesregierung beschlossene IT-Sicherheitsgesetz sieht vor, Meldungen zu Sicherheitsvorfällen von Betreibern kritischer Infrastrukturen zusammenzuführen und auszuwerten (Tz. 2.3). Das ULD hat in den Jahren 2012 und 2013 für ähnliche Szenarien untersucht, inwieweit solche Meldungen personenbezogene Daten enthalten können und wie gewährleistet werden kann, dass der Datenschutz der Nutzerinnen und Nutzer nicht auf der Strecke bleibt (Tz. 8.4.1). Ein weiteres Cybersicherheitsprojekt startet Anfang 2015, das auf eine Erhöhung der Nutzersensibilität für Phishing-Angriffe zielt (Tz. 8.4.2).

8.4.1 MonIKA – Cybersicherheit und Anonymisierung

Bei der Bekämpfung von Botnetzen oder bei der Identifikation und Reduzierung von Spam-Mails spielen heutzutage kollaborative Systeme eine wichtige Rolle. Bei solchen Systemen versuchen mehrere Diensteanbieter, z. B. Internetprovider oder E-Mail-Anbieter, durch gezielten Austausch relevanter Informationen gemeinsam zu einer Erfassung der Lage im gesamten Verbund zu kommen.

So können beispielsweise Muster aus bereits identifizierten Spam-Mail-Kampagnen zwischen den Verbundpartnern ausgetauscht werden, um zukünftige E-Mails derselben Spam-Kampagne effektiver auszufiltern. Ein Anwendungsgebiet kollaborativer Sicherheitssysteme liegt im Umfeld größerer Unternehmensverbünde (Enterprise Networks), bei denen verschiedene Unternehmen mit starken Abhängigkeiten untereinander, z. B. Zulieferer und Produzenten, zusammenarbeiten, um sich gemeinschaftlich gegen Angriffe auf ihre – oft intern vernetzte – IT-Struktur zu wehren. Auch hier werden Informationen zu digitalen Einbruchsversuchen und ungewöhnlichem Netzverhalten untereinander ausgetauscht, um groß angelegte Angriffsversuche frühzeitig zu erkennen und zu unterbinden.

Der hierbei erfolgende Datenaustausch zwischen verschiedenen Akteuren unterliegt jeweils besonderen datenschutzrechtlichen Vorgaben. Das Anfang 2014 erfolgreich abgeschlossene Projekt „MonIKA – Monitoring durch Informationsfusion und Klassifikation zur Anomalieerkennung“ (34. TB,

Tz. 8.9) behandelte unter Mitwirkung des ULD diese Rechtsfragen.

In Zusammenarbeit mit der Rechtswissenschaftlichen Fakultät der Westfälischen Wilhelms-Universität Münster entstanden so zwei rechtliche Gutachten, die drei vorab definierte Szenarien hinsichtlich ihrer Rechtskonformität bewerten. Es zeigte sich, dass kollaborative Systeme zwar einen deutlichen und unverkennbaren Mehrwert gegenüber individuellen Maßnahmen erbringen können, dass sich aber nach aktuellem Stand ein rechtskonformer Betrieb in vielen Szenarien nicht oder nur sehr schwer realisieren lässt.

Für bestimmte Fragestellungen bieten clevere Anonymisierungsverfahren einen Lösungsansatz. Vielfach muss jedoch ein Personenbezug zumindest für einige der beteiligten Stellen bestehen bleiben, wobei mit geschickter Pseudonymisierung Datenschutzrisiken minimiert werden können. Hier besteht weiterer Forschungsbedarf.

Das MonIKA-Gutachten zur datenschutzrechtlichen Zulässigkeit sowie zum Einsatz und zur Gestaltung von Anomalie erkennenden Verfahren in Internetinfrastrukturen ist über die ULD-Webseite abrufbar.

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

Enterprise Monitoring

Der Begriff des Enterprise Monitorings umfasst eine Reihe von Maßnahmen, die in Großkonzernen und in Verbünden kollaborierender Firmen eingesetzt werden, um sich ein Lagebild über den Zustand und die Bedrohungssituation der konzerninternen IT-Systeme zu verschaffen. Hierzu werden Daten über die Nutzung der internen Netze und Internetanbindungen erfasst, aufbereitet, untereinander ausgetauscht und ausgewertet, um ein möglichst umfassendes Gesamtbild der IT-Landschaft im Konzern bzw. im Verbund zu erstellen. Aus den derart gewonnenen Informationen lassen sich geeignete Maßnahmen zur Verbesserung der internen IT-Sicherheit und zur Abwehr laufender und künftiger Angriffe auf die IT-Systeme ableiten. Durch die Betrachtung der Verbundstruktur insgesamt ergeben sich dabei meist deutlich mehr und inhaltlich klarere Informationen über Schwachstellen und laufende Angriffe, als dies bei der Betrachtung einzelner lokaler Netze oder einzelner Firmennetze im Verbund möglich ist.

Was ist zu tun?

Beim Austausch und bei der Auswertung von Meldungen über Sicherheitsvorfälle müssen die Betreiber berücksichtigen, dass diese Daten häufig einen Personenbezug beinhalten. Für die Umsetzung des IT-Sicherheitsgesetzes sind datensparsame Melde- und Analyseverfahren zu definieren.

8.4.2 Stärken des IT-Sicherheitsbewusstseins im Projekt ITS.APT

Um den Grad der IT-Sicherheit bei Betreibern kritischer Infrastrukturen zu prüfen, hat sich die Methode des Penetration Testing bewährt. Ein neues Projekt erweitert die Methode um eine – datenschutzfreundliche – Evaluation des Sicherheitsbewusstseins der Beschäftigten.

Der Faktor Mensch ist nicht nur für Datenschützer ganz wichtig, sondern spielt auch eine wesentliche Rolle, wenn Angreifer versuchen, in ein IT-System einzudringen. Angreifer können z. B. an Passwörter von Beschäftigten gelangen, indem sie sie auf gefälschte Websites locken und dazu bringen, ihre Daten einzugeben. Beschäftigte mit höherem Sicherheitsbewusstsein fallen seltener auf solche Phishing-Angriffe herein.

Das vom Bundesforschungsministerium geförderte Projekt „ITS.APT – IT-Security Awareness Penetration Testing" wird Penetration Testing und die Prüfung des IT-Sicherheitsbewusstseins der Beschäftigten kombinieren und geeignete Schu-

lungsmethoden entwickeln. Natürlich darf dies nicht zulasten des Beschäftigtendatenschutzes gehen. Im Projekt kommen Fachkräfte aus den Disziplinen Informatik, Jura und Psychologie zusammen, um mit Vertretern der Praxis aus dem Anwendungskontext Krankenhaus tragfähige Lösungen zu konzipieren.

Dem ULD kommt die Aufgabe zu, die datenschutzrechtlichen Anforderungen zu erarbeiten und deren Umsetzung auszuwerten.

https://www.datenschutzzentrum.de/projekte/its-apt/

Penetration Testing

Im Auftrag des Betreibers führen spezielle Dienstleister gezielte Angriffe auf ein laufendes IT-System durch. Dabei werden bekannte Schwachstellen der technischen Realisierung durchprobiert. Diese kontrollierten Angriffe dienen der Bewertung des Grads der IT-Sicherheit; erkannte Mängel können behoben werden. Das Sicherheitsbewusstsein der Beschäftigten beim Betreiber wird zumeist beim Penetration Testing nicht betrachtet, ist aber häufig für erfolgreiche Angriffe von großer Bedeutung.

Was ist zu tun?

Mitarbeiterinnen und Mitarbeiter müssen für Angriffe auf IT-Systeme sensibilisiert werden. Bei Verfahren zum Penetration Testing und zum Messen der Sicherheitsrisiken durch den Faktor Mensch müssen die Anforderungen des Beschäftigtendatenschutzes beachtet werden.

8.5 Big Data, soziale Netzwerke und Datenschutz

„Big Data“ war bis vor Kurzem noch ein wenig konturierter modischer Begriff, den die IT-Wirtschaft zur Werbung für technologisch etwas komplexere Innovationen benutzte. Das Bild hat sich in weniger als einem Jahr grundlegend geändert. Edward Snowden enthüllte, wie Big Data bei den Nachrichtendiensten von den USA und Großbritannien, der NSA und dem GCHQ, für die globale Netzüberwachung genutzt wird (Tz. 2.1). Der Einsatz für Sicherheitsbehörden in Europa erfolgt schon oder steht bevor (Tz. 8.5.3). Kommerziell wird Big Data – nicht nur von Facebook, Google oder Amazon, sondern auch von deutschen Kundenunternehmen – immer mehr eingesetzt (Tz. 8.5.2). Selbst in sensiblen Bereichen wie etwa im Gesundheitswesen wird diese Technik genutzt – nicht nur in den USA. Es gibt also genug Gründe, diese mit Heilsversprechen und Horrorszenarien verknüpfte Technik aus Datenschutzsicht zu entmystifizieren und zu gestalten.

Big Data ist begrifflich nicht klar umrissen. Es ist eine Sammelbezeichnung für umfangreiche, oft unstrukturierte Datenbestände, die zumeist im Rahmen einer Zweitverwertung zusammengeführt, verfügbar gemacht und – auch in Echtzeit – ausgewertet werden. Der Begriff steht für die auf der Grundlage gewaltiger Speicher- und Auswertungskapazitäten mögliche Datenanalyse zur Gewinnung neuer Erkenntnisse, mit denen gesellschaftliche, ökonomische oder politische Ziele realisiert werden können: sparsameres Produzieren und Wirtschaften, bessere Planungen und bessere Abläufe in Organisationen, sinnvolleren Ressourceneinsatz und höhere Transparenz.

Mithilfe der Analysewerkzeuge können oft personenbezogene, kontextübergreifende zeitliche Abläufe und digital erfasste Profile über Aufenthaltsorte, Sozialkontakte, Konsum, Verhalten, Interessen, Gesundheit etc. erstellt werden. Neudeutsche Stichworte sind hierfür Scoring, Tracking, Profiling, Personalizing. Verhaltensweisen können prognostiziert und bei Bedarf manipuliert werden. Möglich sind Diskriminierungsaktionen, indem ganz bestimmten Merkmalsträgern der Zugang zu, der Vertragsabschluss in Bezug auf oder die Nutzung von bestimmten Diensten verwehrt wird. Big Data – im politischen Bereich eingesetzt – wäre ein zentrales Instrument zur Verwirklichung einer digitalen Diktatur.

Big Data hat das ULD nicht nur im Rahmen von Forschungsvorhaben beschäftigt. Es war Thema der Sommerakademie 2013 (Tz. 13) sowie extern angeforderter Vorträge. Big Data muss Anlass zum gesetzgeberischen Tätigwerden sein, sowohl auf europäischer Ebene (Tz. 2.2) als auch in Spezialbereichen wie im Gesundheitswesen (Tz. 4.6.1) oder in Bezug auf Sicherheitsbehörden (Tz. 4.2).

https://www.datenschutzzentrum.de/artikel/212-.html

8.5.1 iGreen

Im Projekt „iGreen" wurden Problembereiche des Datenschutzes in der Landwirtschaft in Form von Beratungsleistungen bearbeitet. In der Landwirtschaft findet inzwischen umfangreiche Datenverarbeitung statt. Landwirtschaftliche Maschinen sind mit GPS und Datenfunk ausgestattet, womit z. B. aktuelle Analysen der Bodenbearbeitung durchgeführt oder Zeit, Ort und Zustand von Gerätschaften überwacht werden. Rückschlüsse lassen sich nicht nur auf den Zustand etwa eines Feldes ziehen, sondern auch auf Arbeitsleistungen und finanzielle Verhältnisse des Agrarunternehmens. Die Hersteller und die ein Verfahren nutzenden Stellen sind dabei gehalten, den Datenschutz zu beachten.

Was ist zu tun?

Der Landwirt muss die Möglichkeit haben, selbst zu entscheiden, welche Daten an wen übermittelt werden. Dies muss für ihn ausreichend transparent und nachvollziehbar sein.

8.5.2 SPHERE – Kundenbeziehungsmanagement in sozialen Medien

Soziale Medien wie Facebook und Twitter, Bewertungsportale und Foren und die dabei anfallenden persönlichen Daten wecken Begehrlichkeiten bei Unternehmen. Sie möchten wissen, wie online über sie gesprochen wird, um ihr Vorgehen danach auszurichten. Vielleicht sind dort potenziell Kunden unterwegs. Gewaltige, scheinbar frei verfügbare Datenmengen aus den Profilen von Nutzern sozialer Netzwerke werden erhoben und ausgewertet. Die Ergebnisse können zu detaillierten Persönlichkeitsprofilen zusammengeführt werden. Diese werden genutzt für die Zusendung von individualisierter Werbung, die Gestaltung des Serviceangebots oder eine persönliche Ansprache auf dem Medium Internet. Meistens geschieht dies ohne Kenntnis der Betroffenen, die in der Regel wegen dieser Unkenntnis an der Ausübung ihrer Rechte gehindert sind. Eine Folge können gewichtige wirtschaftliche Nachteile sein.

Das ULD untersuchte in den vergangenen zwei Jahren im Rahmen des vom Bundesministerium für Bildung und Forschung geförderten Projekts „SPHERE – Shielding Privacy within CRM" datenschutzrechtliche Fragestellungen zum Kundenbeziehungsmanagement in sozialen Medien. Am Projektkonsortium waren ein Hersteller von Kundenbeziehungsmanagement-Software, die bowi GmbH, sowie das Institut für Wirtschaftsinformatik der Universität Leipzig beteiligt.

Kundenbeziehungsmanagement (Customer Relationship Management – CRM) zielt auf die Gewinnung, Beibehaltung und Rückgewinnung von Kunden ab. Wichtige Anwendungsfelder sind das Marketing und der Service. Bei „Social CRM" geht es um die Erhebung von Daten aus sozialen Netzwerken über ihre Speicherung und Zusammenführung in Profilen, ihre Veränderung zu Zahlenwerten, ihre Pseudonymisierung und Anonymisierung bis hin zur Nutzung zu werblichen und nicht werblichen Zwecken.

Ziel des Projekts war die Erstellung einer Software, welche als Komponente in ein CRM-System eingebunden werden kann. Sie soll auf der Grundlage von Parametern einer geplanten CRM-Maßnahme die Betroffenen warnen, falls diese datenschutzrechtlich problematisch ist. Hierfür wurden Fragebögen zu typischen Maßnahmen im CRM erstellt, deren Beantwortung eine allgemeine Risikoanalyse erlaubt. Die Hauptaufgabe des ULD bestand darin, anhand von Anwendungsszenarien die rechtlichen Rahmenbedingungen für einen datenschutzgerechten Betrieb von CRM-Systemen herauszuarbeiten. Im Folgenden werden einige wichtige wiederkehrende Leitlinien der Prüfung dargestellt:

- Daten in sozialen Medien sind oft allgemein zugänglich, allerdings aus Datenschutzgründen nicht frei erhebbar. Mit der Erhebung muss ein legitimer Zweck verfolgt werden. Zweckfreie Datensammlungen sind unzulässig. Ebenfalls verboten ist die Erhebung personenbezogener Daten zu Werbezwecken ohne Einwilligung. Der offenkundig entgegenstehende Wille des Betroffenen, der sich z. B. an herausgehobener Stelle aus dem Nutzerprofil erkennen lässt, ist eine weitere rechtliche Grenze.
- Daten, die ursprünglich allgemein zugänglich waren, können durch Zuspeicherung im CRM-System über die Verkettung zu sensiblen Daten werden, deren Nutzung für die verarbeitende Stelle rechtlich nicht mehr erlaubt ist.
- Daten sollen richtig und überprüfbar sein. Zwar gibt es bei der Erhebung von allgemein zugänglichen Daten keine grundsätzliche Prüfpflicht auf die Richtigkeit im Einzelfall. Eine Nutzung, die in Rechte von Betroffenen eingreift, darf jedoch nur aufgrund von zutreffenden Daten erfolgen. Dies schließt viele nicht einwilligungsbasierte Bewertungsverfahren auf der Basis von Social-Media-Daten aus.
- Die verantwortliche Stelle ist grundsätzlich nicht befugt, öffentlich Auskünfte über personenbezogene Daten mittels sozialer Medien zu erteilen. Eine Übermittlung an eine unbestimmte Anzahl Dritte verstößt oft gegen den Grundsatz der Erforderlichkeit. In der Regel ist nicht einmal sicher, ob eine Person die ist, für die sie sich ausgibt. Eine rechtliche Vermutung, dass es sich bei dem Fragenden um den Kunden handelt, besteht nicht. Selbst wenn das Vorliegen bestimmter personenbezogener Daten im CRM nur bestätigt und der Datenumfang scheinbar nicht erhöht wird, besteht die Gefahr eines Identitätsdiebstahls.

Was ist zu tun?

Hinsichtlich der Nutzung von Internetdaten für CRM muss bei den Verantwortlichen ein Bewusstsein für die Grenzen ihrer Verfügungsbefugnis über die fremden Daten hergestellt werden. CRM-Konzepte, die auf Anonymisierung und, wo dies nicht möglich ist, auf Transparenz gegenüber dem Betroffenen setzen, sind zu entwickeln und zu fördern.

8.5.3 VALCRI – Big Data für die Polizei

Im von der Europäischen Kommission geförderten Projekt VALCRI steht die datenschutzgerechte und ethisch vertretbare Realisierung eines Systems zur visuellen Datenanalyse für kriminalpolizeiliche Erkenntnisgewinnung im Vordergrund.

In dem im Mai 2014 gestarteten Projekt „VALCRI – Visual Analytics for Sense-Making in Criminal Intelligence Analysis“ wirken neben Universitäten und Wirtschaftsunternehmen zwei potenzielle Anwender mit: Polizei aus England und Belgien. Die Arbeit von Kriminalanalysten – nicht nur in diesen beiden Ländern – ist heute davon geprägt, dass sie mithilfe einer rudimentären technischen Ausstattung eine Vielzahl von Verbrechensberichten auswerten müssen, um Ähnlichkeiten im Modus Operandi oder andere Gemeinsamkeiten zu finden. Vor allem im Bereich der organisierten Kriminalität geht es um das Aufdecken und Verstehen komplexer Verbrechensnetzwerke. Das VALCRI-Projekt

zielt darauf ab, verschiedene Technologien und Programme zur Datenvisualisierung und -analyse zu entwickeln und zu testen, um Daten effizienter zu verarbeiten und die Analysten technisch zu unterstützen. Komponenten zur Anonymisierung und zur elektronischen Zugangs- und Zugriffskontrolle sollen datenschutzrechtliche Anforderungen umsetzen.

Der Projektbeitrag des ULD befasst sich mit den grundlegenden Fragen der Datenverarbeitung durch Polizeibehörden: Neue Datenverarbeitungssysteme und die damit verbundenen technischen Möglichkeiten einer schnelleren und einfacheren Verarbeitung einer größeren Anzahl von Daten erfordern eine stetige Neubewertung bestehender Gesetze und ihrer Auslegung. Basierend auf dem Konzept der Schutzziele und dem „Privacy by Design"-Ansatz sollen Datenschutzanforderungen von Anfang an in die Technik integriert werden. Zusätzlich zu technischen Vorkehrungen umfasst das Projekt das Training von Kriminalanalysten an dem neuen System. Das ULD wird sich hier einbringen, um zu gewährleisten, dass technische Datenschutzmaßnahmen durch organisatorische Maßnahmen, wie z. B. Schulungen und interne Datenschutzbeauftragte, ergänzt werden. Ein enger Austausch besteht mit den Projektpartnern, die sich mit ethischen Fragen beschäftigen, sowie mit dem Ethik-Board des Projekts.

Die in dem Projekt gewonnenen Erkenntnisse werden vor allem nach Umgestaltung des europäischen Datenschutzrechts bedeutsam sein, da das Konzept „Privacy by Design" zunehmend eine Rolle spielen wird, beispielsweise im kommenden Datenschutzregelungsrahmen (Tz. 2.2). Der im Projekt zu entwickelnde Prototyp soll ein Beispiel dafür sein, wie sich Datenschutz und effektive Polizeiarbeit in Einklang bringen lassen. Die Arbeit in dem Projekt VALCRI ermöglicht dem ULD, die anstehenden Veränderungen des europäischen Datenschutzrechts im Polizei- und Justizsektor zu begleiten, die sich in Deutschland auswirken werden.

http://www.valcri.org/

Was ist zu tun?

In sensiblen Bereichen wie der Datenverarbeitung durch die Polizei ist es besonders wichtig, dass bei der Auswertung großer Datenmengen Datenschutzanforderungen von Anfang an berücksichtigt werden.

8.5.4 iTESA – Reisewarnungen unterwegs

Analyse von Big Data zum Zwecke der zielgruppengenauen Reisewarnung – unter welchen Bedingungen ist dies erlaubt? Damit beschäftigt sich das ULD im Anfang 2015 gestarteten Projekt „iTESA – intelligent Traveller Early Situation Awareness".

Ziel von iTESA ist es, ein automatisches Frühwarnsystem für Reisende zu entwickeln. In Echtzeit können diese noch vor Reiseantritt vor möglichen Risiken, wie z. B. Epidemien und Naturkatastrophen, entlang der Reiseroute oder am Zielort gewarnt werden. Auf diesem Wege soll es ermöglicht werden, bereits bei der Reiseplanung, vor Reiseantritt, während der Reise und auch in Krisensituationen erforderliche Umbuchungen oder Umdispositionen vorzunehmen. Die Echtzeitwarnung, die den Reisenden beispielsweise auf ihre mobilen Endgeräte gesandt werden kann, soll das Ergebnis einer semantischen Auswertung von Daten aus öffentlichen Quellen sein. Das ULD kümmert sich in dem Projekt um die datenschutzrechtlichen, ethischen und gesellschaftspolitischen Fragen. Zunächst wird iTESA im Bereich des Reisemanagements erprobend eingesetzt; eine spätere Übertragung der im Projekt gewonnenen Erkenntnisse auf andere Gewerbezweige ist möglich.

Was ist zu tun?

Big-Data-Projekte sollten stets nach dem Prinzip „Privacy by Design“ entwickelt werden.

8.6 Sicherheit und Datenschutz

8.6.1 GES-3D – dreidimensionale Gesichtserkennung

Das im Jahr 2012 gestartete Projekt „GES-3D – Multi-Biometrische Gesichtserkennung“ sollte ein Verfahren entwickeln, das die polizeiliche Identifizierung von Straftätern aus tatrelevanten Foto-/Videodaten mittels Abgleich mit 3D-Gesichtsbilddaten ermöglicht (34. TB, Tz. 8.8). Das ULD sollte im Rahmen einer rechtlichen Analyse u. a. die rechtliche Zulässigkeit des Einsatzes als auch die datenschutzrechtlichen Anforderungen an die technische Ausgestaltung eines derartigen Systems untersuchen.

Der Einsatz eines 3D-Gesichtserkennungssystems bringt nicht nur Vorteile, sondern verursacht auch beträchtliche Kontroll- und Überwachungsrisiken für die Bürgerinnen und Bürger. Diesbezüglich wurden auch die im Jahr 2013 bekannt gewordenen Überwachungspraktiken der amerikanischen und britischen Geheimdienste in die Beurteilung einbezogen. Die Analyse der datenschutzrechtlichen Zulässigkeit erfolgte exemplarisch für einige reale Einsatzmöglichkeiten sowohl aus dem öffentlichen als auch aus dem nicht öffentlichen Bereich. Relevant sind für die Zulässigkeit der konkrete Einsatzzweck sowie die technische Ausgestaltung des Systems. Ein Bewertungskriterium für die Zulässigkeit ist bei einem hoheitlich veranlassten Einsatz beispielsweise, ob eine große Menge von unbeteiligten und damit unbescholtenen Bürgern betroffen ist.

Für den Einsatz im nicht öffentlichen Bereich besteht ein breites Spektrum an Einsatzmöglichkeiten. Neben der technischen Ausgestaltung kommt es bei der Antwort auf die Frage nach der Zulässigkeit hier auf die Abwägung der widerstreitenden Interessen der Daten verarbeitenden Stelle und des Betroffenen an. Untersucht wurde diesbezüglich auch, ob wirksam in die mit dem Einsatz des Gesichtserkennungssystems einhergehende Datenverarbeitung eingewilligt werden kann.

Aus den Untersuchungsergebnissen der Analyse ergeben sich Anforderungen sowohl an den Gesetzgeber als auch an die Hersteller und Anwender:

- Aufgabe des Gesetzgebers ist es, der Konzeption neuer Technologien und der daraus entstehenden Einsatzbegehrlichkeiten durch die Entscheidung Rechnung zu tragen, ob und in welchen Grenzen innovative Technologien eingesetzt werden dürfen. Dabei ist zu beachten, dass die verfassungsrechtlichen Grenzen einer uneingeschränkten Nutzung entgegenstehen.
- Die Hersteller müssen datenschutzrechtliche Gestaltungsanforderungen an ihr System einhalten und bereits bei der Grundkonzeption des Systems den Ansatz „Privacy by Design“ (PbD) berücksichtigen. Die Hersteller sind gehalten, die Technologie weder Unrechtsstaaten noch Staaten, die sich durch ein geringes bzw. fehlendes Datenschutzniveau auszeichnen, zur Verfügung zu stellen und dafür Sorge zu tragen, dass sich die mit dieser innovativen Technologie einhergehenden Risiken, die insbesondere in Unrechtsstaaten zu einer Gefahr für Leib und Leben erwachsen können, nicht realisieren.
- Die Anwender sind gehalten, die Technologie nur im Rahmen des datenschutzrechtlich Zulässigen anzuwenden. Sie haben dafür Sorge zu tragen, dass die zulässig verwendeten personenbezogenen Daten gegen unberechtigte Zugriffe gesichert sind. Dies gilt für öffentliche und nicht öffentliche Stellen – Unternehmen oder Privatleute – gleichermaßen.

Angesichts stetig zunehmender Begehrlichkeiten nach Überwachungsmedien seitens der Politik und

Sicherheitsbehörden sowie eines gewissen gesellschaftlichen Desinteresses und eines sich schnell und stetig entwickelnden technischen Fortschrittes ist die Entwicklung eines verstärkten gesellschaftlichen und politischen Bewusstseins für das Recht auf informationelle Selbstbestimmung unerlässlich. Dieses Bewusstsein muss dazu führen, dass Gesichtserkennung – wie bei anderen Systemen auch – mit der nötigen Sensibilität angewandt und nicht der Rahmen des technisch Möglichen, sondern allenfalls der Rahmen des rechtlich Zulässigen ausgeschöpft wird.

Was ist zu tun?

Dreidimensionale Gesichtserkennung stellt dem Gesetzgeber, den Herstellern und den Anwendern hohe Anforderungen für eine datenschutzgerechte Konzeption und einen entsprechenden Einsatz.

8.6.2 SurPRISE – Bürger äußern ihre Meinung zum Thema „Überwachung, Sicherheit und Privatsphäre“

SurPRISE ist ein von der EU gefördertes und im Februar 2012 begonnenes Projekt, das die Sichtweise europäischer Bürgerinnen und Bürger im Hinblick auf das Spannungsverhältnis zwischen Sicherheit und Privatsphäre untersucht (34. TB, Tz. 8.7). Kern des Projekts ist die Beteiligung der Bürger zu der Frage des Verhältnisses von Überwachung, Privatsphäre und Sicherheit. Die Projektpartner führten hierzu in neun europäischen Ländern ganztägige Bürgerforen durch. Das ULD organisierte im Frühjahr 2014 in Kiel ein Bürgerforum, wo die 190 Teilnehmenden gemeinsam zum Thema „Staatliche Überwachung und Privatsphäre“ diskutierten und Handlungsempfehlungen für die Politik erarbeiteten.

Das Bürgerforum hatte zwei Schwerpunkte: Zunächst wurden zwei beispielhafte überwachungsbasierte Sicherheitstechnologien, die sogenannte intelligente Videoüberwachung und die Ortung bzw. Verfolgung von Mobilgeräten durch Sicherheitsbehörden, thematisch behandelt. Dann erhielten die Teilnehmenden die Möglichkeit, sich allgemein zu dem Themenkomplex Überwachung, Sicherheit und Privatsphäre zu äußern und ihre Meinung darüber unabhängig von einer spezifischen Technologie kundzutun, auch in Form konkreter Empfehlungen an die Politik – primär auf europäischer, aber auch auf nationaler Ebene.

Bei dem vom ULD organisierten deutschen Bürgerforum wurde deutlich, dass sich die Menschen ein Bewusstsein für die Notwendigkeit des Einsatzes überwachungsbasierter Technologien zum Schutz der öffentlichen Sicherheit haben. Auch kristallisierte sich heraus, dass die Bürgerinnen und Bürger die damit einhergehenden Eingriffe in die Privatsphäre nicht ohne Weiteres akzeptieren. Die Veranstaltung offenbarte ein Meinungsbild von Sorgen über das teilweise erhebliche Missbrauchspotenzial solcher Technologien und der damit erhobenen Daten. Die oftmals nicht nachgewiesene Effektivität jener Technologien für die Erhöhung öffentlicher Sicherheit wurde bemängelt. Die Teilnehmenden zeigten ein vielschichtiges Bild von den angesprochenen Themen und bezogen dabei auch die langfristigen und gesellschaftlichen Auswirkungen staatlicher Überwachung mit ein. Das Bürgerforum legte offen, dass die gegenwärtige Sicherheitspolitik in Deutschland und Europa von vielen als zu einseitig empfunden wird – zum Nachteil der Privatsphäre des Einzelnen wie der Gesellschaft als Ganzes. Es wurde deutlich, dass die Annahme einer automatischen Akzeptanz von überwachungsbasierten Sicherheitstechnologien angesichts erhöhter Sicherheitsrisiken falsch ist. Vielmehr legten die Teilnehmer des Bürgerforums Wert auf die Feststellung, dass sowohl Sicherheit als auch Privatsphäre gleichermaßen bedeutende Güter sind. Eine ernsthafte, objektive und kritische Reflexion hinsichtlich dieser Themen seitens der Politik und der Sicherheitsbehörden wurde vermisst. Die Teilnehmer forderten eine ausgewogenere Balance zwischen Sicherheit und Privatsphäre, was sich in den formulierten Empfehlungen widerspiegelt:

- weniger Überwachung insgesamt, um eine negative Auswirkung auf die Privatsphäre im Allgemeinen zu reduzieren,
- mehr Transparenz gegenüber den Bürgern,
- zwingende, objektive und gründliche Evaluation von überwachungsbasierten Sicherheitstechnologien, insbesondere in Bezug auf
    - Geeignetheit,
    - Erforderlichkeit,
    - Effektivität
    - und Verhältnismäßigkeit,
- das Vorantreiben eines harmonisierten EU-Datenschutzrechts, welches sich hinsichtlich des Schutzniveaus am deutschen Datenschutzrecht als Mindeststandard orientiert,
- effektive Möglichkeiten der Kontrolle und Durchsetzung von Datenschutz.

Diese Empfehlungen werden zusammen mit weiteren Forschungsergebnissen des SurPRISE-Projektes, etwa zu Möglichkeiten datenschutzgerechter Gestaltung von Sicherheitstechnologien, in einen Anforderungskatalog für die Akzeptanzfähigkeit des Einsatzes staatlicher Sicherheitstechnologien einfließen. Dieser Katalog wird als Hilfestellung für die Gestaltung von Sicherheitsstrategien und für entsprechende legislative Maßnahmen auf europäischer Ebene dienen. Die Übersetzung des Länderreports mit den Ergebnissen des deutschen Bürgerforums ist in Arbeit. Das englische Original ist auf der offiziellen Webseite abrufbar als PDF-Dokument D6.3 (Country Report Germany) unter:

http://surprise-project.eu/dissemination/research-results/

8.7 Betroffenenrechte

8.7.1 Datenschutz-Auskunftsportal – eigentlich eine gute Idee

Viele Menschen wissen nicht, dass sie ein Recht auf Auskunft über ihre personenbezogenen Daten haben – sowohl gegenüber Unternehmen als auch gegenüber der Verwaltung. Selbst wer den datenschutzrechtlichen Auskunftsanspruch kennt, hat es heute nicht leicht, davon effektiv Gebrauch zu machen. Abhilfe könnten Datenschutz-Auskunftsportale schaffen.

Das Forschungsprojekt „Datenschutz-Auskunftsportal“ wurde ab August 2011 für 15 Monate vom Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV) gefördert (34. TB, Tz. 8.5). Ziel des Projekts war es, den Aufwand für Verbraucherinnen und Verbraucher bei der Wahrnehmung ihres Auskunftsrechts deutlich zu verringern. Entstanden ist ein Konzept für ein Datenschutz-Auskunftsportal, d. h. eine Internetplattform, die Folgendes leistet:

- Unterstützung der Nutzenden bei der Formulierung ihrer individuellen Anfragen und die Adressierung direkt an die Unternehmen,
- Bereitstellung allgemeiner Informationen zum Auskunftsrecht sowie standardisierter Schreiben an die Unternehmen sowie
- Erleichterung für die Unternehmen durch Tools zur prozessgestützten Bearbeitung der Auskunftsersuchen.

Keinesfalls darf ein solches Datenschutz-Auskunftsportal selbst zu einer Sammelstelle personenbezogener Daten werden. Eine vertrauenswürdige und sichere Realisierung ist notwendige Bedingung für den Betrieb. Es wurde ein Labormuster einer Internetplattform erstellt, mit dem das Potenzial für die Betroffenen deutlich wird. Der Schritt zum regulären Betrieb bedürfte weiterer Fördermittel. Die Projektidee liegt also vorläufig auf Eis. Interessierte können aber von der Ausarbeitung des ULD zu den datenschutzrechtlichen Aspekten profitieren.

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

Was ist zu tun?

Unternehmen sollten aktiv über ihre Datenverarbeitung informieren und die Hemmschwelle für das Wahrnehmen von Betroffenenrechten senken. Die Realisierung eines Auskunftsportals sollte weiterverfolgt werden.

8.7.2 Studie: Scoring nach der Datenschutznovelle 2009

Die Bewertung von Verbraucherinnen und Verbrauchern durch Wirtschaftsunternehmen mithilfe von sogenannten Scoringverfahren hat mit den stetig wachsenden Möglichkeiten der Auswertung von Daten in „Big Data"-Beständen erheblich zugenommen. Das ULD wurde zusammen mit der GP Forschungsgruppe vom Bundesministerium der Justiz und für Verbraucherschutz (BMJV) mit der Studie „Scoring nach der Datenschutznovelle 2009 und neue Entwicklungen" beauftragt. Die Studie behandelt die Frage, ob die mit der Novelle des Datenschutzrechts eingeführten Neuerungen einen angemessenen Schutz der Verbraucherinnen und Verbraucher ermöglichen. Dazu wurden die rechtlichen Grundlagen des Scorings untersucht und Betroffene und Unternehmen zur Scoringpraxis befragt.

Der Einfluss von Scorewerten auf Geschäftsentscheidungen über Kredite, Vertrags- oder Versicherungskonditionen wird – sogar im Medizinbereich – immer größer; der Aussagegehalt ist in vielen Fällen für die Betroffenen beschränkt und nicht nachvollziehbar. Unbekannte Datenquellen und wenig transparente Berechnungsverfahren machen das Scoring undurchschaubar.

Die Studie stellt fest, dass die Datenschutznovelle für Banken und Auskunfteien Auswirkungen hinsichtlich ihres Auskunftsverhaltens hatte, Beeinträchtigungen der Verbraucherrechte aber weiter bestehen. Die kostenlose Selbstauskunft ist vielen Betroffenen weitgehend unbekannt. Erteilte Auskünfte sind oft unverständlich und nicht plausibel. Scores sind prognostische Schätzungen, deren individueller Aussagegehalt oft fragwürdig ist. Es besteht Nachbesserungsbedarf bei der Bestimmung der zulässigen Datenarten und Quellen.

Die Kontrolle der Scoringverfahren erfolgt nur unzureichend, weil die Relevanz der verarbeiteten Daten für die Prognosegüte und deren Gewichtung in mathematisch-statistischen Verfahren ohne Offenlegung der Modelle weder durch die Betroffenen noch durch die Aufsichtsbehörden wirksam überprüft werden können. Die Geheimhaltung der algorithmusbasierten Berechnungen ist zu hinterfragen. Angesichts dieser Situation sind die bestehenden Regelungen für neue Scoringformen mit aus dem Internet stammenden Daten zum Schutz des Grundrechts auf informationelle Selbstbestimmung nicht ausreichend.

Was ist zu tun?

Die Transparenz über Scoringergebnisse kann durch eine inhaltlich präzisierte Auskunftspflicht der Unternehmen verbessert werden. Scoringverfahren sollten einer Qualitätsprüfung im Rahmen einer Zulassung unterzogen werden. Die Regelungen sollten nicht nur für Vertragsverhältnisse, sondern auch für andere besonders eingriffsintensive Anwendungen gelten.

09

KERNPUNKTE

Datenschutzzertifizierung

Europäisches Datenschutzgütesiegel

Auditverfahren

9 Audit und Gütesiegel

Seit den 90er-Jahren wird in Deutschland verstärkt darüber nachgedacht, wie der Schutz des Rechts auf informationelle Selbstbestimmung mithilfe von Wettbewerbsinstrumenten und insbesondere über freiwillige Audit- und Gütesiegelverfahren verbessert werden kann. Im Jahr 2000 wurden dem ULD im Landesdatenschutzgesetz Schleswig-Holstein Befugnisse zur Auditierung und zur Zertifizierung von IT-Produkten und IT-basierten Dienstleistungen zugewiesen. Seitdem führt das ULD erfolgreich Audit- und Gütesiegelverfahren auf der Grundlage des Landesrechts durch. Einige weitere Bundesländer, zuletzt Mecklenburg-Vorpommern, sind diesem Beispiel gefolgt, praktizieren jedoch die gesetzlich vorgesehenen Möglichkeiten noch in einem eingeschränkten Umfang. Aus dem Gütesiegel Schleswig-Holstein hat das ULD das Europäische Datenschutz-Gütesiegel (European Privacy Seal – EuroPriSe) entwickelt, das ab Anfang 2014 an einen privaten Betreiber abgegeben wurde und seitdem erfolgreich im Markt platziert ist (Tz. 9.3).

Die Audit- und Gütesiegelverfahren in Schleswig-Holstein waren von Anfang an und sind weiterhin darauf angelegt, Vorbild für eine nationale und europäische Lösung zu sein. Mit den Entwürfen für eine Europäische Datenschutz-Grundverordnung bekam die Idee einer Datenschutzzertifizierung neuen Aufwind. Während der Vorschlag der EU-Kommission diesbezüglich noch sehr im Unverbindlichen blieb, ist der Entwurf des EU-Parlaments von höherer Klarheit und gibt den Datenschutzbehörden im Verfahren eine wichtige Rolle.

9.1 Wichtiger denn je: eine valide nationale Datenschutzzertifizierung

Seit 2001 enthält das Bundesdatenschutzgesetz (BDSG) eine Regelung, die Auditierungen auf der Grundlage eines speziellen Gesetzes vorsieht. Pläne für ein solches Gesetz scheiterten im Jahr 2009. Mit der Einrichtung der Stiftung Datenschutz machte die schwarz-gelbe Bundesregierung ab Januar 2013 einen weiteren Versuch der Etablierung von bundesweiten Zertifizierungsverfahren im Datenschutz. Leider hat sich die Konzeption der Stiftung als nicht geeignet erwiesen, dieses Ziel zu realisieren (34. TB, Tz. 2.3). Auch die im Vertrag der schwarz-roten Regierungskoalition auf Bundesebene vorgesehenen Erwägungen, die Zertifizierungsaufgaben der Stiftung im Rahmen der Stiftung Warentest umzusetzen, scheinen sich nicht realisieren zu lassen.

Inzwischen gibt es eine Vielzahl von privatwirtschaftlichen Initiativen für Datenschutzzertifizierungen. Diese haben auf dem Markt aber bisher aus mehreren Gründen keine hohe Akzeptanz gefunden: fehlende Einheitlichkeit, ungenügende Transparenz, unklare Zertifizierungskriterien, fehlendes Vertrauen in die Zertifizierungsstelle. Dies hat zur Folge, dass das primär die öffentliche Verwaltung betreffende Landessiegel von Schleswig-Holstein auch für Produkte und Dienstleistungen auf dem privaten Markt die höchste Akzeptanz gefunden hat, wie eine Aufstellung der Stiftung Datenschutz bestätigt.

https://stiftungdatenschutz.org/wp-content/uploads/2014/12/SDS-Zertifizierungsu%CC%88bersicht-20-11-14.pdf

Dem ungenügenden Angebot an etablierter Zertifizierung steht ein zunehmender Bedarf in der Wirtschaft sowie bei den Verbraucherinnen und Verbrauchern gegenüber, ausgelöst nicht zuletzt durch die Spionage von NSA und GCHQ wie auch durch die vielen öffentlich bekannt gewordenen erfolgreichen Angriffe auf IT-Systeme.

Im Auftrag des Bundeswirtschaftsministeriums entwickelt das Kompetenzzentrum Trusted Cloud an der Universität des Saarlandes ein Zertifizierungsschema für die Auftragsdatenverarbeitung in Form des Cloud Computing. Das ULD ist gemeinsam mit anderen Aufsichtsbehörden sowie relevanten Stellen und Unternehmen an dem Projekt beratend beteiligt. Für Online-Shops gibt es schon seit Längerem zur Sicherung des Verbraucherschutzes Gütesiegel der D21-Initiative, an dessen Gütesiegel-Board das ULD ebenfalls als einzige Datenschutzbehörde beratend beteiligt ist, zumal Verbraucherdatenschutz bei Online-Angeboten immer wichtiger wird. Die deutsche Wirtschaft hat gegenüber US-Anbietern, deren Datenschutzniveau in der Regel erheblich niedriger ist, bisher wenige Wettbewerbsvorteile davon, dass sie sich am deutschen und europäischen Datenschutz

orientiert. Ein Grund hierfür liegt im Fehlen einer vertrauenswürdigen Zertifizierung.

Angesichts dieser Sachlage hat sich das ULD an das Bundesministerium des Innern gewandt mit dem Vorschlag, die Erfahrungen mit dem Datenschutzgütesiegel-Schleswig-Holstein national stärker fruchtbar zu machen. Dies könnte in eine gemeinsame Bund-Länder-Initiative münden, deren Autorität sich insbesondere aus der Qualität und Transparenz der Zertifizierung ergibt und die durch Träger gut beraten, aber ohne großen bürokratischen Überhang unabhängig agiert. Wegen der vorhandenen Erfahrungen ist nur ein geringer Konzeptaufwand nötig. Ein deutsches Zertifizierungsverfahren könnte prägend für die europäische Ebene sein.

9.2 Datenschutz-Gütesiegel Schleswig-Holstein

9.2.1 Abgeschlossene Gütesiegelverfahren

In den Jahren 2013 und 2014 konnte das ULD acht Produkten erstmalig ein Datenschutz-Gütesiegel verleihen. Vierzehn weitere Produkte konnten nach Fristablauf der bestehenden Zertifizierung in einem vereinfachten Verfahren rezertifiziert werden.

Die gleichbleibend hohe Anzahl von Rezertifizierungen zeigt, dass das Gütesiegel Schleswig-Holstein für Hersteller von hoher Relevanz ist. In einigen Branchen, wie etwa bei Schredderunternehmen, weist das Gütesiegel eine hohe Marktdurchsetzung auf. Die Umsetzung der nunmehr gültigen DIN 66399 für den Bereich der Akten- und Datenträgervernichtung warf bei den Gutachtern praktische Fragen für aktuelle Zertifizierungsverfahren auf, die zusammen mit dem ULD gelöst werden konnten.

Die Einbindung von Cloud-Diensten gewinnt bei der Zertifizierung zunehmend an Relevanz. Maßgebend für die hierfür notwendigen rechtlichen und technischen Anforderungen an die Ausgestaltung entsprechender Dienste ist die „Orientierungshilfe Cloud Computing“ der Arbeitskreise Technik und Medizin (Tz. 5.5). Zertifizierungsverfahren, die sich mit der Bereitstellung von Dienstleistungen im Bereich der Medizin- und Sozialdaten beschäftigen, nehmen zu. Wegen der sehr unterschiedlichen Ausgestaltung der einzelnen Zertifizierungsgegenstände und der hierbei verarbeiteten hochsensiblen personenbezogenen Daten des Betroffenen gewinnt die Einbindung anderer Referate des ULD wie auch anderer Aufsichtsbehörden im Zertifizierungsprozess zunehmend an Bedeutung.

Folgende Produkte wurden neu zertifiziert:

- „WIMES“, Version 2012.1: Webportal zur Evaluation der Wirksamkeit von Hilfen im Bereich der Erziehung,
- „DIGITTRADE – High Security HDD HS256S“, Version 1.0: Externe Festplattenlösung mit 256-Bit Full Disk AES Hardwareverschlüsselung,
- „Zentrale Kassenprüfung“, Releasestand Mai 2013: Analysetool für Kassendaten zur Aufdeckung von Manipulationen im Kassierprozess,
- „I.S.S Schulmensaverwaltung“, Version 6.0: Software zur Unterstützung von Schulen bei der Verwaltung von Mensen,
- „RED Medical“, Releasestand Juli 2013: Software zur Erhebung, Verarbeitung und Nutzung von medizinischen Patientendaten zur Unterstützung von ärztlichen Anamnesen, Diagnosen und Therapien,
- „Business Keeper Monitoring System (BKMS)“, Version 2.7.3: Onlinegestütztes Tool für den Dialog zwischen Hinweisgebern und Hinweisbearbeitern zur Meldung von Missständen, Gefahren und Risiken in Organisationen,
- „Datenträgervernichtung (DV)“, Stand August 2014: Mobile und stationäre Akten- und Datenträgervernichtung,
- „Stepnova“, Version 4: Webbasiertes Datenbanksystem zur Organisation im Bildungssektor.

Im Rahmen einer Rezertifizierung wurden u. a. folgende Produkte in einem vereinfachten Verfahren erneut erfolgreich überprüft:

- „Akten- und Datenvernichtung“ der Firma MAMMUT Dokumentenservice GmbH, Stand April 2013: Verfahren zur datenschutzgerechten, physikalischen Datenträgervernichtung,
- „Elefant Profi im Security-Mode“, Version 13.02: Verwaltungsprogramm für psychotherapeutische und ärztliche Praxen,
- „e-pacs Speicherdienst“, Version 3.0: Elektronische externe Archivierung von Röntgenbildern und anderen patientenbezogenen medizinischen Daten,
- „BackStor“, Version 1.2: Eine Remote-Backup-Lösung für die Sicherung, Archivierung und Wiederherstellung von Daten für Unternehmen und öffentliche Stellen,
- „Altersverifikation KBA 18“, Version 27R4: Altersüberprüfung durch das Einlesen von Personalausweisen oder Führerscheinen,
- „TeamDrive“, Version 3: Ein Kollaborationstool für den Zugriff mehrerer Benutzer und die gemeinsame Bearbeitung von Dokumenten in einem verschlüsselten Datenbestand,
- „Verfahrensregister“, Version 1.0 (2014): Anwendung zur Unterstützung des betrieblichen Datenschutzbeauftragten bei der Erstellung und Verwaltung eines Verfahrensregisters,
- „KOMMBOSS“: Anwendung zur Unterstützung von Kommunen und öffentlichen Stellen in den Bereichen Personalwesen, zentrale Verwaltung und Organisation,
- „Verfahren zur Akteneinlagerung“ der recall Information Services GmbH: Im Rahmen eines Auftrags zur Akteneinlagerung erfolgt gemäß dem Schutzbedarf sowohl die reine Archivierung von Akten als auch das Bereitstellen einer externen Akten-/Archivhaltung mit Anforderungsmöglichkeit durch den Kunden,
- „Easybooth Modell 37, Easybooth V3 Modell 36, Minicabine3 Modell 38 und UPD Modell 3“: Digitale Fotokabine mit integrierter biometrischer Bildbearbeitung zur Nutzung in Meldebehörden,
- „RED Medical“: Erhebung, Verarbeitung und Nutzung von medizinischen Patientendaten zur Unterstützung von ärztlichen Anamnesen, Diagnosen und Therapien.

Informationen für Hersteller befinden sich im Internet unter:

https://www.datenschutzzentrum.de/guetesiegel/hersteller/

Was ist zu tun?

Die Nachfrage nach Neuzertifizierungen beim ULD ist zwar erfreulich hoch, doch ist die Möglichkeit der Datenschutzzertifizierung noch nicht in allen Bereichen der Wirtschaft bekannt, sodass auch zukünftig ein Augenmerk darauf zu legen ist, diese Bereiche besonders anzusprechen.

9.2.2 Sachverständige und Prüfstellen

Weitere Sachverständige wurden vom ULD für das Verfahren zur Erlangung des Datenschutz-Gütesiegels Schleswig-Holstein anerkannt.

Im Rahmen des zweistufigen Gütesiegelverfahrens erfolgt die Begutachtung der zu zertifizierenden Produkte durch vom ULD anerkannte Datenschutzsachverständige. Dies kann – für Prüfstellen wie für Einzelpersonen – entweder für den Bereich Recht oder für den Bereich Technik erfolgen, bei entsprechender Qualifikation ist auch eine Doppelzulassung möglich. Voraussetzungen für eine Anerkennung sind stets neben der Zuverlässigkeit und Unabhängigkeit der Nachweis der erforderlichen Fachkunde. Diese muss sich insbesondere auf den Datenschutzbereich und dort gesammelte langjährige Erfahrungen erstrecken.

Hinzugekommen als Sachverständige/sachverständige Prüfstellen sind 2013/2014:

- Dr. Christian Szidzek, Giebelstadt (Recht),
- Dr. Markus Lang, Düsseldorf (Recht),
- Prof. Dr. Carsten Noogie Thomas Kaufmann, Hamburg (Recht).

Bei folgender Prüfstelle haben sich Änderungen ergeben:

- ditis Systeme, Niederlassung der JMV GmbH & Co. KG, Ulm (Andreas Zeller (Leiter Recht), Bernd Sobottka (Leiter Technik))

Derzeit sind beim ULD 59 Einzelsachverständige registriert. Hinzu kommen noch 16 Prüfstellen.

Jeweils im August 2013 und 2014 fanden im Anschluss an die Sommerakademie Gutachterworkshops in Kiel statt. Von dieser Möglichkeit des Erfahrungsaustausches machten zahlreiche Sachverständige Gebrauch. Diskutiert wurden u. a. die Zusammenarbeit mit der jetzt eigenständigen EuroPriSe GmbH, aktuelle Erfahrungen mit Neu- und Rezertifizierungen, insbesondere die Umsetzung der Anforderungen der DIN 66399, die Gestaltung von Gutachten, die Überarbeitung des Kriterienkatalogs, typische Fehler bei der Gutachtenerstellung, die aktuelle Gesetzgebung sowie Fragen des Marketings. Eine wichtige Funktion der Sachverständigen liegt darin, bei Herstellern Interesse für das Gütesiegel zu wecken.

Weitere Informationen für Sachverständige befinden sich im Internet unter:

http://www.datenschutzzentrum.de/guetesiegel/sachverstaendige/

Was ist zu tun?

Um das Verfahren der Zertifizierung weiterhin effektiv zu gestalten und den Ablauf stetig zu verbessern, bleibt es wichtig, die Sachverständigen bei ihrer Arbeit zu unterstützen.

9.2.3 Überarbeitung des Gütesiegel-Anforderungskatalogs

Der Gütesiegel-Anforderungskatalog ist die Grundlage für die Sachverständigen für die Prüfung von IT-Produkten. Durch Gesetzesänderungen und die Einführung der Schutzziele im LDSG war es notwendig geworden, den Kriterienkatalog anzupassen und zu modernisieren.

Die Version 2.0 des Anforderungskatalogs ist 2014 in Kraft getreten. Alle seit dem Zeitpunkt des Inkrafttretens begonnenen Zertifizierungsverfahren werden hiernach durchgeführt. Die Struktur des Anforderungskatalogs wurde beibehalten; es erfolgten zahlreiche Anpassungen und Konkretisierungen aufgrund neuerer technischer und rechtlicher Entwicklungen. Vier Komplexe sind zu prüfen: grundsätzliche technische Ausgestaltung des Produkts, Zulässigkeit der Datenverarbeitung, technisch-organisatorische Maßnahmen und Rechte der Betroffenen. Prüfungen nach dem alten Katalog bleiben so mit den neuen Standards vergleichbar.

Ein Prüfungsschwerpunkt liegt nunmehr auf den Schutzzielen, an denen sich zu zertifizierende IT-Produkte ausrichten müssen: Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettbarkeit und Intervenierbarkeit. Eine Herausforderung für die Sachverständigen besteht darin, die Gewichtung dieser Schutzziele vorzunehmen und damit zu einem angemessenen Prüfmaßstab für das jeweilige IT-Produkt zu gelangen.

Gesetzesänderungen werden auch künftig in den Anforderungskatalog eingepflegt. Zur Erleichterung der Arbeit der Sachverständigen und zur Vereinheitlichung der Ergebnisse stellt das ULD regelmäßig Erfahrungen im Zertifizierungsprozess u. a. mittels Beispielen den Sachverständigen zur Verfügung.

9.2.4 Neue Datenschutzgütesiegelverordnung

Die im November 2013 in Kraft getretene Datenschutzgütesiegelverordnung (DSGSVO) ersetzt die bis dahin gültige Datenschutzauditverordnung (DSAVO). Sie nimmt eine Begriffsbestimmung des IT-Produktes als zulässigen Zertifizierungsgegenstand vor und regelt grundsätzliche Voraussetzungen und Abläufe des Zertifizierungsverfahrens sowie der Anerkennung von Sachverständigen für das Gütesiegel Schleswig-Holstein. Die Änderungen betrafen begriffliche Klarstellungen sowie Regelungen zur Verwendung des Gütesiegels über den Gültigkeitszeitraum hinaus. Im Fall der Verwendung des Gütesiegels nach Ablauf der Gültigkeit muss nunmehr in geeigneter Weise ein deutlicher Hinweis auf den Ablauf der Gültigkeit erfolgen. Wurden wesentliche Änderungen an dem IT-Produkt vorgenommen, ist in passender Form darauf hinzuweisen, dass sich das Zertifikat auf eine Vorversion bezieht. Ist innerhalb eines Jahres nach Ablauf der Gültigkeit oder nach Vornahme wesentlicher Änderungen am IT-Produkt keine erneute Zertifizierung erfolgt, darf das Gütesiegel nicht mehr verwendet werden.

9.2.5 Zusammenarbeit mit EuroPriSe

Auch nach dem Übergang von EuroPriSe in die EuroPriSe GmbH bieten das ULD und die EuroPriSe GmbH für Hersteller von IT-Produkten die Möglichkeit einer gemeinsamen Zertifizierung nach beiden Schemata. Die Durchführung eines solchen Kombiverfahrens kann sich für viele Hersteller auch weiterhin lohnen, da die damit einhergehenden Synergieeffekte erhalten bleiben.

Während das Datenschutz-Gütesiegel Schleswig-Holstein die rechtskonforme Einsatzmöglichkeit von IT-Produkten nach dem Recht in Deutschland und in Schleswig-Holstein bestätigt, hat EuroPriSe vorrangig das europäische Recht und die dazu ergangene Rechtsprechung sowie Auslegungen durch die Artikel-29-Arbeitsgruppe im Blick. Will ein Hersteller sowohl national als auch international mit seinem Produkt auftreten, ist ein Kombiverfahren zumeist sinnvoll. Durch die Einreichung eines Gutachtens für beide Verfahren bei einer der beiden Zertifizierungsstellen können Kosten eingespart werden. Eine Zertifizierungsstelle nach Wahl des Antragstellers übernimmt dann in diesem Verfahren die führende Rolle und stimmt den Zertifizierungsprozess mit der jeweils anderen Zertifizierungsstelle ab. Voraussetzung ist, dass die beteiligten Sachverständigen für beide Verfahrensarten anerkannt sind – was für zahlreiche Gutachter gilt. Auch die Gebühren des ULD sind geringer, als wenn zwei getrennte Verfahren durchgeführt werden. Weitere Anträge werden derzeit im ULD bearbeitet.

9.3 EuroPriSe

2014 ging das EuroPriSe-Gütesiegel und damit die Zertifizierung der Datenschutzkonformität nach europäischem Recht von IT-Produkten und IT-basierten Dienstleistungen vom ULD auf die EuroPriSe GmbH über.

Die Behördenstruktur und die eingeschränkten finanziellen Mittel des ULD machten es notwendig, das EuroPriSe-Siegel auf neue Füße zu stellen. So kann dieses Zertifizierungsangebot erhalten und ausgebaut werden. Verantwortlich ist nun die EuroPriSe GmbH, die zur 2B-Advice-Gruppe gehört, einer internationalen Beratungsgruppe für Datenschutz, die mit ihren Beratungsgesellschaften in mehreren Ländern Europas und in den USA vertreten ist. Es erfolgt eine enge Zusammenarbeit, insbesondere im Rahmen von gemeinsamen Verfahren (Tz. 9.2.5). Das ULD ist in einem Expertengremium, dem Advisory Board von EuroPriSe, vertreten.

Mit der neuen Struktur besteht die Möglichkeit, die erlangten Erfahrungen auf die Zertifizierung von Verfahren, Verarbeitungen im Auftrag, Konzepten, Personen, Schulungen oder Webseiten zu übertragen und gemäß den Vorgaben der EU-Datenschutzgesetzgebung und den Festlegungen der Artikel-29-Arbeitsgruppe weiterzuentwickeln. Vorbild hierfür ist das bewährte EuroPriSe-Modell mit der Schulung und Akkreditierung von Prüfern, der

Prüfung durch EuroPriSe-Experten entlang objektiver Schemata und der abschließenden Validierung und Zertifizierung. Gleichzeitig kann die EuroPriSe GmbH den Herstellern und Experten räumlich entgegenkommen, z. B. durch Schulungsangebote in weiteren Mitgliedstaaten der EU und lokalen Dependancen.

9.4 Auditverfahren

Im Berichtszeitraum wurden vier Auditierungen erfolgreich abgeschlossen. Neben den im Folgenden genannten wurden das Zutrittsberechtigungssystem und die Videoüberwachung des Landtags reauditiert (Tz. 3.1).

9.4.1 Unfallkasse Nord

Im März 2013 auditierte das ULD die Unfallkasse Nord. Diese wies im Rahmen des Verfahrens nach, wie sie die datenschutzrechtlichen Vorgaben einhält und die erforderlichen technischen Maßnahmen ergriffen hat. Ein wichtiger Prüfpunkt war die Implementation und die tägliche Umsetzung eines wirksamen Managementverfahrens für Datenschutz und Datensicherheit. Dieses erlaubt es der Unfallkasse Nord, auch in Zukunft und langfristig guten Datenschutz zu gewährleisten. Das Audit umfasste u. a. die allgemeine Datenverarbeitung, die Personalverwaltung, Leistungsgewährung, Teilhabe, den Regress und den Arbeitsschutz.

9.4.2 Bad Schwartau

Zum vierten Mal verlieh das ULD der Stadtverwaltung Bad Schwartau das Datenschutzauditzeichen für eine vorbildliche und ordnungsgemäße Datenverarbeitung. Sie legt damit einen neuen Maßstab in Bezug auf die Beständigkeit des von ihr gelebten Datenschutzes und die stetige Weiterentwicklung der Datensicherheitsmechanismen.

Im Jahr 2004 hatte die Stadtverwaltung Bad Schwartau zum ersten Mal ihr hohes Niveau an Datensicherheit bei der Verarbeitung ihrer Bürgerdaten auf EDV-Systemen vom ULD auditieren lassen. Mit Ablauf des Auditzertifikats nach drei Jahren wurde die Aufrechterhaltung des Sicherheitsniveaus jeweils in den Jahren 2007 und 2010 erfolgreich reauditiert. Für die Mitarbeiterinnen und Mitarbeiter der Stadtverwaltung Bad Schwartau gehören Datenschutz und Datensicherheit inzwischen selbstverständlich zu den täglichen Arbeitsabläufen. Die Verantwortlichen signalisieren, dass nur ein beständig hohes Datenschutzniveau die Daten der Bürgerinnen und Bürger dauerhaft schützt.

Die Reauditierung im Jahr 2013 ergab, dass das Datenschutzkonzept an die Datenverarbeitungsprozesse der Fachabteilungen und an den Stand der Technik angepasst wurde. Das gesetzte Sicherheitsniveau wurde mit der Erneuerung zentraler IT-Systeme und dem Einsatz von Sicherheitssoftware positiv fortentwickelt. Der Bürgermeister, der Büroleiter, die Mitarbeitenden in der IT-Koordination sowie der behördliche Datenschutzbeauftragte sorgen dafür, dass die im Datenschutzkonzept festgelegten Sicherheitsmaßnahmen dauerhaft umgesetzt werden. Sie unterstützen den IT-Sicherheitsprozess vorbildlich.

Was ist zu tun?

Die Stadt Bad Schwartau verfolgt den richtigen Weg. Andere kommunale Verwaltungen sollten diese Stadtverwaltung zum Vorbild nehmen und ihr Datenschutzkonzept ebenfalls durch das ULD auditieren lassen.

9.4.3 Ratekau

Bereits im Jahr 2006 hatte die Gemeindeverwaltung Ratekau ein Datenschutzaudit erfolgreich bestanden. Nach Auslaufen des Zertifikats wurde es jedoch nicht unmittelbar verlängert. Nun beauftragte der Bürgermeister das ULD mit einer erneuten Begutachtung. In der Zwischenzeit war die in der Gemeindeverwaltung Ratekau für die Datenverarbeitung eingesetzte Technik auf einen neuen Stand gebracht worden.

Im Rahmen der Auditierung wurden die internen IT-Systeme sowie die Netzanbindungen an das Internet der Kindergärten der Gemeindeverwaltung Ratekau gründlich überprüft. Die eingesetzten Datenverarbeitungssysteme wurden begutachtet. In einem Datenschutzkonzept sind die Sicherheitsmaßnahmen für die automatisierte Datenverarbeitung und für den Anschluss des Verwaltungsnetzes an externe Netze festgelegt, die auf ihre Umsetzung und Wirkungsweise überprüft wurden. Die durch das Datenschutz-Behördenaudit in der Gemeindeverwaltung Ratekau erfassten Verarbeitungsprozesse zeichnen sich besonders durch folgende datenschutzfreundliche Aspekte aus:

- Die mit den Fachverfahren der Gemeindeverwaltung verarbeiteten Bürgerdaten werden durch ausreichende IT-Sicherheitsmaßnahmen geschützt.
- An den Arbeitsplätzen werden sogenannte Thin Clients eingesetzt, über die ein besonderer Schutz der Datenverarbeitung am Arbeitsplatz gewährleistet wird.
- Die Gemeindeverwaltung hat eine gut strukturierte, systematische und übersichtliche Dokumentation gemäß DSVO als effektive Arbeitsgrundlage für das Datenschutz- und IT-Sicherheitsmanagement erstellt.
- Für den Anschluss des internen Verwaltungsnetzes an das Internet werden Sicherheitskomponenten eingesetzt, die unerwünschte Zugriffe abwehren.
- Die Sicherheitsmechanismen zur zentralen Vergabe von Berechtigungen und zur Steuerung der Arbeitsplatzrechner werden nachhaltig gepflegt.
- Das Datenschutz- und IT-Sicherheitsmanagement führt in regelmäßigen Abständen Sitzungen durch, in denen Datenschutz- und IT-Sicherheitsaspekte bearbeitet werden.

Was ist zu tun?

Das Datenschutz- und IT-Sicherheitsmanagement der Gemeindeverwaltung Ratekau sollte Vorbild für andere kommunale Verwaltungen sein.

9.5 Beratungen

Das ULD führt gemäß dem LDSG gebührenpflichtige Beratungen durch. Hierbei stehen die Erhöhung des Datenschutzniveaus und das Sammeln von Erfahrungen mit neuen Datenschutzinstrumenten im Vordergrund.

9.5.1 Kommunales Rechenzentrum Niederrhein

2013 wurde – nach vorheriger Absprache mit dem dortigen Datenschutzbeauftragten – das Kommunale Rechenzentrum Niederrhein (KRZN) in Nordrhein-Westfalen durch das ULD unterstützt. Dabei wurden die Voraussetzungen für eine ISO-27001-IT-Grundschutzzertifizierung des Rechenzentrums geschaffen.

Die internen Datenschutz- und IT-Sicherheitsbeauftragten des KRZN baten das ULD um Hilfe bei der Implementierung des IT-Grundschutzstandards mit dem Ziel, ein ISO-27001-Zertifizierungsverfahren auf der Basis von IT-Grundschutz durchzuführen. Die angefragten Dienstleistungen stellten sich als besonders anspruchsvoll und komplex dar, sodass die Beratung für das ULD eine Lernerfahrung darstellte.

Gegenstand der Begutachtung und Beratung war die grundschutzkonforme Überprüfung und Herstellung des Rechenzentrumsbetriebes und damit u. a. Folgendes:

- Bestandsaufnahme und Abgrenzung des IT-Verbundes,
- Ermittlung der Schutzbedarfe in einer Schutzbedarfsfeststellung,
- Bausteinzuordnung aus dem Grundschutzkatalog mithilfe des Tools „Verinice“,
- Maßnahmenbearbeitung im Rahmen von Inspektionen und Interviews,
- Prüfung des Umsetzungsstandes der Grundschutzmaßnahmen vor Ort,
- Mitwirkung bei der Erstellung aller erforderlichen IT-Grundschutz-Dokumentationen,
- Durchführung einer Risikoanalyse für Bereiche mit hohem Schutzbedarf,
- Abgleich der Verfahrensschritte mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI),
- Durchführung einer Prüfungssimulation nach dem Auditierungsschema des BSI,
- Einleitung des Zertifizierungsverfahrens nach ISO 27001 auf der Basis von IT-Grundschutz.

Darüber hinaus führte das ULD zielgruppenorientiert mehrere Grundschutzschulungen im Schulungszentrum des KRZN für dessen Mitarbeiterinnen und Mitarbeiter im Rahmen der DATENSCHUTZAKADEMIE Schleswig-Holstein durch.

Die Beratungstätigkeit des ULD wurde mit der vollständigen Implementierung des IT-Grundschutzstandards abgeschlossen. Im Juli 2014 erhielt das KRZN vom BSI das Grundschutzzertifikat für drei Jahre. Die Geschäftsführung des KRZN wies darauf hin, dass Sicherheit Vertrauen schafft, nicht nur bei den Kunden, sondern gerade auch bei den Bürgerinnen und Bürgern, um deren Daten es letztendlich geht. Der wirtschaftliche Vorteil besteht u. a. in einer Optimierung der internen organisatorischen Abläufe und der großen Transparenz der Prozesse. Man könne davon ausgehen, dass künftig öffentliche IT-Dienstleistungen nur noch von zertifizierten Anbietern marktfähig sind.

Was ist zu tun?

Die im ULD gesammelten Erfahrungen sollten für Schleswig-Holstein bei der Zertifizierung der hier tätigen Rechenzentren nutzbar gemacht werden.

9.5.2 AON

AON ist ein weltweit tätiger technischer Versicherungsmakler, Berater für Risikomanagement und Rückversicherungsmakler mit Standorten in mehreren Staaten. Der Konzern beauftragte das ULD mit einer Überprüfung der Datenverarbeitungsprozesse in Bezug auf die IT-Sicherheit an drei Standorten. Im Rahmen eines Audits wurde ermittelt, wie hoch die Aufwände für eine erfolgreiche ISO-27001-Zertifizierung auf der Basis von IT-Grundschutz sind.

Aufgabe des ULD war ein Sicherheitscheck im Bereich der Datenverarbeitung auf der Basis von IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Es sollte festgestellt werden, ob das Datenschutz- und IT-Sicherheitsniveau des AON-Konzerns an den drei Standorten ausreichend ist.

Das übergreifende Audit erfolgte in folgenden Schritten:

- Analyse der Aufbau- und Ablauforganisation,
- Überprüfung des ordnungsgemäßen Einsatzes der Informationstechnik (IT-Komponenten, Fachverfahren),
- Analyse über den Stand der Implementierung von Datenschutz und IT-Sicherheitsmanagement und der dazugehörigen Sicherheitsdokumentation,
- stichprobenartige Überprüfung der Datenverarbeitungsprozesse,
- standortbezogene Gespräche mit den Beteiligten über die festgestellten Sachverhalte.

Darüber hinaus sollte festgestellt werden, welche Aufwände für eine ISO-27001-Zertifizierung auf der Basis von IT-Grundschutz erforderlich sind.

Die Überprüfung der Organisationsstrukturen, des zentral eingerichteten IT-Betriebs, der Kommunikationsprozesse sowie der umgesetzten Datenschutz- und IT-Sicherheitsmaßnahmen erfolgte in Zusammenarbeit mit dem bei AON integrierten Datenschutz- und IT-Sicherheitsmanagement. Die Ergebnisse wurden den Verantwortlichen in einem umfänglichen Auditbericht dargestellt.

Was ist zu tun?

Der IT-Grundschutzstandard des BSI gewinnt zunehmend an Bedeutung. Unternehmen wie AON können ihre Datenverarbeitung durch das ULD auf Herz und Nieren prüfen lassen und dabei feststellen, inwieweit sie die Anforderungen des IT-Grundschutzes des BSI und des Datenschutzes erfüllen.

10

KERNPUNKTE

Tracking

Kryptografie

IT-Forensik

10 Aus dem IT-Labor

10.1 Tracking – Nutzerverfolgung im Wandel der Zeit

PC-Browser haben eine lange Geschichte hinter sich, spätestens seit Googles Markteintritt hat sich die Entwicklungsgeschwindigkeit der Programme massiv erhöht. Das kommt der Funktionalität und der Sicherheit zugute. Die Aktualisierung der Software findet im Hintergrund ohne Zutun des Nutzers statt. Das ist intransparent; der Nutzer weiß nicht, ob und wann sich sein Browser aktualisiert; andererseits sind so weniger Nutzer mit bekannten Sicherheitslücken im Netz unterwegs.

In anderer Hinsicht ist die Transparenz deutlich gestiegen: Umfangreiche Einstellungen zum Umgang mit Cookies und anderen Webseitendaten bieten alle Browser, Erweiterungen zum Filtern von Webseiteninhalten sind ebenfalls allgemein verfügbar. Dem klassischen Tracking können Nutzer so effektiv begegnen. Doch neue Tracking-Technologien machen es zunehmend schwierig, unbeobachtet von Online-Anbietern im Netz unterwegs zu sein. Spätestens seit den Veröffentlichungen von Edward Snowden ist klar, dass der Anwendungsbereich solcher Technologien weit über das Anzeigen von Werbebildchen hinausgeht und dass auch Geheimdienste Techniken wie die sogenannten Evercookies einsetzen, um Internetnutzer zu identifizieren.

Neue Probleme bringen mobile Plattformen mit sich. Browser unter iOS, Android oder Windows Phone sind im Hinblick auf die Einstellmöglichkeiten ein Schatten ihrer großen Desktop-Geschwister. Cookies lassen sich in der Regel zwar löschen, es ist aber nicht möglich, sie nur gezielt anzunehmen oder gar gespeicherte Cookies anzuzeigen. Die Hersteller begründen dies mit der eingeschränkten Bedienbarkeit der Geräte, bedingt durch kleine Bildschirme und das Fehlen von Maus und Tastatur. Spätestens für Tablets gilt dieses Argument jedoch nicht mehr. Wir haben es eher mit dem Unwillen der Hersteller zu tun. Microsoft geht mit schlechtem Beispiel voran: In Windows 8.1. wird der Internet Explorer sowohl als Desktop wie auch als sogenannte Modern App mitgeliefert. Ersteres bietet das gewohnte Set an Konfigurationsmöglichkeiten; Letzteres präsentiert sich „touchoptimiert“: Im Kontext der Einstellmöglichkeiten bedeutet das vor allem, dass der Nutzer auf einen Großteil der Optionen schlicht verzichten muss und sich Tracking-Versuchen, die über klassische Cookies hinausgehen, nicht entziehen kann. Gleiches gilt für Google Chrome, das für Tablets deutlich weniger Möglichkeiten zur Regelung der Datenspeicherung bietet als für den Desktop-PC. Hinzu kommt, dass Browsererweiterungen, mit denen sich oft datenschutzfördernde Funktionen nachrüsten lassen, in mobilen Browsern gar nicht eingebunden werden können. So muss der mobile Nutzer auf das automatische Filtern von Tracking-Code verzichten.

Der Nachteil der mangelnden Konfigurierbarkeit bei mobilen Systemen könnte mittelfristig einen interessanten Nebeneffekt haben. Beim sogenannten Device Fingerprinting wird versucht, serverseitig Informationen über das IT-System des Nutzers zu sammeln und zu analysieren, um so den Nutzer möglichst eindeutig wiederzuerkennen. Das klappt erstaunlich gut aufgrund der Vielzahl von Informationen, die Browser von sich aus oder auf Anfrage bereitwillig mitteilen. Dies sind neben Programm- und Betriebssystemversion die Bildschirmauflösung, verfügbare Schriftarten und Hintergrundfarbe des Desktops. Eine exotische Schrift und eine bestimmte Systemfarbe machen einen Nutzer-PC in der Menge aller Webseitenbesucher eines Servers oft eindeutig. Plug-ins und vom Nutzer veranlasste Browsererweiterungen tun ihr Übriges, um den Browser aus der Masse herauszuheben. Die spezifische Kombination ist häufig einzigartig und kann dazu dienen, einzelne Browser und damit ihre Nutzer wiederzuerkennen. Die Einschränkungen der mobilen Browser können so für den Nutzer von Vorteil sein: Ein Device Fingerprinting von Smartphones ist deutlich ungenauer als bei Desktop-PCs. Da die Systeme sich vom Nutzer schlicht nicht bzw. kaum individualisieren lassen, erscheinen verschiedene Smartphones nach außen hin oft identisch.

Die Werbeindustrie hat aber in dieser Hinsicht nachgerüstet. Mit sogenannten ETags lassen sich Webseitenressourcen ausstatten, die der Browser des Nutzers in seinem Cache zwischenspeichert. Um zu ermitteln, ob die Ressource sich seit dem letzten Abruf verändert hat, schickt der Browser später nur den ETag an den Server mit dem Hinweis, die zugehörige Ressource – zumeist sind das Grafiken – nur im Änderungsfall erneut zu übertragen. Generiert der Server die ETags jedoch

nicht auf die Ressource bezogen, sondern nutzerbasiert, lässt sich mit diesem Verfahren trefflich die Funktionalität von Cookies nachbilden, ohne Cookies einzusetzen.

Auch der Standard „HTTP Strict Transport Security" (HSTS) lässt sich zum Tracking missbrauchen. Eigentlich dient diese Funktion seit 2012 dazu, dass der Browser sich den Kontakt zu einer https-gesicherten Webseite merkt. Bei erneuten Aufrufen derselben Webseite greift er dann von sich aus auf die gesicherte Verbindung zurück, ein böswilliges Umleiten durch Dritte auf unsichere Verbindungen wird verhindert. Zum Tracking-Werkzeug wird diese Funktion, indem eine Webseite mehrere Subdomains betreibt, also z. B. a.beispiel.de, b.beispiel.de. Für jede dieser Adressen lässt sich nun im Browser ein https-Aufrufbefehl hinterlegen. Der Trick liegt darin, nur für einige der Adressen den verschlüsselten Aufruf zu erzwingen, für andere nicht. Bei einem späteren Besuch auf dem Webserver wird der Browser dann Ressourcen von den unterschiedlichen Subdomains nach einem für ihn individuell zusammengestellten Muster abrufen. Der Aufruf mit oder ohne https kann als Binärwert – als Bit – gesehen werden. Die Weltbevölkerung von 7,2 Milliarden Menschen lässt sich mit einem Wert von 33 Bit abbilden – man benötigt also eine Webseite mit 33 Subdomains, von der dann Ressourcen per http oder https abgerufen werden, um alle Menschen mit einer eindeutigen ID markieren zu können. Wenig überraschend ist es, dass die Browser die Tabellen, in denen sie sich solche erzwungenen verschlüsselten Verbindungen merken, nicht anzeigen, geschweige denn vom Nutzer löschen lassen. Werden die Tabellen dann auch noch zwischen verschiedenen Browsern synchronisiert, wie dies bei Apple der Fall ist, wird der Nutzer plötzlich vom Handy bis an den Desktop-Rechner nachverfolgbar.

Die Angriffsfläche für lückenlose Nutzerverfolgung wird also zunehmend größer. Während sich die EU-Kommission mit Mitgliedstaaten wie z. B. Deutschland noch über den Umgang mit Cookies streitet, nutzen Online-Unternehmen mit dem Device Fingerprinting und ETag-basierten Cache-Elementen bereits Tracking-Generation zwei und drei. Für Nutzer wird es schwierig, sich zu wehren. Lassen sich Cookies und Flash-Plug-ins noch einigermaßen gut handhaben, sind die Anwender gegen das Device Fingerprinting machtlos. Cache-Elemente lassen sich zwar auch löschen, jedoch bieten hierfür gerade mobile Browser oft keine automatisierte Möglichkeit. Beide Probleme – Device Fingerprints wie ETags im Browsercache – sind nur durch die Browserhersteller in den Griff zu bekommen. Dabei könnte z. B. das komfortable, regelmäßige Löschen des Cache ein Kinderspiel sein; solche Optionen sind bei Desktop-Browsern seit Jahr und Tag etabliert.

Was ist zu tun?

Bei Browsern auf mobilen Plattformen besteht in Bezug auf die Datenschutzeinstellungen dringender Nachholbedarf.

10.2 Verschlüsselung nach TrueCrypt

„TrueCrypt ist unsicher." Entwickler der verbreiteten Festplattenverschlüsselung überraschten die Öffentlichkeit mit dieser Mitteilung im Mai 2014, ohne den genauen Grund zu benennen, weshalb diese Software nicht mehr genutzt werden soll. Zwecks Bekräftigung der Forderung nach einem Wechsel auf andere Kryptosysteme entfernten sie alle Downloadmöglichkeiten. Offiziell gibt es derzeit nur die eingeschränkte TrueCrypt-Version 7.2 zum Download, die lediglich bestehende Container entschlüsseln, nicht jedoch neue Dateien chiffrieren kann.

Die Warnung wirft Fragen auf. Der Umstand, dass TrueCrypt kürzlich einem umfangreichen Code Review unterzogen worden war, macht einen einfachen Softwarefehler – einen „Bug" – als Ursache unwahrscheinlich. Mehrere Erklärungen sind denkbar:

- Es handelt sich um eine Sicherheitslücke in einem zur Programmerzeugung notwendigen Drittanbieterprodukt, also einem Compiler oder einer Library. Die Entwickler könnten davon erfahren und erkannt haben, dass damit ihr eigenes Produkt kompromittiert ist.
- Es gibt gar keine Sicherheitslücke, die ein solches Vorgehen rechtfertigen würde, die Entwickler wollen sich vielmehr vom Projekt trennen.
- Die Entwickler wollen sich durch die Einstellung einer Einflussnahme durch Sicherheitsbehörden entziehen.

Die Verunsicherung unter den Nutzern von TrueCrypt ist groß. Als Alternative kommt auf Windows-Systemen Microsofts Bitlocker infrage und wird von den TrueCrypt-Entwicklern ausdrücklich empfohlen. Allerdings ist Bitlocker eine ClosedSource-Software. Die NSA hat auf den Hersteller Microsoft als US-Unternehmen Einflussmöglichkeiten. Die Software für die komplette Festplattenverschlüsselung als Bestandteil der Professional- bzw. Enterprise-Versionen der Windows-Betriebssysteme ist zudem für Privatnutzer nicht ohne Weiteres zugänglich.

Das BSI hat im Juni 2014 angekündigt, die in seinem Auftrag von der Firma Sirrix entwickelte Unternehmenslösung TrustedDisk mittelfristig als OpenSource-Software für Privatnutzer verfügbar zu machen. Zum Zeitpunkt der Erstellung dieses Berichts ist dies jedoch noch nicht erfolgt. Die vom BSI derzeit empfohlene Softwarekomponente GpgEX hat nicht den Funktionsumfang von TrueCrypt.

https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Datenverschluesselung/Praxis/Software/software_node.html

Die grundsätzliche Frage, die das TrueCrypt-Dilemma aufwirft, ist die nach dem Angreifer und dem daraus resultierenden geforderten Schutzniveau. Vor allem im Unternehmenseinsatz kommt es darauf an, welche Ressourcen ein Angreifer aufbringen kann. Wenn es gelingt, mithilfe von Social Engineering die Hardware im Unternehmen zu kompromittieren – z. B. durch Keylogger in Tastaturen, die Tastaturanschläge und damit auch die eingegebenen Passwörter aufzeichnen können –, ist Verschlüsselungssoftware obsolet. Ist der Angreifer ein Konkurrenzunternehmen und nimmt den Weg über die IT-Systeme, dürften gängige Verschlüsselungsverfahren wie GPG oder Software wie BoxCryptor, Bitlocker und – immer noch – TrueCrypt ausreichen. Das Risiko, dass Truecrypt in Zukunft gebrochen wird, gilt für jede andere Kryptosoftware. Nachweislich dauerhaft sichere Verschlüsselung gibt es mit Ausnahme von Onetime Pads nicht. Gegen Nachrichtendienste oder die Hersteller der eingesetzten Hardware ist kein sicheres kryptografisches Kraut gewachsen. Erstere haben nicht abschätzbare Ressourcen zur Verfügung, letztere kontrollieren den Fertigungsprozess und damit die Integrität der eingesetzten Hardware. Prüfbarkeit und Sanktionierbarkeit sind angesichts dieser beiden Angreifer weitgehend theoretische Konzepte.

Was ist zu tun?

Ein fortgeführter Einsatz von TrueCrypt bleibt eine Option. Die Berichterstattung zu TrueCrypt und zur Fortentwicklung der geplanten Alternativen sollte aber dringend verfolgt werden.

10.3 WhatsApp, Threema und Telegram – warum Verschlüsselung nicht alles ist

Als Facebook im Februar 2014 bekannt gab, den Dienst „WhatsApp“ zu kaufen, herrschte große Aufregung: „Der Datenkrake verleibt sich den hippen Messenger-Dienst ein und mit ihm all seine Nutzer.“ Nicht nur das ULD empfahl: Wechseln!

Als Alternativen kristallisierten sich schnell zwei Dienste heraus, die jeweils eine nennenswerte Nutzerbasis erringen konnten: Threema und Telegram. Daneben existieren weitere Dienste und Protokolle zum Versand von Kurznachrichten.

Die Unterschiede zwischen den Diensten liegen dabei weniger in ihrer Funktion, sondern im technischen Detail. Nur wenige beherrschen eine echte Verschlüsselung zwischen Kommunikationspartnern. Der Umgang mit Verkehrsdaten unterscheidet sich stark. Einen guten Überblick gibt die „Messaging Scorecard“ der Electronic Frontier Foundation vom November 2014:

https://www.eff.org/de/secure-messaging-scorecard

Die nächste Überraschung folgte Mitte November 2014, als WhatsApp ankündigte, eine vollständige Ende-zu-Ende-Verschlüsselung in sein Produkt zu integrieren. Geschehen soll dies auf Basis des TextSecure-Protokolls, das unter Sicherheitsaspekten aktuell als das Maß der Dinge angesehen wird.

Es drängt sich die Frage auf, ob damit die Forderung nach einem Wechsel weg von WhatsApp obsolet ist. Die genannte Form der Verschlüsselung ist zunächst absolut zu begrüßen, sofern sie fehlerfrei und ohne Hintertüren implementiert wird. Nutzende von WhatsApp könnten damit künftig sicher sein, dass die Inhalte ihrer Kommunikation weder von WhatsApp noch von übereifrigen Geheimdiensten oder anderen Lauschern mitgelesen werden. WhatsApp bleibt aber der Zugriff auf eine Menge von Daten. Dies gilt für das Telefonbuch, das der Nutzer zu WhatsApp hochlädt, um Kommunikationspartner zu identifizieren. Damit werden nach wie vor im großen Stil Daten unbeteiligter Dritter im Klartext in die USA übermittelt. Des Weiteren fallen Informationen über die Umstände der Kommunikation an. Wer zu welchem Zeitpunkt mit wem wie oft kommuniziert, zeichnet ein sehr genaues Bild des sozialen Geflechts der Nutzenden. Zum Zeitpunkt der Berichtsverfassung ist die Verschlüsselung nur für Android-Nutzer aktiv, andere Systeme sollen folgen. Es bleibt abzuwarten, ob WhatsApp die Verschlüsselung flächendeckend einführt und wie es sich zu den weiteren Datenschutzfragen positioniert.

Die beiden zuvor genannten großen Konkurrenten unterscheiden sich grundlegend von WhatsApp. Telegram setzt auf einen offenen Quellcode. Die eingesetzte Kryptografie steht jedoch bei Fachleuten seit Längerem in der Kritik. Auch werden standardmäßig alle Nachrichten lediglich Ende-zu-Server verschlüsselt und somit im Klartext auf den Servern der Telegram-Betreiber gespeichert, was die Benutzung mehrerer Geräte mit dem gleichen Account ermöglicht. Die Ende-zu-Ende-Verschlüsselung muss für jeden Kontakt separat aktiviert werden, Chatverläufe sind dann nur auf dem zugeordneten Gerät lesbar. Adressbuchdaten versendet und verarbeitet Telegram genau wie WhatsApp, nämlich im Klartext, womit auch hier die Daten unbeteiligter Dritter quer über den Globus geschickt werden.

Das Schweizer Unternehmen Threema bezeichnet seine gleichnamige Software als besonders sichere Alternative. Eine Verschlüsselung zwischen den Kommunikationspartnern ist hier immer aktiv. Interaktionsdaten über versendete Nachrichten werden nach Betreiberangaben nicht länger als für die Auslieferung notwendig gespeichert. Ein Telefonbuchabgleich ist bei Threema optional; wenn der Nutzer diesen aktiviert, werden die Daten nur als Hash übertragen. Die Nutzung von Threema ist im Unterschied zu WhatsApp und Telegram bei Bedarf auch gänzlich ohne Telefonnummer möglich. Adressiert werden Nutzer hier über eine sogenannte Threema-ID, die pseudonyme Kommunikation ermöglicht. Internetkontakten muss somit nicht zwangsweise die Handynummer anvertraut werden.

Echte Ende-zu-Ende-Verschlüsselung ist gut. WhatsApp-Nutzende sind damit eine Sorge los. Unbeobachtet oder pseudonym kommunizieren können sie trotzdem nicht. Der Anbieter kennt mit der Telefonnummer mindestens einen eindeutigen Identifikator. Ein Wechsel des Messengers ist also aus Datenschutzsicht nach wie vor sinnvoll.

Was ist zu tun?

Neben verlässlicher Ende-zu-Ende-Verschlüsselung sollten Nutzende bei der Wahl einer Messenger-Alternative Wert auf datensparsamen Umgang mit Metadaten legen.

10.4 STARTTLS und Perfect Forward Secrecy

Für den Versand von E-Mails gibt es unterschiedliche Protokolle zum Datentransfer. Bei dem Protokoll SMTP, mit dem Mails verschickt und zwischen Servern ausgetauscht werden, ist die Unterstützung von Verschlüsselung bereits seit Jahren Stand der Technik. Leider gibt es noch immer Mailserver, bei denen diese elementare Funktionalität nicht aktiviert ist.

Bereits im Jahr 1999 wurde das Kommando STARTTLS als Erweiterung des Mail-Protokolls in RfC 2487 – ein Standardisierungsdokument für das Internet – spezifiziert, das eine verschlüsselte Verbindung zur Übertragung der Kommunikationsinhalte initiiert. Seit ca. 2004 kann die Unterstützung des Kommandos als Stand der Technik angesehen werden, sodass es heute kein tragfähiges Argument mehr gibt, warum ein Betreiber die Funktionalität nicht unterstützt.

TLS – Transport Layer Security

TLS – früher unter dem Namen SSL (Secure Sockets Layer) bekannt – ist ein Verschlüsselungsprotokoll zur gesicherten Datenübertragung im Internet, das z. B. beim Mail-Versand oder beim Aufruf von Webseiten zum Einsatz kommt.

Insbesondere Behörden stehen in der Pflicht, die Vertraulichkeit und Integrität der E-Mail-Kommunikation nach dem Stand der Technik zu gewährleisten. Dies ist nicht möglich, wenn die Mailserver der Behörden noch auf „Internetsteinzeitniveau" konfiguriert sind. Sofern Dienstleister sich sträuben, Sicherheitsanforderungen nach dem Stand der Technik umzusetzen oder dafür gar einen Aufpreis verlangen, sollten diese gewechselt werden.

Leider gibt es hin und wieder Berichte über Antivirensoftware oder sogar böswillige Betreiber von Kommunikationsnetzen, die versuchen, den Aufbau von verschlüsselten Verbindungen zu sabotieren, um auf den Klartext der Kommunikationsinhalte zuzugreifen. Hier sollte auf andere Software und Betreiber ausgewichen werden.

Die Nutzung von Mail-Protokollen wie SMTP, IMAP oder POP3 hat mit der Nutzung von E-Mails über ein Webinterface im Browser erst mal nicht viel zu tun. Technisch unterscheidet sich Webmail nicht vom Aufruf sonstiger Webseiten. Aber auch hier sollte darauf geachtet werden, dass der Zugriff zum Webmail-Anbieter per TLS gesichert ist. Dies erkennt man daran, dass die URL mit https:// statt http:// beginnt. Grundsätzlich sollten persönliche Informationen oder gar Passwörter niemals über unverschlüsselt übertragene Webseiten eingegeben werden.

Verschlüsselung ist nicht unangreifbar. Insbesondere im letzten Jahr sind mehrere schwerwiegende Angriffe gegen SSL/TLS bekannt geworden, die Gegenmaßnahmen der Betreiber zwingend erfordern. So stellte sich u. a. heraus, dass der US-Geheimdienst NSA die amerikanische Standardisierungsinstanz NIST unterwandert hatte, damit vorsätzlich angreifbare Verschlüsselungsalgorithmen in Standards aufgenommen wurden. Betreiber von Servern sollten daher regelmäßig die Aktualität nicht nur der installierten Software, sondern auch der verwendeten Algorithmen überprüfen und gegebenenfalls hier nachjustieren.

Damit Angreifer, die irgendwann in den Besitz der Schlüsselinformationen eines Servers gelangen, nicht nachträglich die vorher mitgeschnittene Kommunikation aufdecken können, ist es wichtig, dass die Server PFS, Perfect Forward Secrecy, unterstützen.

PFS – Perfect Forward Secrecy

PFS beschreibt Verfahren, die sicherstellen, dass eine abgehörte Kommunikation auch dann nicht nachträglich entschlüsselt werden kann, wenn die geheimen (Server-)schlüssel in falsche Hände geraten.

Mit PFS wird der geheime Schlüssel des Servers nur verwendet, um für die jeweils aktuelle Datenübertragung einen jeweils neuen Sitzungsschlüssel (d. h. einen temporären Schlüssel) zwischen den beteiligten Rechnern auszuhandeln, der nach dem Ende der Kommunikation wieder gelöscht wird. Die eigentliche Datenübertragung wird mit dem Sitzungsschlüssel abgesichert. Dadurch können auch Angreifer mit Zugriff auf den Serverschlüssel im Nachhinein keine mitgeschnittene verschlüsselte Kommunikation aufdecken.

Was ist zu tun?

Bei jeglicher elektronischer Kommunikation sollte darauf geachtet werden, dass eine starke Verschlüsselung nach einem offengelegten und geprüften Verfahren eingesetzt wird. Betreiber von Mailservern sollten umgehend TLS-Verschlüsselung aktivieren, um zumindest Server-zu-Server-Verschlüsselung zu ermöglichen. Betreiber von Webservern sollten umgehend auf aktuelle Software umstellen, um Perfect Forward Secrecy zu ermöglichen. Software und verwendete Algorithmen sind regelmäßig dahingehend zu überprüfen, ob es nicht inzwischen erfolgreiche Angriffe dagegen gibt.

10.5 IT-Forensik – Wiederherstellung gelöschter Daten

Praktisch jeder Mensch besitzt heutzutage mindestens ein elektronisches Gerät, auf dem persönliche Daten abgespeichert sind. Neben dem klassischen Computer benutzen viele zusätzlich Notebook, Tablet oder Smartphone. Aufgrund der rasanten technischen Entwicklung werden diese Geräte immer schneller durch neuere Modelle ersetzt, wobei die „alten" Geräte verkauft oder weitergegeben werden. Dabei sollte stets bedacht werden, dass der neue Besitzer des Geräts Einblick in die persönlichen Daten nehmen kann, sofern diese zuvor nicht vollständig gelöscht wurden. Der Neubesitzer muss kein ausgebildeter Forensiker sein, um unzureichend gelöschte Daten des Vorbesitzers sichtbar zu machen. Es existiert eine große Anzahl an Werkzeugen, die eine Wiederherstellung von gelöschten Daten auch Laien ermöglicht.

Die Austauschrate gerade von mobilen Geräten steigt permanent. Das bisher vorhandene Gerät wird verkauft, verschenkt oder an den Provider zurückgegeben. Bei Regress- bzw. Serviceansprüchen kann ein Gerät beim Provider, beim Hersteller, beim Händler oder sogar bei einem externen Dienstleister landen. Nicht selten gelangen so Rückläufer wieder in den Handel, aus denen Daten des Vorbesitzers extrahiert werden können. Oftmals sehen die Routinen zum Wiederverkauf des Geräts nur eine Neuformatierung der Festplatte oder Neuinstallation des Betriebssystems vor. Beides genügt nicht, um das Wiederherstellen zuvor vorhandener Daten zu verhindern. Jeder Nutzer sollte deshalb selbst dafür sorgen, dass seine persönlichen Daten vollständig gelöscht sind, bevor eines seiner Geräte wieder in den Umlauf gebracht wird.

In der Computerforensik und bei der Datenrettung ist das Wiederherstellen von gelöschten Daten Tagesgeschäft. Eine große Anzahl von kommerziellen und freien Tools übernehmen diese Aufgabe unter Einsatz von zwei unterschiedlichen Techniken: Recovering und Carving. Ersteres bedient sich auf der Suche nach gelöschten Dateien des vorhandenen Dateisystems, indem dort im Verwaltungsbereich nach nicht – mehr – validen Datei-Einträgen gesucht wird. Das zweite Verfahren durchsucht den Datenträger (oder dessen Image) nach bekannten Dateistrukturen ohne Hilfe eines zugrunde liegenden Dateisystems. Das Recovering besticht dabei durch Schnelligkeit, das Carving weist eine höhere Wiederherstellungsrate auf.

Die im professionellen Umfeld eingesetzten kommerziellen Werkzeuge sind für den ambitionierten Laien nicht bezahlbar. Werkzeuge, die über Kommandozeilenbefehle gesteuert werden, wirken auf diesen zu sperrig bzw. unkomfortabel und werden somit zumeist ignoriert. Doch existiert eine Menge kostenloser Tools zur Datenwiederherstellung, die mit grafischer Bedienoberfläche und einfacher Handhabung um die Gunst der interessierten Nutzer buhlen. Auf den Webseiten der großen Computer-Online-Magazine werden solche Tools zum Herunterladen angeboten und finden große Resonanz bei den Nutzern. Darunter sind auch einige Softwareangebote zu finden, die sich auf die Wiederherstellung der Daten von defekten Datenträgern spezialisiert haben.

Grundsätzlich ist jeder damit in der Lage, unvollständig gelöschte Daten von gebrauchten Geräten oder Rückläufern wiederherzustellen. Die meisten Werkzeuge bieten eine deutschsprachige grafische Oberfläche, die den Nutzer schrittweise durch den Wiederherstellungsprozess leitet. Durch einfache Mausklicks kann die Wiederherstellung einer ganzen Partition oder von bestimmten Dateitypen

wie Bilder, Dokumente oder E-Mails ausgewählt werden. Ein Einblick in die persönlichen Daten des Vorbesitzers ist somit auch für jeden nicht professionellen Computernutzer ein Kinderspiel.

Was ist zu tun?

Von jedem elektronischen Gerät, mit welchem persönliche Daten bearbeitet wurden oder welches zur Kommunikation genutzt wurde, sollten vor Verkauf oder Rückgabe gründlich die eigenen Daten mit einem Löschprogramm gelöscht werden.

Um das Wiederherstellen von Daten zu verhindern, müssen diese also richtig gelöscht werden. Ein einfaches Verschieben in den Papierkorb mit anschließendem Löschen desselben ist hierzu nicht ausreichend, da nur die Einträge im Dateisystem als ungültig gekennzeichnet, nicht aber die Daten auf dem Datenträger selbst gelöscht oder überschrieben werden. Die Neuinstallation des Betriebssystems oder die Neuformatierung des Datenträgers genügt auch nicht, da nicht sämtliche vorher vorhandenen Daten überschrieben werden. Für das vollständige Löschen existieren kommerzielle und kostenlose Produkte, die den Nutzer dabei unterstützen und kein tiefer greifendes Computerwissen erfordern.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt die Werkzeuge Darik's Boot And Nuke (DBAN) oder Parted-Magic. Auf den Webportalen der großen Computerzeitschriften lassen sich eine Menge anderer freier Löschprogramme finden, ebenso entsprechende Apps für die Systeme iOS und Android.

Eine Beschreibung, wie Daten richtig gelöscht werden, ist auf der Webseite des BSI zu finden:

https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/RichtigLoeschen/richtigloeschen_node.html

11

KERNPUNKTE

Europäischer Gerichtshof

Safe Harbor

Internationale Kooperation

11 Europa und Internationales

Der Datenschutz in Schleswig-Holstein wird stark geprägt durch europäisches Recht. Die europäische Datenschutzrichtlinie aus dem Jahr 1995 musste vom Landesgesetzgeber umgesetzt werden, letztlich auch im Hinblick auf die Unabhängigkeit der Aufsichtsbehörde (34. TB, Tz. 1.1). Mit Artikel 8 der Europäischen Grundrechtecharta kam die EU dem nationalen Verfassungsgeber bei der expliziten Zusicherung eines Datenschutzgrundrechtes zuvor (Tz. 3.3). Die Rechtsprechung des Europäischen Gerichtshofes gewinnt immer mehr an praktischer Relevanz für die konkrete Anwendung des Datenschutzrechtes (Tz. 11.1). Die Europäische Datenschutz-Grundverordnung (EU-DSGVO) wird für private wie öffentliche Stellen direkt anwendbar sein (Tz. 2.2).

11.1 EuGH – ein neuer Motor der Datenschutzrechtsprechung

Das ULD wird von der schleswig-holsteinischen Verwaltungsgerichtsbarkeit nicht gerade verwöhnt. In verwaltungsrechtlichen Streitverfahren urteilte diese, dass das ULD für die Datenschutzkontrolle von US-Anbietern wie z. B. Facebook nicht zuständig sei, selbst dann nicht, wenn eine Stelle in Schleswig-Holstein die Dienstleistung des US-Anbieters in Anspruch nimmt (Tz. 7.1). In der Auseinandersetzung um die von Facebook erzwungene Klarnamenpflicht wurde dem ULD von den Gerichten des Landes bescheinigt, dass insofern deutsches Datenschutzrecht nicht anwendbar sei (Tz. 7.2).

Bessere Karten scheint der Datenschutz beim Europäischen Gerichtshof zu haben. Dieser urteilte im Mai 2014, dass Google als Suchmaschine in Spanien dem spanischen Datenschutzrecht und der lokalen Datenschutzaufsicht unterliegt. Die Urteilsgründe lassen sich auf viele US-Internetangebote – auch auf die in Schleswig-Holstein bereitgestellten und genutzten – übertragen. Damit wurde mit einem Schlag europaweit klargestellt, dass es nicht darauf ankommt, ob eine Niederlassung tatsächlich die Datenverarbeitung durchführt oder rechtlich beherrscht. In Vorwegnahme der insofern klaren EU-DSGVO gilt nach derzeit gültigem Recht das Marktortprinzip.

Diese Rechtsprechung hat auch Relevanz für die Frage der Verantwortlichkeit von Fanpage-Betreibern, die inzwischen zur Revision beim Bundesverwaltungsgericht (BVerwG) liegt (Tz. 7.1). Schon in der Vorinstanz hatte das ULD gegenüber dem Gericht angeregt, bei Unsicherheit über die Frage der datenschutzrechtlichen Verantwortlichkeit diese dem EuGH zur Beantwortung vorzulegen. Diese Anregung hat das ULD im Revisionsverfahren gegenüber dem BVerwG wiederholt. Der Antwort des EuGH käme eine europaweite Bedeutung zu. Angesichts der rechtlich bestehenden Unsicherheit würde so schnell Rechtsklarheit geschaffen.

Bisher war europaweit unbestritten das deutsche Bundesverfassungsgericht (BVerfG) Schrittmacher in der europäischen Rechtsprechung zum Datenschutz mit vielen Urteilen, u. a. dem Volkszählungsurteil von 1983, in dem das Recht auf informationelle Selbstbestimmung abgeleitet wurde, und dem Online-Durchsuchungsurteil von 2008, das ein Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme begründete. Neben das BVerfG ist nun der EuGH mit seinen Urteilen zu Google und im Februar 2014 zur Vorratsdatenspeicherung getreten: Im letzteren Urteil bestätigt der EuGH, dass eine Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten nur unter engen materiell-rechtlichen und prozessualen Voraussetzungen zugelassen werden kann. Im Juni legte der irische High Court dem EuGH die Frage nach der Verbindlichkeit des Safe-Harbor-Beschlusses der EU-Kommission aus dem Jahr 2000 vor (Tz. 11.3).

Was ist zu tun?

Besteht Unklarheit bei der Auslegung europäischen Datenschutzrechts, so sollten nationale Gerichte prüfen, ob sie die Frage nicht dem EuGH zur Beantwortung vorlegen wollen.

11.2 USA – unser Freund, Spion und Konkurrent

Das traditionell freundschaftliche Verhältnis Deutschlands zu den USA ist in Sachen Datenschutz schon lange getrübt. Weit vor den Enthüllungen von Edward Snowden (Tz. 2.1) war klar, dass staatliche wie private Kommunikationspartner in den USA kein Verständnis für Datenschutz und keinen Respekt für europäische Grundrechtsstandards zeigen – anders als viele US-Bürgerrechtsorganisationen und -aktivisten. Hinsichtlich digitaler Grundrechte gibt es offiziell keine US-europäische Wertegemeinschaft. Vielmehr demonstrieren US-Unternehmen wie US-Behörden, dass sie ihre globale sicherheitspolitische Dominanz bzw. ihr Profitstreben über die Achtung des Datenschutzes stellen. Dies zeigt sich bei sicherheitsbehördlichen Kooperationen, etwa dem Austausch von Bank- oder Fluggastdaten oder der Terrorismusbekämpfung. Ebenfalls deutlich wird dies bei auf dem europäischen Markt agierenden US-Internetunternehmen (34. TB, Tz. 11.4). Dies hat vertrauensmindernde Konsequenzen bei der Einschaltung von US-Dienstleistern, etwa im Rahmen der Auftragsdatenverarbeitung bzw. des Cloud Computing (Tz. 5.5; 34. TB, Tz. 11.5).

Aktuelles Beispiel für die reine Interessen- und fehlende Wertegeleitetheit der relevanten US-amerikanischen Stellen ist deren Versuch, über diplomatischen Einfluss und Lobbyarbeit das Datenschutzniveau der Europäischen Datenschutz-Grundverordnung, das dann europaweit auch für US-Unternehmen verbindlich sein wird, abzusenken (Tz. 2.2).

Ein weiteres Beispiel sind die Versuche von US-Administration und -Wirtschaft, auf die Verhandlungen zu einem transatlantischen Freihandelsabkommen zwischen den USA und der Europäischen Union Einfluss zu nehmen. Sie wollen, dass US-Unternehmen im Rahmen der „Trans-Atlantic Trade and Investment Partnership“ (TTIP) von datenschutzrechtlichen Bindungen freigestellt werden. Dies hätte eine Festschreibung des derzeitigen Wettbewerbsvorteils von US-Unternehmen gegenüber ihrer europäischen Konkurrenz zur Folge, die einer direkteren und wirksameren Datenschutzkontrolle unterliegt als bisher noch die Wettbewerber von Übersee. Ein Erfolg der Bestrebungen von US-Seite hätte ein Abweichen von Artikel XIV des GATS-Abkommens der Welthandelsorganisation WTO zur Folge, wonach Datenschutzregeln nicht als Handelshemmnis angesehen werden. Bisher ist nicht erkennbar, dass die europäische Seite dem US-amerikanischen Werben bei den TTIP-Verhandlungen folgen will.

https://www.datenschutzzentrum.de/artikel/772-.html

Was ist zu tun?

Das Verhältnis Deutschlands zu den USA, soll es eine Partnerschaft sein, muss sich an grundrechtlichen Werten orientieren.

11.3 Safe Harbor

Mit seiner „Safe Harbor"-Entscheidung erkannte die Europäische Kommission im Juli 2000 die vom US-Handelsministerium herausgegebenen „Grundsätze des sicheren Hafens zum Datenschutz" an und wollte damit eine verlässliche Grundlage für die Übermittlung personenbezogener Daten in die Vereinigten Staaten schaffen. US-amerikanische Unternehmen sollten nach Abgabe von Selbstverpflichtungen und bei Beachtung bestimmter Formalitäten als vertrauenswürdige Datenempfänger behandelt werden können.

Allerdings haben nicht erst die Erkenntnisse aus den Veröffentlichungen der Snowden-Dokumente Zweifel an der Wirksamkeit der Safe-Harbor-Grundsätze geweckt (32. TB, Tz. 11.4). Die Safe-Harbor-Grundsätze wurden in Evaluationen als zu unbestimmt kritisiert und die Einhaltung durch die teilnehmenden Unternehmen infrage gestellt (34. TB, Tz. 11.4). Die ungenügende Kontrolle durch das zuständige US-Handelsministerium wurde frühzeitig bemängelt. Das ULD hatte im August 2012 dem US-Handelsministerium eine ausführliche Aufstellung zu den Datenschutzverstößen durch die Facebook Inc. übersandt (34. TB, Tz. 7.1.4), hierauf aber niemals eine inhaltliche Reaktion erhalten.

Die bekannt gewordene Überwachung des weltweiten Datenverkehrs durch die NSA demonstriert, wie wirkungslos die Safe-Harbor-Grundsätze 14 Jahre nach ihrer Anerkennung durch die Kommission in der Praxis heute sind. Das massenhafte Auslesen von Daten aus Infrastruktursystemen US-amerikanischer Provider und die rechtsstaatlich nicht überprüfbaren Herausgabepflichten vieler US-amerikanischer Dienstleister haben zur Folge, dass in gerichtlichen und behördlichen Verfahren infrage gestellt wird, ob die Safe-Harbor-Grundsätze überhaupt noch eine Schutzwirkung für Betroffene entfalten können.

Die massenhafte Überwachung des Internets durch den amerikanischen Geheimdienst hat die Schutzwirkung der Safe-Harbor-Grundsätze praktisch aufgehoben.

Mit Blick auf die systematische Verletzung der Datenschutzrechte, denen die Nutzer amerikanischer Dienste ausgesetzt sind, haben die EU-Kommission in ihrer Mitteilung an das Europäische Parlament und den Rat vom November 2013, der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments in seinem Bericht vom Februar 2014 sowie die Artikel-29-Datenschutzgruppe in ihrer Stellungnahme 04/2014 vom April 2014 jeweils festgestellt, dass eine große Wahrscheinlichkeit dafür besteht, dass die Safe-Harbor-Grundsätze keinen angemessenen Schutz vor den anlasslosen und flächendeckenden Zugriffen der NSA gewährleisten können.

Demgemäß entschied der irische High Court in einem Verfahren gegen die irische Datenschutzaufsicht wegen der Datenverarbeitung von Facebook im Juni 2014, dem Europäischen Gerichtshof die Frage nach der Verbindlichkeit des Safe-Harbor-Beschlusses der EU-Kommission aus dem Jahr 2000 vorzulegen. Die Aufsichtsbehörden des Bundes und der Länder prüfen, ob und in welchem Umfang von der Möglichkeit Gebrauch gemacht werden kann, Übermittlungen nach Artikel 3 der Safe-Harbor-Entscheidung an amerikanische Organisationen auszusetzen. Danach können zuständige Behörden in den europäischen Staaten die Übermittlung an US-amerikanische Empfänger aussetzen, wenn etwa eine hohe Wahrscheinlichkeit dafür besteht, dass die Safe-Harbor-Grundsätze verletzt werden. Das ULD beteiligt sich an dieser Prüfung generell wie auch in einem konkreten Verfahren.

Was ist zu tun?

Das ULD wird prüfen, ob gegenüber Unternehmen in seinem Zuständigkeitsbereich von der Aussetzungsbefugnis Gebrauch zu machen ist.

11.4 Internationale Standardisierung

Die Standardisierung von Datenschutztechnologien gewinnt weiter an Bedeutung für den Grundrechtsschutz. In den Entwürfen zur Europäischen Datenschutz-Grundverordnung (EU-DSGVO) vorgesehene Aspekte können so konkretisiert werden. Diese sehen z. B. bei risikobehafteten Datenverarbeitungen Datenschutzfolgenabschätzungen (Data Protection Impact Assessments) vor. Der Parlamentsentwurf enthält Vorschläge, Datenschutzerklärungen durch grafische Symbole leichter verständlich zu machen. Verstärkt wird Bezug genommen auf den Stand der Technik („State of the Art"), ein Begriff, für dessen Auslegung oftmals auf technische Standards zurückzugreifen sein wird.

Das ULD hat im Rahmen seiner drittmittelfinanzierten Projektarbeit über sieben Jahre lang in verschiedenen Gremien der nationalen und internationalen Datenschutzstandardisierung mitgewirkt. Schwerpunkt der Arbeit war die Teilnahme an den Gremien der Internationalen Standardisierungsorganisation (ISO). Daneben brachte sich das ULD in Diskussionen beim World Wide Web Consortium (W3C) und der Internet Engineering Task Force (IETF) ein.

Ein zentraler Standard für die Arbeit in der ISO ist der Rahmenstandard „ISO/IEC 29100 – Privacy Principles". Aufbauend auf den in diesem Dokument beschriebenen Prinzipien wurden mehrere Projekte mit großer Praxisorientierung initiiert. So wurde ein Standard für Auftragsdatenverarbeiter in Cloud-Computing-Umgebungen veröffentlicht (ISO/IEC 27018); die Arbeit an einem Standard für Datenschutzfolgenabschätzungen (ISO/IECC 29134) dauert noch an. Jüngst initiierte zudem die japanische Standardisierungsorganisation JISC (Japanese Industrial Standards Committee) eine Untersuchung zur Entwicklung von Standards für Datenschutzerklärungen, die erhebliches Potenzial für die Vereinfachung solcher Erklärungen birgt.

Auf europäischer Ebene ergriff die französische Standardisierungsorganisation die Initiative für die Gründung einer Arbeitsgruppe zu Datenschutztechnologien innerhalb des europäischen Standardisierungskommitees (CEN). Zudem ist die Kooperation verschiedener Datenschutzbehörden, u. a. auch des ULD, im europäischen Netzwerk IPEN zu Datenschutztechnik im Internet zu nennen (Tz. 11.5).

Die Entwicklung von Datenschutztechnik und ihre Standardisierung ist dem ULD aufgrund von Drittmittelförderungen möglich. Sie gehört nicht zum traditionellen Kernauftrag der Arbeit von Datenschutzbehörden. Bedauerlicherweise ist daher die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit – anders als etwa ihre Kollegen aus Frankreich – in der internationalen technischen Standardisierung bisher nicht oder nur wenig präsent. Um der wachsenden Bedeutung technischer Standards gerecht zu werden, ist hier möglicherweise eine Ausweitung der Tätigkeiten zu erwägen.

Was ist zu tun?

Datenschutzexpertisen sollten bei der Standardisierung stärker einbezogen werden, insbesondere über Datenschutzbehörden, denen dafür ausreichende Mittel zur Verfügung zu stellen sind.

11.5 Technikgestaltung im Internet Privacy Engineering Network (IPEN)

Das Internet hat sich zum Rückgrat der Informationsgesellschaft gemausert und birgt eine Menge Risiken für den Datenschutz, was kein Wunder ist: Die meisten technischen Komponenten und Spezifikationen wurden nicht unter Datenschutzgesichtspunkten entwickelt, und „Privacy by Design" ist auch in den Anwendungen bislang viel zu wenig anzutreffen.

Angesichts dieser Situation hat der Europäische Datenschutzbeauftragte 2014 das „Internet Privacy Engineering Network" (IPEN) gegründet. Dieses

Netzwerk soll die Communitys der Entwickler und der Datenschutzexperten zusammenbringen. Beschäftigte bei Datenschutzbehörden mit Informatik- oder sonstigem technischen Hintergrund sollen sich einbringen, um zu helfen, Datenschutzfunktionalität in Internetanwendungen zu integrieren oder Datenschutztools zu implementieren: „Privacy Engineering". Vertreterinnen und Vertreter aus Unternehmen, der Open-Source-Community sowie Wissenschaft und Forschung sind in dem Netzwerk beteiligt. Das ULD, das sich bereits seit über 20 Jahren für Datenschutz durch Technik und für die Integration von Datenschutzanforderungen in allen Phasen der Systemgestaltung einsetzt, gehört zu den Gründungsmitgliedern von IPEN. Auch Kollegen der Datenschutzbehörden aus England, Frankreich, Irland und den Niederlanden sowie der Berliner Beauftragte für Datenschutz und Informationsfreiheit unterstützen das Team des Europäischen Datenschutzbeauftragten bei der IPEN-Initiative.

Zum Arbeitsprogramm von IPEN gehört die Entwicklung von wiederverwendbaren Bausteinen, Designmustern und sonstigen Komponenten für mehr Datenschutz. Es soll eine öffentliche Wissensdatenbank aufgebaut werden, die dokumentierte Best-Practice-Lösungen – von Konzepten bis zum Softwarecode – aufnimmt und bewertet. Vor allem zielt IPEN auf ein besseres Verständnis für Datenschutzfragen und technische Möglichkeiten ab. Dies ist für ein echtes „Privacy by Design" nötig. So kann IPEN Maßstäbe setzen für die Auslegung der kommenden Europäischen Datenschutz-Grundverordnung in Bezug auf „Privacy by Design" und „Privacy by Default". Das ULD wird hier insbesondere Ergebnisse aus den Modellprojekten (Tz. 8) und Erfahrungen aus dem Audit- und Gütesiegelbereich (Tz. 9) einbringen.

Das Internet Privacy Engineering Network tauscht sich per Mailinglist, in Telefonkonferenzen, auf Kollaborationsplattformen im Internet sowie in Veranstaltungen an verschiedenen Orten Europas aus. Es ist offen für alle Interessierten, die konstruktiv an einem verbesserten Datenschutz im Internet mitarbeiten möchten.

https://secure.edps.europa.eu/EDPSWEB/edps/lang/de/EDPS/IPEN

Was ist zu tun?

Das ULD wird sich weiterhin an IPEN beteiligen und lädt andere Datenschutzexpertinnen und -experten aus Wissenschaft, Industrie und Verwaltung sowie Systementwickler und andere Menschen aus der Praxis zur Mitarbeit ein.

11.6 eIDAS – elektronische Authentisierung und Identifizierung

Weitgehend unbemerkt von der Öffentlichkeit trat im Sommer 2014 die eIDAS-Verordnung in Kraft, die auf europäischer Ebene den Rechtsrahmen für elektronische Identifizierungsmittel und Signaturen definiert. Damit soll das Vertrauen in elektronische Transaktionen im Binnenmarkt gestärkt werden.

Noch sind viele Fragen offen, denn die konkreten Festlegungen werden großteils in weiteren Rechtsakten der Europäischen Kommission getroffen. Das ist unbefriedigend, weil die eIDAS-Verordnung vermutlich künftig erhebliche Auswirkungen auf die digitalen Lebensbereiche der Bürgerinnen und Bürger in der EU haben wird – zumindest hinsichtlich grenzüberschreitender Transaktionen. Die aus Datenschutzsicht besonders relevante elektronische Identifizierung der eIDAS-Verordnung adressiert zunächst den öffentlichen Bereich mit E-Government-Anwendungen, aber mit der aufzubauenden Infrastruktur soll auch der private Sektor erfasst werden.

Die elektronische Identifizierung wird wie folgt vorgesehen: Die EU-Mitgliedstaaten notifizieren ein oder mehrere ihrer national verwendeten eID-Systeme, die einem bestimmten Sicherheitsniveau genügen müssen. In Deutschland könnte dies beispielsweise der elektronische Personalausweis sein, der in anderen Ländern zurzeit nicht unterstützt wird (33. TB, Tz. 4.1.1). Dies soll sich ändern: Nach der eIDAS-Verordnung müssen die notifizier-

ten eID-Systeme von allen anderen Mitgliedstaaten für grenzüberschreitende Transaktionen, z. B. Behördendienste, anerkannt werden. So könnten deutsche Bürgerinnen und Bürger ihren elektronischen Personalausweis im E-Government etwa gegenüber französischen Behörden verwenden, beispielsweise bei einem Umzug nach Frankreich.

eIDAS-Verordnung

Bei der 2014 beschlossenen europäischen Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (EU-Verordnung Nr. 910/2014), auch bekannt unter dem Namen eIDAS-Verordnung, handelt es sich um den Nachfolger der Signaturrichtlinie von 1999. Sie geht im Anwendungsbereich aber weit darüber hinaus: Zusätzlich zu elektronischen Signaturen werden Methoden zur EU-weiten elektronischen Identifizierung und zu sogenannten Vertrauensdiensten normiert. Zu den Vertrauensdiensten gehören digitale Angebote zur Signaturerstellung und -validierung, zu elektronischen Siegeln, zur Zustellung elektronischer Einschreiben, zu Zertifikaten für die Website-Authentifizierung sowie Archivdienste für Signaturen, Siegel oder Zertifikate. Die eIDAS-Verordnung ist bereits in Kraft und gilt in großen Teilen ab Mitte 2016. In einigen Bereichen sind zunächst konkretisierende Rechtsakte zu erlassen.

Technisch notwendig ist dafür eine interoperable Infrastruktur, für die die eIDAS-Grundlage Anforderungen definiert. Die genaue Ausgestaltung ist noch offen. Eine naheliegende Realisierung bestünde darin, dass jeder Mitgliedstaat ein oder mehrere Gateways einrichtet, die in der grenzüberschreitenden Kommunikation zwischengeschaltet werden und die nachgewiesenen Identitäten konvertieren. Diese Idee der Identitätsvermittler spielt auch im Projekt FutureID (Tz. 8.2.2) eine zentrale Rolle. Die Mitgliedstaaten müssen gewährleisten, dass diese Gateways korrekt funktionieren. Aus Haftungsgründen läge es nahe, sämtliche grenzüberschreitende E-Government-Kommunikation – und bei Verwendung dieser Systeme im privaten Sektor auch solche Kommunikation – zu protokollieren.

Nachdem im ersten öffentlichen Entwurf der eIDAS-Verordnung Datenschutzfragen kaum eine Rolle gespielt hatten, wurde in der beschlossenen Version nachgelegt: Artikel 5 enthält den Hinweis auf die Einhaltung der EU-Datenschutzrichtlinie und stellt klar, dass die Benutzung von Pseudonymen bei elektronischen Transaktionen nicht untersagt werden darf. Die zu entwickelnde Infrastruktur muss die Umsetzung des Grundsatzes des „eingebauten Datenschutzes“ (Privacy by Design) fördern. Was das bedeutet und ob damit das Überwachungspotenzial der Identitätsvermittler zurückgestutzt wird, ist jedoch nicht klar.

Schon zu einem frühen Zeitpunkt wies das ULD auf dieses Risiko hin und mahnte zudem an, nicht stets eine volle elektronische Identifizierung vorzunehmen, sondern auch datensparsamere Authentisierungsmöglichkeiten zu ermöglichen. An einigen Stellen der Verordnung erfolgt nun der Verweis auf eine Authentifizierung: Es sollen nur solche Identifizierungsdaten verarbeitet werden, die für den Zugang zum Online-Dienst erforderlich sind – z. B. die Information „volljährig“ anstelle eines genauen Geburtsdatums. Da bislang außer dem deutschen Personalausweis kaum eines der verbreiteten nationalen eID-Systeme solche Datenreduktionen unterstützt, wird diese Idee aber womöglich ins Leere laufen. Abhilfe wäre möglich durch attributbasierte Berechtigungsnachweise (Tz. 8.2.1) – doch dafür müssten darauf aufbauende Verfahren von den Mitgliedstaaten zusätzlich notifiziert werden.

Was ist zu tun?

Bei der Definition der konkretisierenden Rechtsakte müssen Datensparsamkeitsprinzipien in den Vordergrund gestellt werden. Die europäischen Mitgliedstaaten sollten datenschutzfreundliche eID-Verfahren notifizieren.

11.7 Simulationsübung zu grenzüberschreitenden Datenschutzvorfällen

Gelangen personenbezogene Daten Dritten unrechtmäßig zur Kenntnis, spricht man von einem Datenschutzvorfall. Zumindest wenn es sich um sensible Daten handelt und daraus schwerwiegende Risiken für die Betroffenen resultieren, muss die verantwortliche Stelle die Aufsichtsbehörde und möglicherweise auch die Betroffenen unverzüglich informieren. Wie kann dies grenzüberschreitend funktionieren?

In der globalisierten Welt betreffen Datenschutzvorfälle häufig nicht nur eine Region, sondern zeigen Auswirkungen in mehreren Nationen. Dies war in der Vergangenheit beispielsweise der Fall bei international agierenden Auktionsplattformen im Internet, Telekommunikationsfirmen oder Anbietern von Online-Spielen oder Entertainment-Diensten. Die verantwortlichen Stellen unterliegen zwar in Europa der Meldepflicht über solche Vorfälle, doch gelangen häufig die Informationen – sofern überhaupt eine zeitnahe Benachrichtigung einer Aufsichtsbehörde stattfindet – nicht oder zu langsam an die Betroffenen. Die 2013 eingeführte EU-Verordnung 611/2013, welche die Benachrichtigungspflicht nach der E-Privacy-Richtlinie konkretisiert, fordert eine Zusammenarbeit der zuständigen nationalen Behörden in Fällen grenzübergreifender Verletzungen des Schutzes personenbezogener Daten.

Meldepflichten über Datenschutzvorfälle

Meldepflichten über Datenschutzvorfälle bestehen im Telekommunikationsrecht (§ 109a TKG), im Bundesdatenschutzgesetz (§ 42a BDSG) und auch in mehreren Landesdatenschutzgesetzen (z. B. § 27a LDSG Schleswig-Holstein). Für den Telekommunikationssektor erstreckt sich die Benachrichtigungspflicht seit 2009 auch auf den europäischen Bereich (Artikel 4 Abs. 3 E-Privacy-Richtlinie 2002/58/EG nach der Änderung von 2009); für sonstige personenbezogene Daten wird dies mit der europäischen Datenschutz-Grundverordnung geregelt werden.

Im Bereich der Informationssicherheit sind die positiven Effekte grenzüberschreitender Kooperationen bereits anerkannt. In Planspielen wird seit Jahren eingeübt, wie die Zusammenarbeit am besten funktioniert. Beispielsweise wurde Ende 2014 von der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) die große Cybersicherheitsübung „Cyber Europe 2014“ durchgeführt, an der mehr als 200 Organisationen und 400 Cybersicherheitsexperten aus 29 europäischen Ländern an einem Tag ein realitätsnahes Szenario simulierten. Initiiert vom Joint Research Centre im italienischen Ispra soll eine erste Kooperationsübung zu Datenschutzvorfällen im September 2015 erfolgen, allerdings in kleinerem Ausmaß – mit sieben Datenschutzbehörden.

Zur Vorbereitung fanden im Jahr 2014 mehrere Workshops statt, an denen das ULD gemeinsam mit den Datenschutzbehörden aus Frankreich, Griechenland, Irland, Italien, Polen und Spanien mögliche Szenarien erarbeitete. Es macht einen Unterschied, ob die Übung mit einer Meldung an eine Aufsichtsbehörde startet oder ob auf anderem Weg ein mutmaßlicher Datenschutzvorfall bekannt wird. Bei im Internet veröffentlichten Daten ist nicht immer unmittelbar klar, welche Stellen für den Vorfall verantwortlich sind, was die Klärung von Zuständigkeiten erschwert. Auch Probleme im Workflow werden zu lösen sein, z. B. die schnelle Erreichbarkeit der zuständigen Beschäftigten in den jeweiligen Aufsichtsbehörden auf einem sicheren Weg. Sprachbarrieren müssen überbrückt werden, ohne dass sich Ungenauigkeiten einschleichen, z. B. beim Übersetzen der Korrespondenz mit der Stelle, die ihrer Benachrichtigungspflicht nachgekommen ist. Zudem wird das Zusammenspiel mit Medienvertretern oder Strafverfolgungsbehörden rechtlich und kulturell unterschiedlich in den EU-Mitgliedstaaten gehandhabt.

Die Simulation im September 2015 soll einen Tag lang dauern, an dem im Zeitraffer die Ereignisse von etwa zwölf Tagen komprimiert werden. Das ULD wird sich beteiligen und die in der Übung gewonnenen Erfahrungen kommunizieren. Wichtig ist, dass alles dafür getan wird, um den möglichen Schaden für die Betroffenen zu minimieren – durch zeitnahe, akkurate Warnungen sowie Hilfestellungen, die darüber Auskunft geben, was jede und jeder tun kann, um sich zu schützen.

Was ist zu tun?

Um eine verbesserte grenzüberschreitende Kooperation bei Datenschutzvorfällen unter den Aufsichtsbehörden zu etablieren, sollten geeignete Verfahren definiert und eingeübt werden.

12

KERNPUNKTE

Verfahren des Informationszugangsgesetzes

Auskunftsverweigerungsgründe

12 Informationsfreiheit

Die Verbesserung der Transparenz in der Verwaltung wie im gesellschaftlichen Leben generell ist ein zentrales Thema der Landespolitik geworden. Hierzu gehören Überlegungen und Vorbereitungen zur Schaffung eines landesweiten Transparenzregisters (Tz. 1.3). Das Informationszugangsgesetz (IZG) bewährt sich in der Praxis (34. TB, Tz. 1.2) und erweist sich sogar als wirksames Instrument gegen die auskunftsunwillige Finanzverwaltung (Tz. 4.8.1). Dessen ungeachtet kann und muss das Recht weiterentwickelt werden. Hierzu gehören auch parlamentarische Initiativen zur Schaffung von mehr Informationsfreiheit in einzelnen Bereichen. Zu diesen wird das ULD regelmäßig gehört. Dies gilt für einen Antrag, die Informationsfreiheit im NDR-Staatsvertrag zu regeln, oder einen Gesetzentwurf zur Veröffentlichung der Bezüge der Mitglieder von Geschäftsführerorganen und Aufsichtsgremien öffentlicher Unternehmen.

http://www.landtag.ltsh.de/infothek/wahl18/umdrucke/2200/umdruck-18-2255.pdf

http://www.landtag.ltsh.de/infothek/wahl18/umdrucke/3700/umdruck-18-3756.pdf

http://www.landtag.ltsh.de/infothek/wahl18/umdrucke/3800/umdruck-18-3884.pdf

Das ULD nimmt an den zweimal jährlich stattfindenden Konferenzen der Informationsfreiheitsbeauftragten (IFK) teil, deren Tätigkeit vom Arbeitskreis Informationsfreiheit (AKIF) vorbereitet wird. Eine wichtige Funktion des AKIF ist es, die operative Arbeit der Informationsfreiheitsbeauftragten untereinander abzustimmen und, wo nötig, zu koordinieren. Die IFK verabschiedet Entschließungen zur Verbesserung der Informationsfreiheit in Deutschland. Deren Hauptadressaten sind die Gesetzgeber auf Bundes- und Landesebene.

http://www.lda.brandenburg.de/sixcms/detail.php?template=bbo_lda_sitzungen_dfb_d&_konf=bb1.c.281402.de&_aria=ae&_typ=Entschlie%C3%9Fung

12.1 IZG und immer wieder die Kostenfrage

In der Beratungspraxis des ULD zum IZG sind Kostenfragen sowohl für Antragsteller als auch für informationspflichtige Stellen immer wieder mit Unsicherheiten verbunden und somit eine Herausforderung. Das ULD hat eine Handreichung auf seiner Homepage veröffentlicht mit einer Zusammenfassung der wesentlichen Gerichtsentscheidungen und den Auskünften aus der Beratungspraxis des ULD.

https://www.datenschutzzentrum.de/artikel/857-.html

Am häufigsten wird gefragt, wann eine nach der Kostenverordnung zum IZG-SH kostenfreie „einfache Auskunft“ vorliegt. Hierbei ist auf den notwendigen Verwaltungsaufwand abzustellen. Zeitaufwände von einer halben bis zu einer Dreiviertelstunde sind noch als einfache und kostenfreie Auskunft zu behandeln.

12.2 Rechtsgutachten zur Vorbereitung von Entscheidungen

Das ULD befasst sich immer wieder mit der Frage, welche Unterlagen für den Schutz des behördlichen Entscheidungsprozesses wichtig sind (34. TB, Tz. 12.3). Geschützt sind ausschließlich solche Informationen, die es der informationspflichtigen Stelle ermöglichen, das Für und Wider einer Entscheidung umfassend zu würdigen und so unvoreingenommen zu einem Ergebnis zu gelangen. Maßgeblich ist allein der Verwendungszweck des Dokuments. Lässt eine Behörde zum Zwecke der Vorbereitung auf eine Entscheidung ein Rechtsgutachten anfertigen, das insbesondere Vorzüge, Nachteile und Risiken der unterschiedlichen Handlungsoptionen aufzeigt, dient dieses genau dem Zweck, alle Fakten unvoreingenommen würdigen zu können, und fällt deshalb unter den Schutz des behördlichen Entscheidungsprozesses.

Gegenüber dem Bundesrecht enthält das IZG keine Klarstellung, dass Gutachten und Stellungnahmen Dritter nicht der Entscheidungsvorbereitung dienen. Bloße Sachverhaltsdarstellungen und allgemeine rechtliche Ausführungen unterliegen auch nach Landesrecht voll der Auskunftspflicht. Bis zur Entscheidung dürfen zum Schutz interne Mitteilungen zurückgehalten werden, die unmittelbar den Abwägungsprozess betreffen und vorbereiten. Gerade bei Kommunen mit vielen ehrenamtlichen Entscheidungsträgern muss auf externe Gutachter als Helfer zur Entscheidungsfindung zurückgegriffen werden. Soweit diese in den Entscheidungsprozess einbezogen werden, rechtfertigt dies eine gesonderte Handhabung. Unmittelbar auf die Entscheidung gerichtete Inhalte eines beratenden Gutachters sollten in einem gesonderten Schriftstück übermittelt werden oder im Gutachten gekennzeichnet sein. Das Ergebnis des Entscheidungsprozesses und sämtliche Erwägungen unterliegen spätestens nach Abschluss des Entscheidungsprozesses umfassend dem Herausgabeanspruch.

Der Schutz behördlicher Entscheidungsprozesse wird oft zu Unrecht als Ausrede bemüht, um unliebsame Auskunftsansprüche abzuwehren. Bei der beratenden Einschaltung Dritter kann indes ein partielles Zurückhalten bis zum Zeitpunkt der Entscheidung gerechtfertigt sein.

12.3 Informationsherausgabe an Anonyme?

Immer wieder wird das ULD mit der Frage konfrontiert, ob unter Pseudonym oder per E-Mail gestellte Anträge wirksam sind. Informationspflichtige Stellen verweigerten die Bearbeitung, wenn Name und Adresse des Antragstellers nicht vorlagen. Teilweise wurde gar ein eigenhändig unterschriebener Antrag gefordert.

Das IZG sieht solche Voraussetzungen nicht vor. Jedermann hat Anspruch auf Informationen, die bei einer Behörde vorliegen. Eine bestimmte Form des Antrags ist nicht vorgeschrieben. Grenzen werden dem Anspruch lediglich zum Schutz überwiegender öffentlicher oder privater Belange gesetzt. Die Erteilung mündlicher oder einfacher schriftlicher Auskünfte mit der Herausgabe von bis zu zehn Duplikaten ist gebührenfrei. Zur Erfüllung der Aufgabe „Auskunft nach dem IZG“ ist weder zur Prüfung des Antrags noch zu Abrechnungszwecken die Erhebung der Identität erforderlich. Eine dahin gehende Nachfrage ist datenschutzwidrig. Der Behörde müssen aber Rückfragen zur Konkretisierung des Antrags und die Zustellung der Antwort möglich sein. Beides ist bei telefonischen Anfragen, bei digitalen Eingängen per E-Mail oder über eine vermittelnde Webseite möglich.

Ist nach erster Sichtung des Vorgangs absehbar, dass abrechenbare Kosten für die Auskunftserteilung entstehen, ist eine Rückfrage beim Antragsteller unter Bezifferung der voraussichtlichen Kosten geboten. Dabei ist zu berücksichtigen, dass einfache Anfragen kostenfrei zu erteilen sind (Tz. 12.1). Eine Vorleistungspflicht des Antragstellers für Gebühren besteht nach dem IZG nicht. Zwecks Sicherung des Gebührenanspruchs kann dann die Identität erfragt werden. Die informationspflichtige Stelle ist gehalten, soweit möglich eine anonyme Zahlung per Vorkasse in bar oder per Überweisung an ein Kassenzeichen zu ermöglichen.

Was ist zu tun?

Anonyme Anträge sind zu bearbeiten. Dies kann im IZG klargestellt werden; eine Regelung könnte die anonyme Abwicklung und Bezahlung vorsehen.

12.4 Wahlausschüsse und sonstige Gremien

Ein Kreiswahlausschuss verweigerte die Einsicht in die Niederschriften über seine Sitzungen. Er sei keine Behörde und damit nicht auskunftspflichtig. Gemäß dem IZG sind alle Behörden des Landes, der Gemeinden, Kreise und Ämter sowie der sonstigen juristischen Personen des öffentlichen Rechtes informationspflichtige Stellen. Der Behördenbegriff ist funktional zu verstehen und erfasst alle Stellen, die mit Verwaltung befasst sind. Ausnahmen bilden lediglich der Landtag, Gerichte, Strafverfolgungsbehörden, der Landesrechnungshof und oberste Landesbehörden, soweit letztere im Gesetzgebungsverfahren tätig werden. Die engen Ausnahmen vom Anwendungsbereich des IZG machen deutlich, dass die Tätigkeit von Wahlausschüssen dem Informationsanspruch unterliegt. Das Oberverwaltungsgericht Bremen entschied bereits im August 2011, dass wahlrechtliche Vorschriften und Wahlgrundsätze einer Einsicht Dritter in Wahlniederschriften nicht entgegenstehen. Der Wahlausschussleiter muss über entsprechende Anträge schon nach dem Wahlrecht nach pflichtgemäßem Ermessen entscheiden und bei Geltendmachung eines berechtigten Interesses die Einsichtnahme in der Regel gewähren.

Was ist zu tun?

Der Behördenbegriff des IZG ist weit zu verstehen. Ist eine Stelle nicht explizit vom IZG ausgenommen, ist ein Antrag schon mit Blick auf die neue Regelung in der Landesverfassung informationsfreundlich zu behandeln.

12.5 Kommunen sind keine Dokumenten-Lieferdienste

Oft, aber nicht immer kann das ULD auf eine Herausgabe der begehrten Information hinwirken. Nicht helfen konnte es einem Antragsteller, der einen Artikel aus einem Fachverlag für Kommunen begehrte. Ist eine Gemeinde Mitglied in dem Verband, der die Schriftenreihe herausgibt, erhält sie kostenlosen Online-Zugang zur Bibliothek. Für Externe ist der Artikel nur im teuren Einzelabruf erhältlich. Der Antragsteller suchte eine Mitgliedsgemeinde und stellte dort einen Antrag nach dem IZG. Die Gemeinde hatte den betreffenden Artikel selbst für eigene Zwecke noch nicht heruntergeladen. Wäre dem so gewesen und wäre der Artikel zu den Akten genommen worden, hätte der Anspruch dem Grunde nach bestanden. Als Ausschlussgrund hätte möglicherweise – je nach Schöpfungshöhe des Artikels – das Urheberrecht eingreifen können.

Informationen werden von einer informationspflichtigen Stelle „bereitgehalten“, wenn Dritte diese für die informationspflichtige Stelle vorhalten und ein rechtlicher Anspruch auf die Herausgabe besteht. Beispiele sind untere Behörden, die Informationen für die jeweilige Oberbehörde vorhalten, sowie Fälle des Outsourcing und der Aufgabenteilung. Nicht erfasst werden im Gegenzug Informationen bei Dritten, die keiner gesetzlichen Herausgabepflicht unterliegen.

12.6 Kein Anspruch auf digital signierte Dokumente

Ein Petent forderte, dass informationspflichtige Stellen bei elektronischer Auskunftserteilung gemäß dem IZG die übermittelten Dokumente zwecks Authentisierung mit einer qualifizierten elektronischen Signatur unterzeichnen. Das ULD musste ihm mitteilen, dass hierfür kein gesetzlicher Anspruch besteht. Es ist der Gesetzesbegründung zu entnehmen, dass die Auskunftserteilung wie die Ablehnung eines Antrags formfrei erfolgt und auch elektronisch möglich ist, ohne aber diesbezüglich weitere Vorgaben zu machen. Das IZG kann nicht dahin gehend verstanden werden, dass alle informationspflichtigen Stellen, also fast alle öffentlichen Stellen des Landes und der Kommunen, zur Bereithaltung einer Infrastruktur für die Erstellung qualifizierter Signaturen verpflichtet sind. Als praktischen Lösungsweg bis zur technischen Einführung elektronischer Signaturen bei den informationspflichtigen Stellen schlug das ULD vor, sich schriftlich bescheiden zu lassen und damit ein beweissicheres Dokument zu erlangen und vorab oder parallel um eine digitale Mitteilung zu bitten.

13

KERNPUNKTE

Sommerakademien

Schulungsbetrieb

13 DATENSCHUTZAKADEMIE Schleswig-Holstein

Gemäß dem Landesdatenschutzgesetz Schleswig-Holstein führt das Unabhängige Landeszentrum für Datenschutz Fortbildungsveranstaltungen zu den Themen „Datenschutz und Datensicherheit“ durch. Für die Konzeption und Organisation dieser Veranstaltungen ist seit 1993 die DATENSCHUTZAKADEMIE Schleswig-Holstein zuständig.

Neu * Neu * Neu * Neu * Neu

Einführung in IT-Systeme und IT-Komponenten für Anfänger

Dieser neue Kurs der DATENSCHUTZAKADEMIE hilft Ihnen, die IT-Infrastruktur Ihres Umfelds besser zu verstehen. Sie erlernen grundlegende Zusammenhänge der Datenverarbeitung und erkennen Datenschutz- und IT-Sicherheitsschwachstellen.

Neu * Neu * Neu * Neu * Neu

Im Schulungsjahr 2013 fanden 26 reguläre Kurse statt – zumeist jeweils zweimal pro Jahr –, in denen 371 Teilnehmende von zwölf Dozentinnen und Dozenten zu vielfältigen Themen von Datenschutz, Datensicherheit und Informationsfreiheit geschult wurden. 2014 betrug die Zahl der Teilnehmenden 355 in 23 Kursen.

Im Rahmen der „DATENSCHUTZAKADEMIE vor Ort“ nahmen in Inhouse-Sonderkursen 2013 und 2014 weitere 587 Personen an Fortbildungen zu folgenden Themen teil:

- BSI IT-Grundschutz/ISO
- Datenschutz für Schulsekretärinnen
- Beschäftigtendatenschutz
- Führung von Personalakten
- Das Informationszugangsgesetz SH
- IT-Sicherheit am Arbeitsplatz
- Datenschutz im Sozialamt
- Informationssicherheit für IT-Verantwortliche
- Datenverarbeitung in Betrieben der Handwerkerschaft
- Datenschutz in der Systemadministration
- Einführung in den Sozialdatenschutz
- Grundschutz und Grundschutztool
- Sicherer Serverbetrieb
- Datenschutzrechtliche Anforderungen bei der Durchführung von Maßnahmen für Sozialleistungsträger
- Datenschutz und Datensicherheit für Informatiklehrer
- Beschäftigtendatenschutz im privatwirtschaftlichen Bereich
- Datenschutz im Leistungs- und Vermittlungsbereich

Diese Inhouse-Veranstaltungen wurden von folgenden Stellen in Auftrag gegeben, wobei die acht erstgenannten „Stammkunden“ der DATENSCHUTZAKADEMIE sind:

- Ministerium für Landwirtschaft, Umwelt und ländliche Räume (MLUR/MELUR)
- Mürwiker Werkstätten
- TU Hamburg-Harburg
- Institut für Qualitätsentwicklung an Schulen Schleswig-Holstein (IQSH)
- IT-Planungsstab im Innenministerium SH
- Jobcenter Segeberg
- Kreis Herzogtum Lauenburg
- Amt Hohe Elbgeest
- Fortbildungsakademie der Wirtschaft (FAW)
- Jugendaufbauwerk der Kreishandwerkerschaft Stormarn gGmbH
- AON Versicherungsmakler GmbH
- Stadt Elmshorn
- Kommunales Rechenzentrum Niederrhein (KRZ), Kamp-Lintfort
- Kreis Nordfriesland
- Kreishandwerkerschaft Kiel
- Zentrales IT-Management SH

Sommerakademien

Die alljährlich am letzten Montag im August stattfindenden Sommerakademien der DATENSCHUTZAKADEMIE waren mit jeweils 500 Gästen im Atlantic

Hotel Kiel sowohl 2013 als auch 2014 ausverkauft. Mit den Themen „Big Data – Informationelle Fremd- oder Selbstbestimmung?!“ und „Supergrundrecht Sicherheit contra digitale Menschenrechte“ wurden aktuelle und brisante Themen aufgegriffen und fachkundig diskutiert. Deren Dokumentation findet sich unter:

https://www.datenschutzzentrum.de/sommerakademie/2014/

https://www.datenschutzzentrum.de/sommerakademie/2013/index.html

Aus dem Schulungsbetrieb

Die 2011 eingeführten Schülerkurse „Entscheide DU – sonst tun es andere für dich!“ haben sich in schleswig-holsteinischen Schulen herumgesprochen. Insgesamt 1.421 Schülerinnen und Schülern der Mittelstufenklassen aller Schultypen wurde in den vergangenen zwei Jahren vermittelt, wie sie mit ihren persönlichen Daten achtsam umgehen können. Aufgrund des großen Echos und des anhaltenden Bedarfs wurde eine ähnliche Informationsveranstaltung für Eltern ins Programm aufgenommen: „Entscheiden SIE – sonst tun es andere für Ihre Kinder!“ 80 Eltern ließen sich 2014 im ULD in puncto Medienkompetenz weiterbilden. Auch diese Infoveranstaltung wird im kommenden Jahr fortgeführt.

Der „Power-Lehrgang Datenschutz & Datensicherheit“ konnte leider wegen personeller Engpässe 2013/14 nicht wie geplant weiter angeboten werden. Damit fällt vorerst auch das Datenschutzzertifikat für Systemadministratoren weg. Die Erarbeitung von E-Learning-Methoden muss in diesem Zusammenhang ebenso storniert werden wie das Angebot von Linux- und Netzwerksicherheitskursen.

Die IT-Sicherheitskurse (unter Berücksichtigung der BSI-Grundschutztools) wurden weiter ausgebaut. Dazu gehören:

- IT-Sicherheitsmanagement
- Mit dem BSI-Grundschutztool zum IT-Sicherheitskonzept
- IT-Grundschutz nach BSI

Datenschutzkontrolle, Sicherheitschecks und Datenschutzaudits

Die Absolventen werden dort befähigt, die Sicherheit von Verfahren oder Geschäftsprozessen und die Verwaltung von IT-Verbünden von Organisationen mithilfe der IT-Grundschutzmethode umzusetzen. Neu in diesem Bereich sind die Kurse „Einführung in IT-Systeme und IT-Komponenten für Anfänger“ sowie „Mit dem Grundschutztool ‚Verinice‘ zum IT-Sicherheitskonzept“.

Die traditionellen behördlichen Grundlagenkurse der DATENSCHUTZAKADEMIE werden weiterhin gut angenommen, seien dies „Datenschutzrecht/Datensicherheit für behördliche Datenschutzbeauftragte“, „Einführung Datenschutz im Schulsekretariat“ oder „Führung von Personalakten“, „Rechtsfragen des Landesdatenschutzgesetzes“ oder „Informationszugangsgesetz SH“.

Kontinuierlich wachsenden Zuspruch erfährt der dreitägige Lehrgang „Betrieblicher Datenschutz Kompakt“, der in handlungsoptimierter und praxisbezogener Form betrieblichen Datenschutzbeauftragten einen guten Start in ihre Tätigkeit bietet. Von ursprünglich zwei Terminen pro Jahr ist der Kurs mittlerweile auf vier Jahrestermine bei guter Auslastung gediehen. In den weiteren Angeboten zum privatwirtschaftlichen Sektor vermitteln engagierte Dozentinnen und Dozenten „Beschäftigtendatenschutz“, „Kundendatenschutz“, „Workshop für betriebliche Datenschutzbeauftragte“ und „Datenschutz in Internet und Social Media“.

„Datenschutz im Krankenhaus“ und „Datenschutz in der Arztpraxis“ sind mangels Resonanz 2013 zum Kurs „Datenschutz im Medizinbereich“ zusammengefasst worden. Trotz zunehmender Datenschutzsensibilisierung im medizinischen Bereich und trotz erheblichem Bedarf erfahren die Kurse nicht die ihnen zustehende Beachtung seitens der Verantwortlichen. Dies trifft auch auf die Kurse „Datenschutz in Pflegeheimen und Pflegediensten“ sowie „Datenschutz in der Jugendhilfe“ zu.

Dagegen werden Sonderkurse mit speziell auf den Auftraggeber zugeschnittenen Themen im Sozialbereich regelmäßig nachgefragt: Jobcenter, Pflegedienste und Behinderteneinrichtungen buchen für ihre Mitarbeitenden Fortbildungsveranstaltungen zu Themen des Sozialdatenschutzes – wenngleich dies aus Kostengründen oft nur halbtägige Infoveranstaltungen sind.

Das Jahresprogramm der DATENSCHUTZAKADEMIE finden Sie unter

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

auf der Homepage des Unabhängigen Landeszentrums für Datenschutz (ULD).

Index

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z