ULD

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein

TÄTIGKEITSBERICHT
2013

ULD – SCHLESWIG-HOLSTEINS SERVICEZENTRUM FÜR DATENSCHUTZ UND INFORMATIONSZUGANG

Tätigkeitsbericht 2013
des Unabhängigen Landeszentrums
für Datenschutz Schleswig-Holstein

BERICHTSZEITRAUM: 2011/2012

REDAKTIONSSCHLUSS: 15.02.2013

LANDTAGSDRUCKSACHE 18/555

(34. 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

1	**DATENSCHUTZ UND INFORMATIONSFREIHEIT IN SCHLESWIG-HOLSTEIN**	**9**
1.1	LDSG „die erste, die zweite …“	9
1.2	Informationszugangsgesetz Schleswig-Holstein – IZG-SH	10
1.3	Erwägungen zu einem Transparenzgesetz	11
1.4	Erwartungen des ULD an Landtag und Regierung	12
1.5	Öffentliche Stellen und das Betreiben einer Facebook-Fanpage	12
2	**DATENSCHUTZ – NATIONAL UND GLOBAL**	**15**
2.1	Internetgesetzgebung	15
2.2	Datenschutz bei Social Media	16
2.3	Stiftung Datenschutz	18
2.4	Beschäftigtendatenschutz	19
2.5	EU-Rechtsrahmen – Entwurf einer Datenschutz-Grundverordnung	19
3	**DIE DIENSTSTELLE**	**23**
3.1	Das Konzept des ULD	23
3.2	Neue Zuständigkeit für die Verfolgung von Ordnungswidrigkeiten	24
3.3	Öffentlichkeitsarbeit	24
3.4	Social-Media-Dienstvereinbarung	25
4	**DATENSCHUTZ IN DER VERWALTUNG**	**27**
4.1	Allgemeine Verwaltung	27
4.1.1	Entwurf eines E-Government-Gesetzes des Bundes	27
4.1.2	Outsourcing öffentlich-rechtlicher Forderungen an private Inkassobüros	28
4.1.3	Geodaten und Verhaltenskodex	29
4.1.4	Geodaten und das Geodateninfrastrukturgesetz (GDIG)	29
4.1.5	Einheitliches Zeitwirtschaftssystem der Landesverwaltung	30
4.1.6	KoPers – ein neues Personalmanagementsystem	31
4.1.7	Übertragung von IT-Dienstleistungen auf einen Zweckverband	32
4.1.8	Kommunaler Bürgerservice – Nutzung von eIDs	34
4.1.9	Bürgerbegehren und der Umgang mit Unterschriftenlisten	35
4.1.10	Was bringt das neue Bundesmeldegesetz?	36
4.1.11	Externe Dienstleister als behördliche Datenschutzbeauftragte?	37
4.2	Polizei und Verfassungsschutz	38
4.2.1	@rtus beschäftigt die Polizei – und das ULD	38
4.2.2	Sicherheitsüberprüfungen	40
4.2.3	Gemeinsames TKÜ-Zentrum Nord	40
4.2.4	Sicherheitsbehörden in sozialen Netzwerken: Öffentlichkeitsfahndung	41
4.2.5	Umgang mit Auskunftssperren im Melderegister in Strafverfahren	42
4.2.6	Was für die Polizei INPOL ist, ist für die Dienste NADIS – in neuem Gewand	43
4.2.7	Entwicklungen im Verfassungsschutz	44
4.2.8	Neuorganisation der behördlichen Datenschutzbeauftragten der Polizei	45
4.2.9	Die Polizei als Informant des Arbeitgebers	46

4.3	Justizverwaltung	46
4.3.1	Der Staatstrojaner ohne rechtliche Grundlage	46
4.3.2	Anordnung von Blutproben – Richtervorbehalt stärken statt abschaffen	47
4.3.3	MESTA – erste Fortschritte	48
4.3.4	Sicherstellung von Datenträgern im Strafverfahren	49
4.3.5	Therapieunterbringungsvollzugsgesetz	50
4.3.6	Sicherungsverwahrungsvollzugsgesetz	50
4.3.7	Einführung eines bundesweiten Vollstreckungsportals	51
4.3.8	Dokumentation von Grundbucheinsicht	52
4.3.9	Gerichtsvollzieher-Durchsuchungen in Abwesenheit des Schuldners	53
4.3.10	Protokollierung (auch) der lesenden Zugriffe im Justizvollzug	53
4.4	Ausländerverwaltung	54
4.4.1	Visa-Warndatei	54
4.4.2	Daten über EU-Bürger im Ausländerzentralregister	55
4.5	Soziales	55
4.5.1	Das Ende von ELENA	55
4.5.2	ULD kein Ansprechpartner für AOK, MDK und Jobcenter mehr – und nun?	56
4.5.3	Arbeitslosengeld II – Kopien von Kontoauszügen und Personalausweisen	56
4.5.4	TK-Ärztezentrum – ein störrischer Patient	57
4.5.5	Kindervernachlässigung in Segeberg – Wer kontrolliert das Jugendamt?	58
4.5.6	Leumundsanfrage bei Tagesmüttern und ärztliches Attest von Pflegeeltern	58
4.5.7	Wiener Übereinkommen: Daten vom Jugendamt fürs Konsulat	59
4.5.8	Willkommensbesuche des Jugendamtes bei Familien mit Neugeborenen	60
4.5.9	Aufbewahrung von Betreuungsakten	60
4.6	Schutz des Patientengeheimnisses	61
4.6.1	Hausarztzentrierte Versorgung	61
4.6.2	Privatärztliche Verrechnungsstelle und Einwilligung der Patienten	61
4.6.3	Nationales Krebsregister	62
4.6.4	Klinisches Krebsregister Schleswig-Holstein	63
4.6.5	Apothekerverband und Clearingstelle	64
4.6.6	Patientenarmbänder – Sicherheit auf Kosten des Patientengeheimnisses?	64
4.6.7	Elektronische Gesundheitskarte – Was kann sie wirklich?	65
4.7	Wissenschaft und Bildung	66
4.7.1	Schulen und Facebook	66
4.7.2	LanBSH mausert sich zur „Allzweckwaffe“ für mehr Effizienz	67
4.7.3	Neue Möglichkeiten des EDV-Einsatzes in der Schule – neue Fragen	67
4.7.4	Handreichung für die Schulsozialarbeit	68
4.7.5	Regeln für die Videoüberwachung in Schulen	68
4.7.6	Tausche Fingerabdruck gegen Schulmittagessen	69
4.7.7	Zwischen Schule und Beruf – datenschutzkonformes Übergangsmanagement	69

4.8	Steuerverwaltung	70
4.8.1	Die Steuerverwaltung ohne Auskunftsanspruch	70
4.8.2	Zusendung falscher Steuerunterlagen	71
5	**DATENSCHUTZ IN DER WIRTSCHAFT**	**73**
5.1	Datenschutz in der Versicherungswirtschaft	73
5.1.1	Hinweis- und Informationssystem der Versicherungswirtschaft (HIS)	73
5.1.2	Einwilligungs- und Schweigepflichtentbindungserklärung	74
5.1.3	Verhaltensregeln – der „Code of Conduct“	77
5.2	Geldkarten mit Funkchips	78
5.3	Elektronisches Lastschriftverfahren – der Kunde bezahlt mit seinen Daten	80
5.4	Geldwäsche nicht um jeden Preis	81
5.5	Der gläserne Mietinteressent	82
5.6	Einwilligungen, Bonitätsabfragen und öffentlicher Personennahverkehr	83
5.7	Orientierung in der Datenwolke	84
5.8	Dopingbekämpfung	85
5.9	Einzelfälle	86
5.9.1	Teure Datensammlung ohne Überblick	86
5.9.2	Berechtigungen für Bankmitarbeiter und Handelsvertreter	87
5.9.3	Aufzeichnen von Gesprächen in Callcentern	88
5.9.4	Ohne Führungszeugnis kein Sport	89
5.9.5	Sensible Daten auf dem Kontoauszug	89
5.9.6	Maßnahmen gegen volle Briefkästen	90
5.9.7	Umfang der Auskunftspflicht gegenüber dem ULD	91
5.9.8	Geldinstitute als Daten-Banken	91
5.9.9	Löschpflichten bei Verkauf gebrauchter Mobiltelefone	92
5.9.10	Videoüberwachung an Tankstellen	93
5.9.11	Überwachung von Kuchen und Broten	94
6	**SYSTEMDATENSCHUTZ**	**97**
6.1	Mandantenfähigkeit	97
6.2	Zusammenarbeit auf Landesebene	98
6.3	Zusammenarbeit auf Bundesebene	99
6.3.1	KoSIT-Beirat	99
6.3.2	Informationssicherheitsleitlinie (ISMS) für Bund, Länder und Gemeinden	100
6.3.3	XTA	100
6.4	Ausgewählte Ergebnisse aus Vorabkontrollen	101
6.4.1	Vorabkontrollen sind gebührenpflichtig	101
6.4.2	KoPers	102
6.4.3	BAföG21	102
6.4.4	forumSTAR	103

6.5	Ausgewählte Ergebnisse aus Prüfungen	104
6.5.1	Nachkontrollen	104
6.5.2	Prüfung der Verfahrensverzeichnisse	105
6.5.3	Öffnen persönlicher E-Mail-Postfächer während einer Prüfung	106
6.6	Beratung des Rechenzentrums der CAU	107
6.7	Intelligente Energieversorgung: Smart Meter	108
7	**NEUE MEDIEN**	**111**
7.1	Facebook	111
7.1.1	Die Verantwortlichkeit der Webseitenbetreiber bei Facebook Insights	111
7.1.2	Facebook – Verfahren zur automatischen Erkennung von Gesichtern	112
7.1.3	Facebook – Aufgabe der Pseudonymität oder Kontosperrung	113
7.1.4	Facebook – Verstoß gegen die Safe Harbor Principles	115
7.2	IPTV – die Sicht auf den Fernsehkonsum aus der Nähe	116
7.3	Verhaltensbasierte Werbung – Online Behavioural Advertising	117
7.4	Rundfunkänderungsstaatsvertrag	118
8	**MODELLPROJEKTE UND STUDIEN**	**121**
8.1	PrimeLife	121
8.2	ABC4Trust – vertrauenswürdige digitale Identifikation im Pilotversuch	122
8.3	FutureID – Wie soll die Zukunft von elektronischen Identitäten aussehen?	123
8.4	TClouds – Trustworthy Clouds	124
8.5	Datenschutz-Auskunftsportal	125
8.6	Anfragen zu Datenschutz in Online-Spielen nehmen zu	126
8.7	SurPRISE – Sicherheit versus Privatsphäre aus Bürgersicht	127
8.8	Multi-Biometrische 3D-Gesichtserkennung	127
8.9	MonIKA – Erkennung und Bekämpfung von Botnetzen und Cyber-Angriffen	128
9	**AUDIT UND GÜTESIEGEL**	**131**
9.1	Datenschutzaudits	131
9.1.1	KVSH	131
9.1.2	Kreis Plön	132
9.1.3	„ZIAF“ – Landwirtschaftsministerium	133
9.1.4	Nordbits	133
9.1.5	Statistikamt Nord	134
9.2	Datenschutz-Gütesiegel Schleswig-Holstein	135
9.2.1	Abgeschlossene Gütesiegelverfahren	135
9.2.2	Sachverständige und Prüfstellen	136
9.2.3	Überarbeitung des Gütesiegel-Anforderungskatalogs	137
9.2.4	Zusammenarbeit mit EuroPriSe	137
9.3	EuroPriSe – europäisches Datenschutz-Gütesiegel	138
9.3.1	Zertifizierungskriterien	138
9.3.2	Fachinformationen für EuroPriSe-Gutachter und Antragsteller	138
9.3.3	Zertifizierungsverfahren	139

9.3.4 Zulassung von Gutachtern 140
9.3.5 Zertifizierung und Rezertifizierung 141
9.3.6 Zusammenarbeit mit anderen Datenschutzbehörden 144

10 AUS DEM IT-LABOR 147
10.1 Bring Your Own Device 147
10.2 Browsersicherheit – aktuelle Empfehlungen 148
10.3 Schnittstellensicherheit 149
10.4 Windows Server 2012 und Windows 8 150

11 EUROPA UND INTERNATIONALES 153
11.1 Europäische Regulierung 153
11.2 Artikel-29-Datenschutzgruppe 154
11.3 Artikel-29-Datenschutzgruppe zu Cloud Computing 154
11.4 Datenschutz in den USA 155
11.5 Der Zugriff der USA auf europäische Daten 156
11.6 Internationale Standardisierung 157

12 INFORMATIONSFREIHEIT 159
12.1 Eckpunktepapier zu Open Data 159
12.2 Informationsfreiheit in der Verwaltung 160
12.3 Stellungnahme oder internes Arbeitspapier? 160
12.4 IZG-SH und Einsicht in Steuerakten 160
12.5 Zugang zu Kaufverträgen 161

13 DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN 163

Index 166

01

KERNPUNKTE

Landesdatenschutzgesetz

Mehr Transparenz im Land

1 Datenschutz und Informationsfreiheit in Schleswig-Holstein

Die Jahre 2011 und 2012 brachten eine Vielzahl von Veränderungen für den Datenschutz und die Informationsfreiheit in Schleswig-Holstein: Das Landesdatenschutzgesetz (LDSG) wurde zweimal novelliert. Das Informationsfreiheitsgesetz und das Umweltinformationsgesetz wurden in einem Informationszugangsgesetz (IZG-SH) zusammengefasst. Beim Einsatz von Informationstechnik in der Landesverwaltung erfolgt eine zunehmende Standardisierung und Vereinheitlichung und zugleich eine verstärkte Nutzung von Internettechnologie, was eine Anhebung des Datenschutzniveaus sowie eine verbesserte Bürgerorientierung durch Kommunikations- und Informationsangebote ermöglicht. Dieser technische wie normative Prozess ist nicht abgeschlossen und macht weitere politische und administrative Anstrengungen nötig. Durch die zunehmende Bereitschaft, auch der Verwaltung, Angebote insbesondere von US-amerikanischen Internetanbietern zu nutzen, eröffnen sich neue Risiken für den Datenschutz.

1.1 LDSG „die erste, die zweite …“

Aufgrund eines Urteils des Europäischen Gerichtshofes (EuGH) vom 9. März 2010 (Rs. C-518/07) zur Unabhängigkeit der Datenschutzaufsichtsbehörden musste das Landesdatenschutzgesetz (LDSG) bis Oktober 2011 geändert werden. Das Land Schleswig-Holstein setzte die Änderungen mit einem Gesetz vom 30. September 2011 um. Danach kann das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) als Anstalt des öffentlichen Rechts in keinem Bereich mehr Weisungen unterworfen werden und ist so in noch stärkerem Maße unabhängig.

Der EuGH stellte mit seinem Urteil fest, dass die deutsche Datenschutzaufsicht entgegen der EG-Datenschutzrichtlinie ihre Aufgaben nicht in völliger Unabhängigkeit wahrnahm. Sie unterlag in den einzelnen Bundesländern in unterschiedlicher Weise der Fach-, Rechts- und Dienstaufsicht, was einen Verstoß gegen die Richtlinie bedeutete. Der EuGH befürchtete, dass staatliche Aufsicht – gleich welcher Art – es ermögliche, auf Entscheidungen der Datenschutzaufsichtsbehörden mittelbar und unmittelbar Einfluss zu nehmen. Das ULD als Aufsichtsbehörde über nicht öffentliche Stellen unterliegt nunmehr weder der Rechtsaufsicht des Innenministeriums noch einer Fachaufsicht.

Durch die neu geschaffene Abwahlmöglichkeit der oder des Landesbeauftragten für Datenschutz mit qualifizierter Mehrheit, die nur bei besonders schwerwiegenden Gründen zur Anwendung kommen soll, wurde die Verantwortung des Parlaments gestärkt. § 36 Abs. 4 LDSG sieht die Möglichkeit des Landtags und seiner Ausschüsse vor, die Anwesenheit der oder des Landesbeauftragten für Datenschutz zu verlangen. Damit wird sichergestellt, dass das Parlament jederzeit Auskünfte zur Tätigkeit des ULD verlangen kann.

Diesen organisationsrechtlichen Änderungen folgte am 27. Januar 2012 eine zweite Novelle des LDSG mit wichtigen neuen materiell- sowie verfahrensrechtlichen Regeln. In erster Linie ging es darum, das LDSG an neue technische Gegebenheiten anzupassen. Das LDSG enthält in § 5 nun in Weiterentwicklung der bisherigen technisch-organisatorischen Maßnahmen moderne Datenschutz-Schutzziele: Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettbarkeit und Intervenierbarkeit. In § 7 LDSG werden alle datenverarbeitenden Stellen verpflichtet, Verfahrensverzeichnisse zu veröffentlichen. Haben datenverarbeitende Stellen keinen behördlichen Datenschutzbeauftragten nach § 10 LDSG bestellt, führt das ULD ein Verzeichnis der Meldungen. Diese Verfahrensverzeichnisse enthalten wesentliche Angaben zum Verfahren, zum Zweck und zur Rechtsgrundlage des Verfahrens sowie die geplanten Datenübermittlungen und die allgemeinen Beschreibungen der nach den §§ 5 und 6 LDSG zur Einhaltung der Datensicherheit getroffenen Maßnahmen. Das ULD veröffentlicht die Verfahrensverzeichnisse auf seiner Internetseite.

In § 8 LDSG wurde eine Regelung zu gemeinsamen Verfahren und Abrufverfahren aufgenommen. Erstmalig ist geregelt, dass 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 kann. Die zentrale Stelle sowie Einzelheiten über Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung werden durch Verordnung der für das Verfahren zuständigen obersten Landesbehörde bestimmt. Ein derartiges Verfahren wird in Schleswig-Holstein in der Personalverwaltung des Landes mit dem Personalverwaltungssystem KoPers eingerichtet werden (Tz. 4.1.6).

Die Regelungen zur Videoüberwachung in § 20 LDSG wurden den heutigen technischen Gegebenheiten angepasst.

Erstmalig wird nun im LDSG die Veröffentlichung von Daten im Internet geregelt. Gemäß § 21 LDSG ist eine Veröffentlichung personenbezogener Daten im Internet nur zulässig, wenn diese Form der Veröffentlichung durch eine Rechtsvorschrift erlaubt ist oder wenn die oder der Betroffene in diese Form der Veröffentlichung eingewilligt hat. In Bezug auf Mandatsträger- und Funktionsträgerdaten ist die Veröffentlichung zulässig, wenn keine überwiegenden schutzwürdigen Interessen entgegenstehen. Internetveröffentlichungen sind zu befristen und dürfen einen Zeitraum von fünf Jahren nicht überschreiten. Die öffentlichen Stellen werden verpflichtet, schon bei Einstellung personenbezogener Daten ins Internet Löschfristen zu setzen.

Innovativ ist § 27a LDSG, wonach datenverarbeitende Stellen eine Informationspflicht trifft, wenn bei ihnen gespeicherte personenbezogene Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Die datenverarbeitende Stelle hat dies unverzüglich den Betroffenen und dem Unabhängigen Landeszentrum für Datenschutz mitzuteilen – die sogenannte Breach Notification. Anwendungsgebiete für derartige Informationspflichten sind der Verlust von USB-Sticks, externen Festplatten, Laptops oder die unzulässige, wenn auch nicht beabsichtigte Veröffentlichung von personenbezogenen Daten im Internet.

Die Serviceaufgaben des ULD wurden erweitert. Eine Behörde kann jetzt auch ohne ein Behördenaudit ihre technisch-organisatorischen Verfahren durch das ULD prüfen lassen. Führt das ULD für Behörden des Landes Schleswig-Holstein Vorabprüfungen durch, so sind diese gebührenfähig (§ 43 Abs. 4 LDSG).

Einige weiter gehende Vorschläge, wie die verpflichtende Bestellung eines behördlichen Datenschutzbeauftragten für Behörden des Landes Schleswig-Holstein, fanden keine Berücksichtigung bei dieser Novellierung des LDSG. Immer noch fehlt eine gesetzlich geregelte einheitliche Zuständigkeit hinsichtlich der Durchführung von Bußgeldverfahren (siehe aber Tz. 3.2). Die neuen Regelungen zu gemeinsamen Verfahren haben bisher die Landesverwaltung im Blick. Tatsächlich besteht ein großer Bedarf auch auf kommunaler Ebene.

Was ist zu tun?

Mit den neuen Regelungen des LDSG hat Schleswig-Holstein ein fortschrittliches Datenschutzrecht. Die Erfahrungen zeigen, dass weitere Änderungen wünschenswert sind.

1.2 Informationszugangsgesetz Schleswig-Holstein – IZG-SH

Parallel zur Änderung des LDSG wurde in Schleswig-Holstein auch das Informationsfreiheitsrecht überarbeitet. In dem neuen Informationszugangsgesetz des Landes Schleswig-Holstein (IZG-SH) wurden die bisher getrennt geregelten Materien des Informationsfreiheitsgesetzes (IFG) und des Umweltinformationsgesetzes (UIG) zusammengeführt. Ein solches einheitliches Gesetz für den Zugang zu behördlichen Informationen und Umweltinformationen ist bisher bundesweit einzigartig. Zielsetzung der Zusammenführung ist eine Vereinfachung und Vereinheitlichung der Verfahren und eine Vermeidung von Abgrenzungsproblemen bei Informationsgesuchen von Bürgerinnen und Bürgern gegenüber der Verwaltung. Das ULD ist nunmehr auch explizit zuständig für den

Zugang zu Umweltinformationen. Die Regelungen im neuen IZG-SH entsprechen im Wesentlichen den Regelungen im bisherigen UIG.

Der Landtag konnte sich beim Erlass des IZG-SH nicht dazu durchringen, generell proaktive Veröffentlichungspflichten vorzusehen, sodass diese weiterhin nur für Umweltinformationen gelten. Für sonstige Informationen in der öffentlichen Verwaltung hängt die Transparenz des Verwaltungshandelns von der sehr unterschiedlichen Praxis der jeweiligen Behörden ab.

1.3 Erwägungen zu einem Transparenzgesetz

Mit seinem neuen Transparenzgesetz bekennt sich die hamburgische Verwaltung zu proaktiver Informationspolitik im Sinne von Open Data. Dieses liefert Anregungen für Schleswig-Holstein.

Von allen in der Hamburgischen Bürgerschaft vertretenen Fraktionen wurde gemeinsam ein Entwurf eines Transparenzgesetzes für die Hansestadt eingebracht und verabschiedet. Das im Oktober 2012 in Kraft getretene Gesetz setzt neue Maßstäbe im Bereich der Informationsfreiheit. Zweck des Gesetzes ist es nicht nur, Informationen der Verwaltung auf Antrag bereitzustellen, sondern diese – im Sinne von Open Data – unmittelbar der Allgemeinheit von sich aus zugänglich zu machen und zu verbreiten, um die demokratische Meinungs- und Willensbildung zu fördern und die Kontrolle staatlichen Handelns zu verbessern.

Das ULD wurde von mehreren Seiten darauf angesprochen, inwieweit die Regelungen unseres südlichen Nachbarn in Schleswig-Holstein übernommen werden können. Das Ziel solle sein, all die Informationen bereitzustellen, die aus Gründen des Schutzes von öffentlichen oder privaten Interessen nicht vertraulich behandelt werden müssen. Ein öffentliches Interesse besteht insbesondere an der Bekanntgabe folgender Informationen: Aktivitäten und Entscheidungen der Regierung und der Ministerien, Richtlinien, Verwaltungsvorschriften, Verordnungen und Gesetze, Haushalts-, Organisations-, Geschäftsverteilungs- und Aktenpläne, Regelungen zur Daseinsvorsorge, Statistiken, Tätigkeitsberichte, Gutachten, Studien, Geodaten, Pläne, Karten und öffentliche Register, Angaben über öffentliche Unternehmen und öffentliche Verträge. Auch anonymisierte behördliche Einzelentscheidungen können für Bürgerinnen und Bürger von großem Interesse sein.

Ein Transparenzgesetz verspricht mehrere positive Effekte: Mehr Transparenz der Verwaltung kann das Vertrauen in die Verwaltung und damit die Akzeptanz in Entscheidungen und Aktivitäten erhöhen. Die Bürgerpartizipation wird erleichtert. Die Verwaltung wird von Einzelanfragen entlastet. Zugleich bewirkt die strukturierte Bereitstellung von Verwaltungsinformationen in einem über das Internet erschlossenen Informationsregister, dass die verwaltungsinternen Abläufe vereinfacht und Doppelarbeit vermieden wird.

Gegenüber den hamburgischen Regelungen müssen bei einem Transparenzgesetz in Schleswig-Holstein einige Besonderheiten beachtet werden: Die im IZG-SH erfolgte Zusammenführung von Umweltdaten und Daten der allgemeinen Verwaltung sollte nicht aufgegeben werden. Die Verwaltung in unserem Flächenland ist weitgehend kommunal organisiert. Es ist naheliegend, ein landesweites Informationsregister für die Kreise, Städte und Gemeinden zu öffnen. Aus Respekt vor der kommunalen Selbstverwaltung sollte der Landesgesetzgeber insofern den Kommunen aber keine Veröffentlichungspflichten auferlegen, sondern eher ein technisches Angebot unterbreiten, das diese gemäß dem politischen Willen und den Möglichkeiten vor Ort in Anspruch nehmen können.

Ein Informationsregister gibt es aber nicht zum Nulltarif. Es bedarf einer strukturierten technischen Plattform, auf der die Behörden ihre Informationen mit entsprechenden Schnittstellen bereitstellen können. Der Datenabruf über das Internet ist benutzungsfreundlich auszugestalten. Es bietet sich an, die bisherigen Internetangebote der öffentlichen Verwaltung auf einer Plattform zu bündeln, was eine landesweite Koordination bedingt.

Für Open Data kann in Schleswig-Holstein förderlich sein, dass hierzu derzeit in Bremen und Hamburg erste Erfahrungen gesammelt werden. Dem gemeinsamen Dienstleister Dataport kann dabei eine wichtige Funktion zukommen. Denkbar ist sogar, in Kooperation mit den Hansestädten diesbezüglich ein länderübergreifendes Angebot zu gestalten. Erste Gespräche hierüber unter Einbindung des Innenministeriums Schleswig-Holstein haben schon stattgefunden (Tz. 12.1).

1.4 Erwartungen des ULD an Landtag und Regierung

Anlässlich des Beginns der 18. Legislaturperiode des im Mai 2012 neu gewählten Landtags von Schleswig-Holstein hat das ULD seine Vorstellungen und Erwartungen an die Landespolitik formuliert.

Das Anfang 2012 in Kraft getretene neue LDSG sieht vor, dass das ULD nur noch alle zwei Jahre einen Tätigkeitsbericht erstellt. Das ULD nahm den Beginn der neuen Legislaturperiode zum Anlass, dem neu gewählten Landtag – als eine Art Ersatz – aktuelle Handlungsempfehlungen zu geben. Darin beschreibt das ULD in komprimierter Form die Geschichte und die Organisation von Datenschutz und Informationsfreiheit im Land und schildert den Stand auf Landes-, Bundes- und europäischer Ebene.

Auf dieser Grundlage macht das ULD eine Vielzahl von konkreten Vorschlägen zur Verbesserung von Datenschutz und Informationsfreiheit im Land in den Bereichen Allgemeine Verwaltung, Sicherheitsbehörden, Soziales und Gesundheit, Bildung und Wissenschaft, Finanzverwaltung sowie hinsichtlich des Einsatzes und der Nutzung sozialer Medien und lädt zum Dialog hierüber ein. Das ULD bringt zum Ausdruck, dass ein verstärktes Engagement des Landes in diesem Bereich auf Bundesebene, etwa über den Bundesrat, äußerst wünschenswert ist, zumal – anders als auf Landesebene – die nationalen politischen Bestrebungen und Projekte fast durchgängig unzureichend waren und weiterhin sind (Tz. 2).

Das ULD sieht einen Schwerpunkt der künftigen Politik in der Weiterentwicklung des E-Government, wobei hier die Vorgehensweise zwischen Bund, dem Land und den Kommunen koordiniert und abgestimmt werden sollte. Dem Land kommt insofern die zentrale Funktion zu, die Entwicklungen auf Bundesebene in die richtige Richtung zu lenken und zugleich die Kommunen einzubinden.

https://www.datenschutzzentrum.de/ldsh/20120611-Vorstellungen-und-Erwartungen-an-die-Politik.html

1.5 Öffentliche Stellen und das Betreiben einer Facebook-Fanpage

Die Veröffentlichung einer datenschutzrechtlichen Bewertung der Reichweitenanalyse von Facebook und die damit verbundene Aufforderung an Webseitenbetreiber in Schleswig-Holstein im August 2011, ihre Facebook-Fanpages und Social Plugins zu deaktivieren, war der Startschuss einer intensiven öffentlichen Auseinandersetzung über den Datenschutz bei Facebook (Tz. 2.2, 7.1).

Das ULD forderte die öffentlichen Stellen des Landes Schleswig-Holstein auf, ihre Fanpages bei Facebook und Social Plugins wie den „Gefällt mir"-Button von ihren Webseiten zu entfernen. Nach eingehender technischer und rechtlicher Analyse kommt das ULD zu dem Ergebnis, dass derartige Angebote gegen das Telemediengesetz und gegen das Bundesdatenschutzgesetz bzw. das Landesdatenschutzgesetz Schleswig-Holstein verstoßen. Bei der Nutzung der Facebook-Dienste erfolgt eine Datenweitergabe von Verkehrs- und Inhaltsdaten in die USA und eine qualifizierte Rückmeldung an den Betreiber hinsichtlich der Nutzung des Angebotes, die sogenannte Reichweitenanalyse (Tz. 7.1.1).

Einige öffentliche Stellen des Landes Schleswig-Holstein haben daraufhin ihre Fanpages bei Facebook herausgenommen und Social Plugins von ihren Webseiten entfernt. Andere öffentliche Stellen haben ihr Angebot noch erweitert. Das ULD hat exemplarisch vier öffentliche Stellen ausgewählt und angeschrieben. U. a. weigerten sich die Staatskanzlei und die Industrie- und Handelskammer (IHK), ihre Fanpages aufzugeben. Deshalb musste das ULD Beanstandungen gegenüber den Fanpage betreibenden datenverarbeitenden Stellen aussprechen, was auch den zuständigen Aufsichtsbehörden mitgeteilt wurde. Keine der Aufsichtsbehörden, die teilweise selbst solche Seiten betreiben, wurden rechtsaufsichtlich tätig. Die daraufhin stattfindende Anrufung des Innen- und Rechtsausschusses des Landtags war ebenfalls erfolglos. Eine weiter gehende Handhabe gegenüber öffentlichen Stellen hat das Unabhängige Landeszentrum für Datenschutz bisher nicht.

02

KERNPUNKTE

Bundesdatenschutzgesetz

Social Media

Europäische Datenschutz-Grundverordnung

2 Datenschutz – national und global

Während auf Landesebene die Diskussion um Datenschutz und Informationsfreiheit – manchmal schwerfällig – vorankommt, erleben wir auf nationaler Ebene fast nur – manchmal geschwätzige – Untätigkeit, ja Lähmung. So positiv die schwarz-gelbe Koalition mit Absichtserklärungen startete (32. TB, Tz. 2.2), so folgenlos sind diese geblieben. Nicht einmal Ansätze zur überfälligen grundsätzlichen Überarbeitung des Bundesdatenschutzgesetzes sind erkennbar; auch in den Spezialbereichen Internetdatenschutz (Tz. 2.1) und Beschäftigtendatenschutz (Tz. 2.4) war es schwer, ernsthafte Bestrebungen zu sachorientierten Lösungen zu erkennen. Das ursprünglich unterstützungswürdige Projekt einer Stiftung Datenschutz wurde sehenden Auges an die Wand gefahren.

Die tendenziell eher zu begrüßenden Aktivitäten der Europäischen Union (EU) (Tz. 2.5) können für diesen Sachverhalt keine Rechtfertigung sein. Bis ein neuer normativer Rahmen für den Datenschutz in Europa in Kraft getreten ist, können die bestehenden Defizite nur schwerlich hingenommen werden. Zugleich bestünde mit einer vorbildlichen deutschen Gesetzesinitiative die Chance, die europäische Diskussion konstruktiv voranzubringen. Ein Warten bliebe in den Bereichen ohne Gewinn, wo bisher in Europa keine Gesetzgebungsaktivitäten geplant sind, also in den Bereichen Telekommunikation, Beschäftigtendatenverarbeitung sowie beim Projekt einer Stiftung Datenschutz.

2.1 Internetgesetzgebung

Auf Bitte des Schleswig-Holsteinischen Landtags hat das ULD auf einen Antrag zu einer Bundesratsinitiative Stellung genommen, deren Ziel die „Stärkung der Freiheit und der Privatsphäre im Internet“ ist.

Unsere Informationsgesellschaft ist vom stationär wie mobil nutzbaren interaktiven Internet geprägt. Dieses Netz weist vier technikspezifische Eigenschaften auf, die gravierende Konsequenzen für die Datenschutzregulierung haben:

- Die Virtualität des Netzes schafft neben der analogen eine digitale Realität, die mit der analogen in einem engen gestaltbaren Wechselspiel steht. Wegen der Auswirkungen dieser digitalen Realität auf das Persönlichkeitsrecht des Menschen kann und muss ordnend bzw. regulierend eingegriffen werden.
- Das Netz ist universell und konvergent. Dadurch werden im analogen Raum bestehende Grenzziehungen zwischen Lebens- und Medienwelten, also etwa zwischen privat und öffentlich, Konsument und Produzent, Information und Einwirkung, eingeebnet.
- Die Globalität des Netzes erschwert eine Lokalisierung informationstechnischer Sachverhalte, die Zuordnung von Verantwortung hierfür und staatliche Interventionen.
- Das Netz ist gekennzeichnet durch den paradox erscheinenden Widerspruch von Intransparenz der Datenverarbeitung bzw. Anonymität und absoluter Kontrollierbarkeit der Nutzenden.

Die hieraus zu ziehenden Konsequenzen für die Datenschutzgesetzgebung werden seit den 90er-Jahren diskutiert. Seit der Jahrtausendwende gibt es hierzu konkrete Vorschläge:

2001 wurde von Prof. Alexander Roßnagel, Prof. Andreas Pfitzmann und Prof. Hansjürgen Garstka das vom Bundesinnenministerium in Auftrag gegebene Gutachten „Modernisierung des Datenschutzrechts“ vorgelegt.

http://www.sachsen-anhalt.de/fileadmin/Elementbibliothek/Bibliothek_Politik_und_Verwaltung/Bibliothek_LFD/PDF/binary/Service/Sonstige_Infos/gutachten_zur_modernisierung_des_datenschutzes.pdf

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder veröffentlichte im März 2010 den ausführlichen Katalog „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ (33. TB, Tz. 2.1). Das ULD präsentierte im Oktober 2010 konkrete Formulierungen zur Änderung des Internetdatenschutzes im BDSG.

https://www.datenschutzzentrum.de/internet/gesetzentwurf.html

Ein Regulierungsvorschlag des Bundesinnenministeriums vom Dezember 2010, bekannt geworden unter dem Begriff „rote Linien“, war nicht problemadäquat. Demgegenüber unterbreitete das Bundesland Hessen im März 2011 einen Gesetzentwurf, bei dem einige Regelungsdefizite beim Internetdatenschutz durch eine Änderung des Telemediengesetzes beseitigt werden sollten. Damit wäre auch die überfällige Umsetzung der von der EU vorgegebenen Cookie-Regelung angegangen worden (Tz. 7.3). Trotz positiver Behandlung im Bundesrat wurde diese Initiative vom Bundestag nicht weiterverfolgt.

Die aktuellste, äußerst wertvolle Initiative kam vom 69. Deutschen Juristentag im September 2012, wo unter dem Titel „Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung“ durch ein ausführliches Hauptgutachten von Prof. Gerald Spindler sowie eine Vielzahl von hoch qualifizierten Diskussionsbeiträgen versucht wurde, dem Gesetzgeber die Hand zu führen – wieder ohne erkennbare politische Resonanz.

Dies hinderte das ULD nicht, anlässlich eines Antrags im Landtag Schleswig-Holstein erneut ausführlich und unter Hinzuziehung der aktuellen Entwicklungen in der Diskussion, in der Praxis sowie in der Rechtsprechung auf die nötigen und möglichen Regelungen hinzuweisen (Landtag Schleswig-Holstein Umdruck 18/553). Dabei geht es um Neujustierungen und Vorschläge in folgenden datenschutzrechtlich zentralen Bereichen:

- Verantwortlichkeit,
- Anwendbarkeit des Rechts und Aufsichtszuständigkeit,
- Verhältnis des Datenschutzes zu den Grundrechten auf Informations-, Presse- und Meinungsfreiheit,
- Zweckbindung in Hinblick auf Person, Lebensbereich und Rolle,
- Betroffenenrechte (Datenlöschung, Auskunft, Portabilität) und Transparenz,
- Einwilligung aus rechtlicher sowie technischer Sicht,
- Beschwerdemanagement und Sanktionen.

https://www.datenschutzzentrum.de/internet/20121219-stellungnahme-freiheit-internet.html

Wegen der anstehenden Bundestagswahl ist nicht damit zu rechnen, dass kurzfristig den bestehenden Regelungsmängeln auf Bundesebene abgeholfen werden wird.

Was ist zu tun?

Die laufenden Diskussionen – auch in den Ländern und im Landtag von Schleswig-Holstein – sollten dazu beitragen, dass tatsächlich umgehend nach der Bundestagswahl begonnen wird, beim Internetdatenschutz die Regelungsdefizite abzubauen.

2.2 Datenschutz bei Social Media

Die Begeisterung für das Web 2.0 scheint ungebrochen. Die Hoffnungen sind groß: an Jugendliche heranzukommen, die eigene Technikaffinität und Modernität der ganzen Welt unter Beweis stellen zu können, neue kommunikative Werbe- und Vertriebswege zu eröffnen – und all das zu geringen Kosten, mit geringem Aufwand und zumeist mit wenig Datenschutz.

Öffentliche und private Stellen nutzen oft wegen der technischen Möglichkeiten mit ungetrübter Faszination Facebook, Twitter, Google & Co. Doch nun kommen die Datenschutzbeauftragten, hinterfragen die Technik und teilen mit, dass die Nutzung vieler Social-Media-Angebote mit der Gesetzmäßigkeit der Verwaltung bzw. mit den gesetzlichen Pflichten von Unternehmen nicht in Einklang zu bringen ist. Bei der Nutzung der Social-Media-Angebote ergeben sich einige zentrale, zumeist nicht befriedigend beantwortete Datenschutzfragestellungen:

- Übernimmt die Stelle in Deutschland die ihr zukommende datenschutzrechtliche Verantwortung?
- Sind die Einwilligungen und allgemeinen Geschäftsbedingungen, etwa in Form von Terms of Use und Privacy Policies, mit den rechtlichen Vorgaben vereinbar, mit den Anforderungen an Kleingedrucktes, an Datensparsamkeit und an verbindliche Willenserklärungen der Nutzenden?
- Ist die Inanspruchnahme der Betroffenenrechte, etwa auf Auskunft und Datenlöschung, technisch und organisatorisch umgesetzt?
- Wo und wie erfolgt die Datenverarbeitung – das Setzen und Nutzen von Cookies, die Auswertung für Werbezwecke, die Nutzungsanalyse, der Zugriff Dritter einschließlich ausländischer Sicherheitsbehörden – und ist diese rechtskonform?
- Können die Bürgerinnen und Bürger die Dienste anonym oder unter Pseudonym nutzen?

Ansatzpunkt der Fragen waren zunächst die Fanpages und Social Plugins von Facebook, die sich bei öffentlichen und privaten Stellen großen Zuspruchs erfreuen (Tz. 1.5, 7.1.1). Das ULD kam diesbezüglich jeweils zu klaren Antworten: Nein. Die weitere öffentliche Diskussion bestätigte dieses Ergebnis und zeigte, dass die Antworten bei Google+ und anderen Social-Media-Anbietern oft nicht besser ausfallen.

Dies führte dazu, dass einige Stellen auf die Nutzung kritikwürdiger Angebote verzichteten. Andere Stellen versuchten, die kritisierten Aspekte aufzugreifen und zu korrigieren. So wurden für die Nutzenden auf den Seiten Warnhinweise oder Doppelklick-Lösungen bei Social Plugins wie den „Gefällt mir"- und „+1"-Buttons eingeführt nach dem Motto: „Sie nutzen diese Seite auf eigene Gefahr." Dies kann nicht wirklich befriedigen: Warnhinweise machen rechtswidriges Handeln nicht rechtmäßig. Verlinkte Inhalte werden z. B. von Facebook vollständig erfasst, gespeichert und ebenso wie originäre Inhalte der Fanpages in die automatisierte personenbezogene Reichweitenanalyse einbezogen. Selbst die Einbindung von Inhalten von Websites in ein sogenanntes Page Tab, auch IFrame-Einbindung genannt, unterliegt einer – auf die Anzeige des Page Tabs beschränkten – Reichweitenanalyse.

Social Media können von privaten und öffentlichen Stellen genutzt werden, selbst in sensiblen Bereichen. Voraussetzung dafür ist aber, dass die Stellen rechtlich wie faktisch, also technisch-organisatorisch, die Verantwortung übernehmen und dass vor der Inbetriebnahme erfolgreich eine qualifizierte Prüfung erfolgt. Das gibt es nicht zum Nulltarif, sondern verlangt IT-Qualität und Kompetenz bei Entwicklern, Entscheidern, Anwendern und Nutzern.

Statt die billigsten Angebote ungeprüft zu übernehmen, die sämtliche Inhalts- und Kommunikationsdaten sowohl der Werbenutzung als auch ausländischer Sicherheitsbehörden auf dem Tablett servieren, müssen datenschutzkonforme technische Lösungen entwickelt, implementiert und betrieben werden. Zum Betrieb gehören knappe und klare Regeln für Anwender und Nutzer, in denen die Verantwortlichkeiten sowie die Rechte und Pflichten benannt werden, und Privacy-by-Default-Einstellungen.

Es gibt keinen Grund, Social Media insgesamt abzulehnen; diese können eine massive Bereicherung für Information und Kommunikation sein. Wichtig ist ein bewusster, verantwortungsvoller Umgang hiermit. So kann die Verbreitung von Nachrichten über Twitter eine sinnvolle Ergänzung – aber eben nur eine Ergänzung – zur eigenen Webpräsenz und Öffentlichkeitsarbeit sein. Statt der Einbindung von Google oder Bing als Daten fressende Suchmaschinen gibt es brauchbare, als datenschutzkonform zertifizierte, kostenfreie Alternativen wie Ixquick und Startpage (Tz. 9.3.5).

Hier besteht ein Markt für IT-Dienstleister. Technische Lösungen, die nicht auf ausländischen Servern laufen, sondern selbst verantwortet und administriert werden können, sind – teilweise als Open Source – auf dem Markt verfügbar. Bisher konnten sich datenschutzfreundlichere Alternativlösungen wie Diaspora, Friendica oder Identica nicht durchsetzen, weil alle meinen, zu den Billigangeboten, bei denen schon die Massen der Nutzenden sind, gäbe es keine Alternative.

Facebook & Co. verkommen immer mehr zu reinen Werbeplattformen, die zu promoten es keinen Anlass gibt. Soziale Netzwerke, die diesen Namen zu Recht tragen und die zugleich auch noch das Gütesiegel der Akzeptanz der Datenschutzbehörden vorweisen können, haben ein – bisher ungenutztes – Potenzial, gerade in Deutschland, wo informationelle Selbstbestimmung und Rechtsstaatlichkeit kulturell anerkannte Werte sind.

Gefordert sind auch die politischen Akteure und Gremien auf Landes- und auf Bundesebene: Statt sich als wirksame Werbeplattform von Anbietern aus Übersee, deren soziales Engagement sich

durch Steuervermeidung und Datenschutzignoranz auszeichnet, gebrauchen zu lassen, könnten und sollten das Know-how und die Infrastruktur in Deutschland genutzt werden. Hieran fehlt es nicht; woran es fehlt, ist ein wenig Geld und vor allem der politische Wille.

Was ist zu tun?

Die eigene Erforschung, Entwicklung und Implementierung dezentraler, selbst verantwortbarer und datensparsamer Social Media sollte gefördert und vorangetrieben werden.

2.3 Stiftung Datenschutz

Bei der Einrichtung der Stiftung Datenschutz wurden die Datenschutzbeauftragten des Bundes und der Länder nicht beteiligt. Das Ergebnis ist der Verzicht der Datenschutzbeauftragten auf die Entsendung von Vertretern in den Stiftungsbeirat.

Eines der großen Datenschutzprojekte der aktuellen Bundesregierung sollte die Stiftung Datenschutz werden, die Audit- und Gütesiegelverfahren durchführen, vergleichende Datenschutztests vornehmen, Bildungsangebote bereitstellen und Forschungsprojekte koordinieren sollte. Anders als andere Landesdatenschutzbeauftragte reagierte das ULD von Anfang an positiv auf die Idee; wir boten unsere Unterstützung und insbesondere das Einbringen unserer langjährigen Erfahrungen in den Bereichen an, die genau das Tätigkeitsfeld der künftigen Stiftung sein sollten (33. TB, Tz. 2.3). Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erklärte sich zur konstruktiven Zusammenarbeit mit dem federführenden Bundesinnenministerium bereit. Dieses zeigte jedoch an einer Zusammenarbeit keinerlei Interesse.

Was sich schon abzeichnete, wurde dann wahr: Alle Energie wurde darauf gelenkt, einen bürokratischen Apparat zu schaffen, nicht handlungsfähige Arbeitsstrukturen: „Um das Stiftungsvermögen dauerhaft zu erhalten, sollten die Personal- und Sachkosten gering gehalten werden“, so die Bundesregierung. Groß wird dagegen ein Beirat mit über 30 Mitgliedern sein, wovon gemäß der Satzung etwa die Hälfte von der Wirtschaft gestellt werden soll, weitere Mitglieder von Bundestagsfraktionen und der Verwaltung. Die Datenschutzbehörden sollten insgesamt drei Mitglieder benennen können. Ein Verwaltungsrat soll von der Bundesregierung beschickt und vom Bundesinnenministerium dominiert werden. Ein Konzept wurde nicht vorgelegt, geschweige denn ein konkreter Plan, wie die Zertifizierung – also die ursprüngliche Hauptaufgabe – durchgeführt werden soll. Damit sind praktisch alle Erwartungen an die Stiftung unerfüllt geblieben: Kompetenz, Unabhängigkeit, Transparenz. Für eine enge Zusammenarbeit zwischen Stiftung und Datenschutzbeauftragten, bei der die Arbeit nicht auf Letztere abgewälzt wird, gibt es keine Anzeichen.

Angesichts dieses Resultats beschloss die Konferenz der Datenschutzbeauftragten des Bundes und der Länder im November 2012, von der Möglichkeit, Vertreter in den Stiftungsbeirat zu entsenden, keinen Gebrauch zu machen. Diesem Vorbild folgten einige benennungsberechtigte Stellen aus der politischen Opposition und aus den Bereichen Gewerkschaften und Verbraucherschutz. Die Konferenz wie auch das ULD sind weiterhin zu einer Unterstützung und Beratung bereit. Voraussetzung hierfür ist aber, dass damit ein Vorteil für den Datenschutz erkennbar wird. Einrichtungen, die entgegen den rechtlichen Anforderungen insbesondere Wirtschaftsunternehmen datenschutzrechtliche Persilscheine ausstellen, gibt es im kommerziellen Bereich schon mehr als genug.

Was ist zu tun?

Die weitere Entwicklung ist aufmerksam und kritisch zu verfolgen. Sinnvoll wäre ein kompletter Neuanfang.

2.4 Beschäftigtendatenschutz

Keinen Erfolg hatte bisher der Versuch der Bundesregierung, ein bundesweit einheitliches, praktikables und auf Ausgleich zwischen Arbeitnehmer- und Arbeitgeberseite abzielendes Beschäftigtendatenschutzrecht zu schaffen.

Es könnte so einfach sein: Es liegt eine Vielzahl von sinnvollen Formulierungsvorschlägen von Oppositionsparteien und von Interessenverbänden vor; es kann auf eine gefestigte Arbeitsgerichtsrechtsprechung zurückgegriffen werden. Doch das seit knapp 30 Jahren bestehende Versprechen, ein valides Beschäftigtendatenschutzrecht zu schaffen, das Rechtsfrieden und einen fairen Interessenausgleich schafft, droht weiterhin unerfüllt zu bleiben. Vorausgegangen waren in den Jahren 2008/2009 Überwachungsskandale im Arbeitsbereich. Im August 2010 war ein Entwurf einer Änderung des BDSG vorgelegt worden, der das Versprechen des Koalitionsvertrages, den Beschäftigtendatenschutz zu verbessern, nicht halten konnte (33. TB, Tz. 5.1). Vertreter der Arbeitgeber- wie der Arbeitnehmerseite, juristische und betriebliche Praktiker und die Datenschutzbeauftragten machten eine Vielzahl von konstruktiven Vorschlägen, wie aus dem schlechten Entwurf noch ein gutes Gesetz gemacht werden kann.

Bei den Gesetzesberatungen wurden die Datenschutzbeauftragten praktisch nicht eingebunden. Gerüchte waren zumeist die einzige Informationsquelle. Auch nur gerüchtehalber war zu erfahren, dass sich die Arbeitgeberseite massiv in den Entscheidungsprozess der Gesetzgebung einmischte. Die Gerüchte über die inhaltlichen Änderungsvorschläge deuteten darauf hin, dass der Datenschutz für Beschäftigte noch weiter abgebaut werden könnte. Ein Warten auf Europa ist nicht angebracht; der Regelungsvorschlag der EU-Kommission zum Datenschutz (Tz. 2.5) überlässt diesen Bereich ausdrücklich den Mitgliedstaaten. Im Januar 2013 wurde bekannt, dass die Regierungskoalition mit einem nur in wenigen Punkten geänderten Entwurf im Schnelldurchgang die Gesetzgebung abschließen möchte. Nach heftigem öffentlichen Protest, u. a. in Form einer Entschließung der Datenschutzbeauftragten des Bundes und der Länder, wurde die Beschlussfassung aufgeschoben und weitere Diskussionen angekündigt. Dass diese erfolgreich sein werden, ist nicht zu erwarten.

http://www.datenschutz-bremen.de/konferenzbeschluesse2.php?konfid=166

Was ist zu tun?

Der Gesetzgeber sollte sich beim Beschäftigtendatenschutz beeilen, was aber nicht zulasten der Qualität des Grundrechtsschutzes gehen darf.

2.5 EU-Rechtsrahmen – Entwurf einer Datenschutz-Grundverordnung

Die EU-Kommission hat am 25. Januar 2012 den Entwurf für eine Datenschutz-Grundverordnung veröffentlicht, die die Maßstäbe für den Schutz personenbezogener Daten in der EU vereinheitlichen soll. In 91 Artikeln finden sich wertvolle Bestimmungen zum Schutz und zur Stärkung der

allgemeinen Persönlichkeitsrechte der Bürgerinnen und Bürger. Allerdings besteht auch Änderungs- und Ergänzungsbedarf, der in die laufenden Abstimmungen und in das Gesetzgebungsverfahren einfließen sollte. Das ULD unterstützt die EU-Kommission in ihrem Vorhaben, einen harmonisierten und technikneutralen Datenschutz in Europa zu schaffen. Eine Modernisierung des Datenschutzes und dessen Vereinheitlichung auf europäischer Ebene sind dringend notwendig, um den immer neuen Risiken für die Persönlichkeitsrechte der Bürgerinnen und Bürger wirksam zu begegnen und um einen Datentransfer im Binnenmarkt zu ermöglichen sowie dessen Zulässigkeit zugleich an klare Bedingungen zu knüpfen.

Positiv hervorzuheben sind Bestimmungen zur Stärkung des Einwilligungserfordernisses, zum Schutz personenbezogener Daten von Kindern, zu den Betroffenenrechten gegenüber den verantwortlichen Stellen – auf Information, Auskunft, Vergessenwerden bzw. Löschung und Datenübertragbarkeit –, die Reglementierung von auf Profiling basierenden Maßnahmen, das Gebot datenschutzfreundlicher Voreinstellungen, die haftungsrechtliche Gleichstellung von für die Datenverarbeitung Verantwortlichen und den Auftragsdatenverarbeitern, die Einführung umfassender Dokumentationspflichten, die Verpflichtung zur Datenschutzfolgenabschätzung, die Befürwortung datenschutzspezifischer Zertifizierungsverfahren und die Erweiterung der Sanktionsmöglichkeiten für die Aufsichtsbehörden im Falle von Verstößen gegen die Grundverordnung.

Änderungs- und Korrekturbedarf sieht das ULD insbesondere bei folgenden Punkten:

- Die vorgesehenen Ermächtigungen für die Kommission für sogenannte delegierende Rechtsakte müssen auf das erforderliche Maß reduziert werden. Den Mitgliedstaaten muss die Möglichkeit verbleiben, für den Grundrechtsschutz wesentliche Gesichtspunkte selbst zu regeln.
- Technisch-organisatorische Maßnahmen zur Gewährleistung der Datensicherheit und damit auch des Datenschutzes, wie die Grundsätze der Integrität, der Verfügbarkeit, der Vertraulichkeit, der Transparenz, der Intervenierbarkeit und der Nichtverkettbarkeit, sollten in der Grundverordnung verankert werden.
- Beabsichtigt ist, dass im Wege eines „One-Stop-Shops" nur noch eine Aufsichtsbehörde europaweit im Hinblick auf ein bestimmtes Unternehmen als zuständige Kontrollbehörde tätig werden kann. Hier sollte berücksichtigt werden, dass für bestimmte Sachverhalte hauptsächlich nationale Datenschutzvorschriften eingreifen können, sodass die Bestimmung eine Art europäische Federführung vorsehen sollte.
- Für die EU-Kommission enthält der Entwurf zahlreiche Befugnisse, wie etwa die Erarbeitung und Aufstellung von Ausführungsbestimmungen, was die Unabhängigkeit der europäischen Datenschutzaufsichtsbehörden beeinträchtigen würde. Hier muss Abhilfe geschaffen werden.
- Die vorgesehene Verpflichtung, betriebliche Datenschutzbeauftragte erst ab einer Anzahl von 250 Beschäftigten bestellen zu müssen, ist deutlich zu niedrig. Die Bestellpflicht sollte vorrangig von qualitativen Aspekten der automatisierten Datenverarbeitung und weniger von quantitativen Merkmalen abhängig gemacht werden.

Mit Datum vom 17. Dezember 2012 legte der Berichterstatter des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments Änderungsvorschläge zur Grundverordnung vor, welche die Anregungen der Datenschutzbeauftragten weitgehend aufgreifen.

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+COMPARL+PE-501.927+04+NOT+XML+V0//DE

Was ist zu tun?

Die Chance, ein EU-weit einheitliches Datenschutzniveau zu schaffen, darf nicht leichtfertig verspielt werden. Ein solcher Rechtsrahmen führt zu mehr Rechtsklarheit und stärkt das Persönlichkeitsrecht der Bürgerinnen und Bürger, zu dessen Gewährleistung die europäische Verfassung verpflichtet. Alle Verantwortungsträger, vor allem auf parlamentarischer Ebene, sind aufgerufen, dazu beizutragen, diese Ziele zu erreichen.

03

KERNPUNKTE

ULD-Dienststellenkonzept

Effektivierung der Aufsichtstätigkeit

3 Die Dienststelle

Die Spannung zwischen dem, was aus Sicht von Datenschutz und Informationsfreiheit wünschenswert ist, und dem angesichts der angespannten Haushaltssituation Möglichen nimmt weiter zu.

Das ULD versucht diesen Herausforderungen durch ein hohes Arbeitspensum zu genügen. Dessen ungeachtet wird es zunehmend schwieriger, auf die Anfragen und Beschwerden von Bürgerinnen und Bürgern zeitnah zu antworten und zugleich die nötigen strategischen Maßnahmen durchzuführen. Die Kommunikationsmöglichkeiten des Internets führen in immer schnellerer Folge zu Problemen und Konfliktlagen für die Betroffenen, auf die vom ULD umgehend Reaktionen erwartet werden. Dass diese Erwartungen nicht immer erfüllt werden, liegt nicht an der fehlenden Bereitschaft hierzu, sondern an den hierfür verfügbaren begrenzten Ressourcen.

Das ULD bekennt sich zu dem Ziel der Konsolidierung des Landeshaushaltes. Die Ausgaben des Landes für die Dienststelle konnten trotz eines Zuwachses an Aufgaben und Anforderungen seit Jahren fast konstant gehalten werden. Dies war nur dadurch möglich, dass insbesondere über Projektfinanzierungen durch die Europäische Union und durch Entgelte Einnahmen erzielt wurden, mit denen die Finanzierung von zusätzlichen Beschäftigten mit befristeten Arbeitsverträgen erfolgte. Das ULD hat sich an den Landtag mit der Bitte gewandt, hierzu unbefristete Stellen im Haushalt auszuweisen (Schleswig-Holsteinischer Landtag, Umdruck 18/489). Hierdurch könnte für die betroffenen Mitarbeiterinnen und Mitarbeiter mehr Arbeitsplatzsicherheit geschaffen werden; für das ULD ließe sich so mehr Kontinuität erreichen.

3.1 Das Konzept des ULD

Anfang 2011 legte das ULD ein Konzept vor, in dem nach einer Analyse der rechtlichen, technischen und finanziellen Ausgangssituation strategische Ziele und Maßnahmen abgeleitet wurden (33. TB, Tz. 1.2). Nach zwei Jahren muss zunächst festgestellt werden, dass eine Funktion des Konzeptes nicht erfüllt wurde: Die Hoffnungen auf Diskussionen, sowohl innerhalb der Datenschützerinnen und Datenschützer als auch mit den tangierten Bereichen, also insbesondere Politik, Verwaltung, Wirtschaft und Wissenschaft, haben sich als unberechtigt erwiesen. Selbst der Landesrechnungshof, der fünf Jahre zuvor die Tätigkeit des ULD konzeptionell massiv kritisiert hatte, sah keine Veranlassung, auf das von uns veröffentlichte Konzept zu reagieren.

https://www.datenschutzzentrum.de/ldsh/konzept/

Für die konkrete praktische Tätigkeit des ULD erwies und erweist sich das Konzept als förderlich. Schon während des ULD-internen Prozesses der Erarbeitung des Konzeptes konnte mehr Klarheit über Defizite und Möglichkeiten der eigenen Tätigkeit sowie über die damit verfolgten Ziele erlangt werden. Angesichts eines großen Vollzugsdefizits ging es und geht es weiterhin darum, Schwerpunktsetzungen vorzunehmen, sodass einerseits den zwingenden gesetzlichen Anforderungen genügt wird, andererseits aber ein Optimum an Zielerreichung im Sinne einer Verbesserung des Datenschutzes und der Informationsfreiheit generell erreicht wird.

Zwingend ist die Bearbeitung der Eingaben von betroffenen Bürgerinnen und Bürgern in jedem Einzelfall. Obligatorisch ist weiterhin die Beratung von öffentlichen Stellen und Politik im Land. Eine Beschränkung auf die Kontrolle und Sanktionierung sowie Beratung von Politik und öffentlichen Stellen des Landes würde zwangsläufig zum Ausblenden der sich abzeichnenden technischen Entwicklungen sowie der überregionalen Bezüge führen. Diese sind aber prägend für die konkreten Formen personenbezogener Datenverarbeitung und damit für die Sachverhalte, die das ULD kontrollieren und zu denen das ULD beraten muss. Insofern erweist sich der Ansatz des ULD als effektiv, Ressourcen in die in § 43 LDSG geregelten Serviceaufgaben zu stecken. Über die Fortbildungsaktivitäten, die Projektarbeit, das Erstellen von Studien und Gutachten, die Beratung von privaten Stellen, die Öffentlichkeitsarbeit und die Zertifizierung von Produkten, Dienstleistungen und Verfahren können Ressourcen erschlossen und Erkenntnisse gewonnen werden. Ohne diese zusätzlichen Ressourcen und Erfahrungen könnte das ULD seinen klassischen Aufsichtsaufgaben nicht sinnvoll nachkommen.

Das Image des ULD in der öffentlichen Wahrnehmung ist oft das einer eher strengen Behörde. Dies ist für das ULD keinesfalls nur Anlass zur Freude. Eigentlich sollte es eine Selbstverständlichkeit sein, dass eine Ordnungsbehörde, die das ULD auch ist, versucht, ansatzweise für Ordnung zu sorgen. Hinsichtlich des Datenschutzes wird dies von vielen Menschen in unserer Gesellschaft jedoch anders gesehen. Die Wahrnehmung als repressive Behörde verstellt zudem den Blick auf die proaktiven Aufgaben des ULD, zu denen wir uns mit tiefer Überzeugung bekennen. Im Interesse einer umfassenden Implementierung des Datenschutzes in unserer Informationsgesellschaft ist der forschende, erläuternde, helfende, bildende und fördernde Aspekt mindestens so wichtig wie der von Kontrolle und Sanktion. Wer von der Notwendigkeit des Datenschutzes überzeugt und wem bei dessen Umsetzung geholfen wird, den muss eine Behörde nicht bestrafen.

Die im ULD-Konzept dargestellten Analysen und Strategien haben sich weitgehend als richtig erwiesen. Auch wenn in dieser Hinsicht auf nationaler Ebene keine großen sichtbaren Fortschritte vorzuweisen sind (Tz. 2.4), konnte bisher nicht widerlegt werden, dass es nötig ist, Datenschutz als Marktfaktor zu stärken. Die Zuspitzung der Verhältnisse auf dem gewaltigen globalen Internetmarkt zeigte uns, dass ein Teil unserer Analyse nicht tief genug schürfte: Angesichts des Umstands, dass personenbezogene Daten im Internet die Währung sind, mit der – zumindest bei unentgeltlichen Diensten – bezahlt wird, haben wir dem Umstand, dass viele Geschäftsmodelle auf einer datenschutzwidrigen Verarbeitungsweise beruhen, noch zu wenig Gewicht beigemessen. Mit der Fokussierung von Aktivitäten auf diesen Bereich haben wir im Berichtszeitraum versucht, hierzu Gegenstrategien zu starten.

Was ist zu tun?

Das ULD-Konzept muss regelmäßig mit den aktuellen Entwicklungen abgeglichen werden. Mittelfristig wird das Konzept einer umfassenden Revision unterzogen und auf dieser Grundlage fortgeschrieben.

3.2 Neue Zuständigkeit für die Verfolgung von Ordnungswidrigkeiten

Durch Änderung der Ordnungswidrigkeiten-Zuständigkeitsverordnung des Landes wurde die Aufgabe der Verfolgung von datenschutzrechtlichen Ordnungswidrigkeiten nach dem Telemediengesetz (TMG) dem Vorstand des ULD übertragen. Nach den Bußgeldregeln im Telemediengesetz kann damit der Landesbeauftragte für Datenschutz als Vorstand des ULD gegenüber privatwirtschaftlichen Stellen Bußgeldbescheide bis zu einer Höhe von 50.000 Euro erlassen. Die Änderung der Zuständigkeitsverordnung dient der Klarstellung und wurde notwendig, nachdem die Befugnis zum Erlass von Bußgeldern öffentlich infrage gestellt worden war. Bisher gab es keine explizite Regelung in der Zuständigkeitsverordnung. Die Verfolgung von Ordnungswidrigkeiten steht im pflichtgemäßen Ermessen der Verwaltungsbehörde. Bußgelder werden in der Praxis nur in gravierenden Fällen erwogen und wenn die verantwortlichen Stellen vorsätzlich gegen Datenschutzregeln verstoßen. Werden von Stellen aufgrund unserer Intervention Maßnahmen ergriffen, die künftigen Verstößen wirksam entgegenwirken, so wird dies strafmindernd berücksichtigt.

3.3 Öffentlichkeitsarbeit

Für das ULD ist Öffentlichkeitsarbeit ein zentraler Schlüssel zur Verwirklichung von mehr Datenschutz in unserer Gesellschaft. Dem dienen Printveröffentlichungen, Vorträge und Veranstaltungen sowie Darstellungen im Internet.

Das ULD veröffentlichte nach den Änderungen im LDSG und IZG-SH eine umfangreiche neue Broschüre mit allen datenschutzrechtlich relevanten Rechtsnormen für öffentliche und nicht öffentliche Stellen in Schleswig-Holstein. Diese Broschüre

„Datenschutzrecht in Schleswig-Holstein“ ist beim ULD zu bestellen.

https://www.datenschutzzentrum.de/gesetze/20120817-ULD-Gesetzessammlung-Auflage5.pdf

Die Bundeszentrale für politische Bildung sprach uns wegen der geplanten Herausgabe eines Bandes „Datenschutz – Grundlagen, Entwicklungen und Kontroversen“ an. In enger Kooperation von über 40 Autorinnen und Autoren – sieben davon aus dem ULD, aus anderen Dienststellen sowie aus den Bereichen Wissenschaft, Verwaltung und Wirtschaft – konnte dieser Band im September 2012 fertiggestellt werden und wird seitdem von der Bundeszentrale vertrieben.

http://www.bpb.de/shop/buecher/schriftenreihe/143502/datenschutz

3.4 Social-Media-Dienstvereinbarung

Das ULD hat 2012 eine „Dienstvereinbarung soziale Medien“ erarbeitet und für sich selbst erlassen. Hiermit wird den Mitarbeiterinnen und Mitarbeitern eine Handreichung gegeben, wie sie dienstlich mit sozialen Medien wie sozialen Netzwerken, Blogs, Foren usw. umgehen sollen. Auch werden Probleme aufgezeigt, die im privaten Umfeld bei der Nutzung dieser Medien mit dienstlichem Bezug entstehen können, und Tipps gegeben, wie die Mitarbeiterin bzw. der Mitarbeiter hiermit umgehen sollte. Die Dienstvereinbarung ist speziell auf die Bedürfnisse des ULD angepasst. Es ist geplant, hieraus einen allgemeinen Vorschlag für die Gestaltung solcher Richtlinien zu erstellen.

https://www.datenschutzzentrum.de/ldsh/dv-social-media.html

04

KERNPUNKTE

E-Government

Moderne Sicherheitsstruktur

Umgang mit sensiblen Daten

4 Datenschutz in der Verwaltung

4.1 Allgemeine Verwaltung

4.1.1 Entwurf eines E-Government-Gesetzes des Bundes

Mit dem im September 2012 vom Bundeskabinett verabschiedeten Entwurf eines E-Government-Gesetzes sollen die von der Bundesregierung geförderten IT-Infrastrukturmaßnahmen für nutzerfreundliche und effiziente Verwaltungsdienste nutzbar gemacht werden.

Das ULD geht davon aus, dass der Entwurf eines Gesetzes zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften (E-Government-Gesetz), auch wenn es dem Wortlaut nach auf Bundesbehörden beschränkt ist, starke Auswirkungen auf die Länder und deren Verarbeitung personenbezogener Daten durch öffentliche Stellen haben wird. Ziel des Gesetzes soll es sein, durch den Abbau bundesrechtlicher Hindernisse generell die elektronische Kommunikation mit der Verwaltung zu erleichtern.

Das ULD begrüßt im Wesentlichen die vorgeschlagenen Regelungen. Sie können in den Bereichen der elektronischen Aktenführung und elektronischen Kommunikation mit Bürgerinnen und Bürgern Rechtssicherheit und Rechtsklarheit bringen. Um den datenschutzkonformen Einsatz der elektronischen Kommunikation zu gewährleisten, sind aber noch Änderungen nötig.

So sind die Rechte der Betroffenen bei Einsicht in elektronische Akten und die Verhältnisse zu anderen Informationszugangsrechten, wie z. B. dem Informationszugangsgesetz und dem Geodateninfrastrukturgesetz des Landes Schleswig-Holstein, nicht ausreichend klar dargelegt. Datenschutzrechtlich relevant sind die Regelungen zur elektronischen Kommunikation über die De-Mail. So soll es den Bürgerinnen und Bürgern nicht ermöglicht werden, differenziert nur mit einzelnen Behörden über De-Mail zu kommunizieren. Die Veröffentlichung der De-Mail-Adresse des Nutzers als Verbraucher mit diesem Zusatz im Verzeichnisdienst gilt generell als Zugangseröffnung. Mit Ablage der De-Mail im Postfach gilt ein Verwaltungsakt bzw. das Verfahrensschriftstück als zugegangen. Die für die Briefpost geltende Dreitagesfiktion soll nicht anwendbar sein; dies ist nicht gerade verbraucherfreundlich.

Gemäß dem Entwurf soll § 36a Abs. 2 SGB I geändert werden, wonach künftig bei der Kommunikation mit den Krankenkassen die Versicherten ihre Identität auch mit der elektronischen Gesundheitskarte (eGK) elektronisch nachweisen können. Dies bedeutet, dass die eGK entgegen den geltenden Bestimmungen in § 291a SGB V gegenüber der Krankenkasse als Identitätsnachweis genutzt werden darf, während in allen anderen vom E-Government-Gesetz erfassten Fällen nur der neue Personalausweis mit seinen höheren Sicherheitsanforderungen akzeptiert wird. Die eGK und deren Technik sind nicht für Identifikationsnachweise konzipiert. Eine Nachrüstung der eGK mit den zum Personalausweis geltenden Sicherheitsmerkmalen ist nicht sinnvoll, zumal 75 % der elektronischen Gesundheitskarten im Jahr 2012 schon ausgegeben worden sind.

Der Entwurf sieht für sämtliche Verwaltungskommunikation vor, dass beim Versenden von Daten durch eine De-Mail-Nachricht die jeweiligen akkreditierten Diensteanbieter eine kurzfristige automatische Entschlüsselung zum Zweck der Überprüfung auf Schadsoftware und zum Zweck der Weiterleitung an den Adressaten der De-Mail-Nachricht vornehmen sollen.

Entsprechendes soll für Sozial- und Steuerdaten durch eine Änderung des Sozialgesetzbuches X und der Abgabenordnung gelten. Dies hätte zur Folge, dass De-Mail-Nachrichten mit Daten, die dem Sozial- oder dem Steuergeheimnis unterliegen, durch Dritte zur Kenntnis genommen werden könnten, was deren Vertraulichkeit beeinträchtigen würde. Eine derartige Durchbrechung des Sozial- und des Steuergeheimnisses weitet die Zugangsmöglichkeit dieser besonders schutzbe-

dürftigen Daten ohne ausreichende Absicherungen unerwünscht aus. Durch eine Ende-zu-Ende-Verschlüsselung bei De-Mail könnte dagegen ein angemessenes Schutzniveau für die Versendung besonders schutzbedürftiger personenbezogener Daten erreicht werden.

Was ist zu tun?

Im Gesetzgebungsverfahren sollte der E-Government-Gesetzentwurf entsprechend nachgebessert werden.

4.1.2 Outsourcing öffentlich-rechtlicher Forderungen an private Inkassobüros

Unterstützungsleistungen privater Inkassobüros bei der Einziehung öffentlich-rechtlicher Forderungen sind nicht generell unzulässig. Sie unterliegen aber im Hinblick auf den Funktionsvorbehalt für den öffentlichen Dienst Restriktionen.

Bereits im Jahr 2003 haben wir uns eingehend mit der Einziehung privatrechtlicher kommunaler Forderungen durch private Inkassobüros befasst (25. TB, Tz. 4.1.5). Datenschutzrechtliche Bedenken können dadurch ausgeräumt werden, wenn für die Einhaltung der strengen Maßgaben zur Auftragsdatenverarbeitung gesorgt wird. Dies lässt sich allerdings nicht ohne Weiteres auf die Einziehung öffentlich-rechtlicher Forderungen übertragen. Das Landesverwaltungsgesetz erlaubt die Übertragung von Aufgaben der öffentlichen Verwaltung zur Erledigung in den Handlungsformen des privaten Rechts nur durch oder aufgrund eines Gesetzes. Eine solche Norm für die eigenverantwortliche Übertragung von Vollstreckungstätigkeiten auf Private besteht nicht. § 17 Abs. 6 LDSG erlaubt für den engen Bereich der beratenden oder begutachtenden Tätigkeiten im Zweifel die Übermittlung personenbezogener Daten, soweit dadurch die Grenzen der Auftragsdatenverarbeitung, insbesondere die Notwendigkeit der Erteilung abschließender Weisungen für die Durchführung des Auftrages, nicht außer Acht gelassen werden. Darüber hinaus muss sich Auftragsdatenverarbeitung auf bloße Hilfstätigkeiten ohne eigene Gestaltungs- und Entscheidungsmöglichkeiten des Auftragnehmers beschränken. Ein hoheitliches Auftreten des Auftragnehmers nach außen ist in jedem Fall ausgeschlossen.

Fraglich ist zudem, ob und in welchem Umfang eine Auftragsdatenverarbeitung im Kernbereich originärer Staatsaufgaben verantwortbar ist. Im Datenschutzrecht findet dieser Kernbereich z. B. darin seinen Ausdruck, dass für Steuerverfahren in der Abgabenordnung die Offenbarung personenbezogener Daten in sehr engen materiellen Grenzen abschließend geregelt ist. Eine Anwendung landesrechtlicher Vorschriften zur Auftragsdatenverarbeitung würde gegen höherrangiges Recht verstoßen und scheidet deshalb für diesen Bereich aus. Entsprechendes gilt für personenbezogene Daten, die einem besonderen Berufs- oder Amtsgeheimnis, etwa der ärztlichen Schweigepflicht, unterliegen.

Angesichts dieser Anforderungen bleiben bei der Einziehung öffentlich-rechtlicher Forderungen nur wenige Hilfs- und Unterstützungstätigkeiten, die einem privaten Inkassobüro übertragen werden können. Zugleich muss die Behörde einen nicht unerheblichen Verwaltungsaufwand auf sich nehmen, um ausreichend detaillierte Verträge und Weisungen mit dem Auftragnehmer zu vereinbaren und um anschließend die ordnungsgemäße Erfüllung des Auftrags zu kontrollieren. Angesichts dessen und der generellen Risiken, die immer mit einer Bekanntgabe besonders geschützter Daten aus hoheitlichen Verfahren an private Stellen verbunden sind, muss von einer Beteiligung privater Inkassobüros an der Einziehung öffentlich-rechtlicher Forderungen grundsätzlich abgeraten werden.

Was ist zu tun?

Schleswig-holsteinische Behörden sollten bei der Vollstreckung öffentlich-rechtlicher Forderungen auf die Einschaltung privater Inkassobüros in Form einer Auftragsdatenverarbeitung verzichten.

4.1.3 Geodaten und Verhaltenskodex

Die Datenschutzbeauftragten von Bund und Ländern sowie die Kommission für Geoinformationswirtschaft (GIW) des Bundesministeriums für Wirtschaft und Technologie erarbeiten ein gemeinsames Konzept zur datenschutzkonformen Geodatennutzung durch Wirtschaftsunternehmen und zur Bereitstellung von Geodatendiensten durch öffentliche Stellen.

Im Rahmen der Erarbeitung des Konzeptpapieres erwies es sich als sinnvoll, dass eine Abstimmung mit dem Landesvermessungsamt Schleswig-Holstein und dem Innenministerium des Landes Schleswig-Holstein stattfand. Auf Grundlage der erarbeiteten Studien des ULD aus den Jahren 2007, 2008 und 2010 konnten wir gemeinsam die wesentlichen Eckpunkte aus schleswig-holsteinischer Sicht festlegen.

https://www.datenschutzzentrum.de/geodaten/

Das ULD und das Landesvermessungsamt gehen davon aus, dass schutzwürdige Interessen Betroffener durch eine Übermittlung von Geodaten grundsätzlich nicht beeinträchtigt werden, wenn ein Kartenmaßstab größer als 1:5000 oder bei Bilddaten eine Auflösung von 20 cm pro Bildpunkt (Pixel) verwendet wird. Entsprechendes soll für Flächen gelten, die in einem Raster von mindestens 100 Meter mal 100 Meter dargestellt sind, sowie für Informationen, bei denen Daten von mindestens acht Haushalten aggregiert wurden.

Wollen Unternehmen darüber hinausgehende Geodaten mit Personenbezug erhalten und weiterverarbeiten, so planen die Landesbeauftragten und der Bundesbeauftragte für Datenschutz und die GIW-Kommission, ein Akkreditierungsverfahren für diese Unternehmen zu etablieren. Für die Akkreditierung selbst müssen die Unternehmen das Vorliegen eines Datenschutzmanagementsystems mit einem betrieblichen Datenschutzbeauftragten, geeigneten technisch-organisatorischen Maßnahmen nach § 9 BDSG, geeigneten Transparenzmaßnahmen, einer regelmäßigen Auditierung und einem Beschwerdemanagement nachweisen. Hat eine Akkreditierung des Unternehmens stattgefunden, so soll dies bei der Prüfung der schutzwürdigen Interessen Betroffener und der Nutzungsinteressen der Unternehmen durch die Geodaten haltende öffentliche Stelle berücksichtigt werden.

Wie und in welcher Form das Konzept von den Landesbeauftragten für den Datenschutz, dem Bundesbeauftragten für den Datenschutz und der GIW-Kommission verabschiedet wird, ist noch nicht abschließend entschieden. Für Schleswig-Holstein ist die Festlegung der aufgeführten Eckpunkte bereits in der Praxis bei Anfragen zu Geodaten hilfreich und kann technisch im Rahmen der Geodateninfrastruktur umgesetzt werden.

4.1.4 Geodaten und das Geodateninfrastrukturgesetz (GDIG)

Gemeinsam mit dem Landesamt für Vermessung Schleswig-Holstein hat das ULD entsprechend der sogenannten Ampelstudie die Kriterien zur Bewertung der Sensibilität von Geoinformationen weiterentwickelt und eine Klassifizierung vorgenommen.

Bei der Umsetzung der europäischen INSPIRE-Richtlinie, die zur Bereitstellung von behördlichen Geodaten für die Öffentlichkeit verpflichtet (30. TB, Tz. 8.14), hat das ULD für die einzelnen dort aufgeführten Daten eine Kategorisierung entspre-

chend einem vom ULD entwickelten Ampelsystem (31. TB, Tz. 5.2) gemeinsam mit dem Landesvermessungsamt vorgenommen. Für die im Annex I der INSPIRE-Richtlinie genannten Daten konnte weitgehend festgestellt werden, dass keine schutzwürdigen Belange von Personen betroffen sind, sodass aus Datenschutzgründen grundsätzlich keine Einwände gegen eine Veröffentlichung – auch über das Internet – bestehen. Eine solche Veröffentlichung erfolgt über das Geoportal des Landes Schleswig-Holstein:

http://www.gdi-sh.de/GDISH/DE/Service/GdiShDatenschutz/gdiShDatenschutz_node.html

4.1.5 Einheitliches Zeitwirtschaftssystem der Landesverwaltung

Elektronische Zeiterfassungssysteme sind mittlerweile zu komplexen Verfahren mutiert, in denen für unterschiedliche Zwecke auch Urlaubs- und Krankheitsdaten verwaltet werden.

Im Wortlaut: § 59 Abs. 1 MBG SH

Allgemeine Regelungen in Angelegenheiten, die nach § 51 der Mitbestimmung unterliegen und die über den Geschäftsbereich einer obersten Landesbehörde hinausgehen, sind zwischen den Spitzenorganisationen der zuständigen Gewerkschaften und der zuständigen obersten Landesbehörde zu vereinbaren.

Zur Modernisierung und Steigerung der Wirtschaftlichkeit der Landesverwaltung führt das Innenministerium als ressortübergreifendes Verfahren ein zentrales digitales Zeitwirtschaftssystem ein. Nach einer europaweiten Ausschreibung erhielt ein Produkt den Zuschlag, dessen Einsatz nicht nur einheitliche neue Hardware, sondern auch einheitliche Regelungen und Vorgaben zum Datenumgang nötig macht. Diese sind in Form einer Vereinbarung nach § 59 Mitbestimmungsgesetz Schleswig-Holstein (MBG SH) inzwischen geschaffen worden, die als öffentlich-rechtlicher Vertrag als Befugnisgrundlage zur Datenverarbeitung infrage kommt. In Vorbereitung der Verhandlungen mit den Spitzenorganisationen der Gewerkschaften haben wir das zuständige Finanzministerium bei der Erstellung eines entsprechenden Entwurfstextes beraten und folgende Punkte herausgearbeitet:

- Einrichtung einer zentralen Leitstelle

Um die mit einem einheitlichen Verfahren verbundenen Synergieeffekte real nutzen zu können, war von Anfang an geplant, die Zugriffsberechtigungen und Rollen durch eine ressortübergreifende Leitstelle für das digitale Zeitwirtschaftssystem zu vergeben. Diese sollte über die Berechtigung zur Wahrnehmung von Wartungsarbeiten und von vergleichbaren Unterstützungstätigkeiten verfügen sowie für Test und Freigabe des Systems verantwortlich sein. Da damit die Grenzen der Auftragsdatenverarbeitung weit überschritten werden, musste ein neuer Lösungsansatz gesucht werden.

Ähnliche Leitstellenprobleme treten auch in anderen Verfahren auf. Eine Neuregelung im LDSG gibt hierauf eine Antwort: Danach kann durch Rechtsverordnung der für das Verfahren zuständigen obersten Landesbehörde festgelegt werden, dass die Verantwortung für die Rechtmäßigkeit des automatisierten Verfahrens von der Verantwortung für die gespeicherten Daten abgetrennt und einer zentralen Stelle übertragen wird. Eine solche Funktionsübertragung ist nach dem Landesverwaltungsgesetz nur durch oder aufgrund eines Gesetzes zulässig. Die „Landesverordnung über die zentrale Stelle für das einheitliche und zentrale digitale Zeitsystem der Landesverwaltung Schleswig-Holstein“ ist inzwischen in Kraft. Erhebliche Einspareffekte ergaben sich schon allein dadurch, dass Dokumentation, Test, Freigabe und Vorabkontrolle für das Verfahren nur von einer Stelle vorgenommen werden mussten.

- Speicherfristen

Mit dem Finanzministerium besteht Einigkeit darüber, dass es sich bei den im Verfahren gespeicherten personenbezogenen Daten um sogenannte Personalaktendaten im beamtenrechtlichen Sinn handelt. Für Urlaubs- und Krankheitsdaten legt das Beamtenrecht ausdrücklich eine Speicherfrist von fünf Jahren nach Ablauf des Jahres, in dem die Bearbeitung des einzelnen Vorgangs abgeschlossen wurde, fest. Für Arbeitszeitdaten besteht keine vergleichbare spezielle Regelung. Diese Daten sind gemäß den allgemeinen Regeln zu löschen, wenn sie zur rechtmäßigen Aufgabenerfüllung der datenverarbeitenden Stelle nicht mehr erforderlich sind. Zwischen

dem Ministerium und dem ULD konnte Einvernehmen erzielt werden, dass weder für Revisionszwecke noch für statistische Auswertungen zum Zweck der Personalplanung oder der Personalwirtschaft eine personenbezogene Speicherung für mehr als ein Jahr erforderlich ist. Die Frist wurde deshalb entsprechend verkürzt.

- Revision der Arbeitszeitdaten

Das Erforderlichkeitsprinzip und das besondere Vertraulichkeitsgebot für Personalakten verpflichten dazu, Kenntnisnahmen innerhalb einer Verwaltung nur so weit zuzulassen, wie dies im Rahmen ihrer funktionalen Zuständigkeit notwendig ist. Dabei ist der Gesetzgeber davon ausgegangen, dass Personalverwaltungsaufgaben in einer eigenständigen Organisationseinheit, losgelöst von den unmittelbaren Dienst- und Fachaufsichtsaufgaben unmittelbarer Vorgesetzter, wahrgenommen werden. Das Beamtenrecht beschränkt das Zugangsrecht zu Personalakten auf Beschäftigte, die mit der Bearbeitung von Personalangelegenheiten beauftragt sind. Andere Mitarbeiter, und damit sind insbesondere die unmittelbaren Vorgesetzten gemeint, dürfen nur im Einzelfall die für ihre Aufgabenerfüllung tatsächlich erforderlichen Daten zur Kenntnis erhalten.

Zur notwendigen Revision der Arbeitszeitdaten der Mitarbeiter gehört eine Plausibilitätsprüfung der erfolgten Buchungen. Entsprechende Kenntnisse über Abwesenheiten der Mitarbeiter sind üblicherweise nur bei den zuständigen Fachvorgesetzten vorhanden. Diese haben deshalb die erfassten Daten auf ihre Richtigkeit hin zu überprüfen. Darüber hinaus ist eine Einsicht in diese automatisierte Personalteilakte des Mitarbeiters nicht erforderlich. Aus der Natur der Sache heraus muss eine Revision zeitnah erfolgen, da dem Beschäftigten bei Unstimmigkeiten eine Stellungnahme nur zuzumuten ist, wenn er sich an die Umstände einzelner Buchungen noch erinnern kann. Als zumutbare Frist können drei Monate angesehen werden.

In der Ausschreibung für das Zeitwirtschaftssystem war vorgesehen, nur ein einmaliges Leserecht der Fachvorgesetzten in den Arbeitszeitkonten ihrer Mitarbeiter zu erlauben. Gleichzeitig sollte ein entsprechender Prüfungsvermerk protokolliert werden. Leider ist das ausgewählte Produkt nicht in der Lage, diese Anforderung zu erfüllen. Als Alternative haben wir uns mit dem Finanzministerium darauf verständigt, dass den Fachvorgesetzten ein eingeschränktes Leserecht für drei Monate rückwirkend ab Monatsabschluss eingeräumt werden soll. Diese Frist berücksichtigt den Umstand, dass Vorgesetzten nicht immer unmittelbar nach Monatsschluss eine Plausibilitätsprüfung möglich ist, weil sie selbst krank sind oder sich im Urlaub befinden. Alle lesenden Zugriffe der Vorgesetzten sollen protokolliert und im Konto der Mitarbeiter angezeigt werden. Diese Anforderung wurde inzwischen technisch umgesetzt. Damit ist eine ausreichende Revisionsfähigkeit gegeben.

4.1.6 KoPers – ein neues Personalmanagementsystem

Das neue Personalmanagementsystem KoPers ist als „integriertes Verfahren“ geplant, in dem notwendige Personaldaten sowohl für Personalverwaltungs- als auch für -abrechnungszwecke nur einmal vorgehalten werden. Wesentliche Einsparungen und Rationalisierungseffekte werden damit angestrebt.

Um dieses Ziel zu erreichen, sind noch einige Hürden zu überwinden. Ursprünglich sollte die Einführung ausschließlich elektronisch geführter Personalakten in KoPers erst in einer späteren Ausbaustufe erfolgen. Allerdings mussten wir bei einer Prüfung im Finanzverwaltungsamt feststellen, dass die dort geführten Besoldungs-, Vergütungs- und Beihilfeakten bereits seit Längerem nur noch papierlos vorgehalten werden. Eine entsprechende Ermächtigung ist zwar im Landesbeamtengesetz enthalten. Allerdings sind bei solchen Akten die Vertraulichkeit der Daten sowie die Rechte der Betroffenen durch geeignete technische und organisatorische Maßnahmen sicherzustellen. Hierzu gehört nicht nur deren Personalakteneinsichtsrecht, sondern auch der Anspruch auf effektiven Rechtsschutz durch eine beweissichere Dokumentation der sie betreffenden dienstrechtlichen Entscheidungen in ihrer elektronischen Personalakte. Die zu ergreifenden Maßnahmen müssen dem Stand der Technik entsprechen und im Hinblick auf die Schutzbedürftigkeit der Daten erforderlich und angemessen sein.

Aus unserer Sicht kann nur eine qualifizierte elektronische Signatur diesen Anforderungen angemessen genügen. Eine solche Signatur ist seit Anfang 2012 im Personenstandswesen zwingend vorgeschrieben. Nennenswerte Probleme sind hierbei in der Praxis nicht aufgetreten. Ein personeller Mehraufwand bei der Bearbeitung war nicht festzustellen. Auch die Kosten für die

auszustellenden Signaturkarten blieben im vertretbaren Rahmen. Eine entsprechende Klarstellung für elektronische Personalakten im Landesbeamtengesetz, wie sie beispielsweise in Mecklenburg-Vorpommern besteht, wäre hier sehr hilfreich.

Die Personalakte dient der rechtssicheren Dokumentation des Rechtsverhältnisses zwischen dem Beschäftigten und seinem Dienstherrn. Insoweit haben papierene Dokumente in Personalakten wegen ihrer hohen Fälschungssicherheit als Urkunde einen hohen Beweiswert. Nachträgliche Veränderungen oder Einfügungen sind relativ leicht zu erkennen und nachzuweisen. Die für das Dokument verantwortliche Person kann durch ihre handschriftliche Unterschrift zweifelsfrei identifiziert werden. Eine vergleichbare Beweiskraft für elektronisch gespeicherte Dokumente liegt nach der Zivilprozessordnung erst vor, wenn sie mit einer qualifizierten elektronischen Signatur versehen sind.

Eine Dokumentation der für elektronische Personalakten getroffenen Datensicherheitsmaßnahmen des Finanzverwaltungsamtes lag uns bis Redaktionsschluss noch nicht vor. Es besteht aber Einvernehmen, dass der Status quo nicht für KoPers übernommen werden kann. Wir empfehlen als zukunftsfähige Lösung die Einführung der qualifizierten elektronischen Signatur, weil damit ein Höchstmaß an Datensicherheit auf Dokumentenebene erreicht werden kann. Für die Übernahme papierener Unterlagen in elektronische Personalakten können so alle beim Finanzverwaltungsamt eingescannten Dokumente vor der Vernichtung per Sammelsignatur beweiskräftig gesichert werden. Entscheidungen über Besoldung und Vergütung, die den Betroffenen per Stammblatt mitgeteilt werden, können zusätzlich als elektronisches Dokument im Verfahren gespeichert und ebenfalls durch eine qualifizierte elektronische Signatur gesichert werden. Damit wäre gleichzeitig eine halbwegs verständliche Einsichtnahme für Betroffene in ihre elektronische Personalakte möglich.

Neu bei KoPers wird die Einrichtung einer zentralen Stelle für die Gewährleistung der Ordnungsmäßigkeit der automatisierten Datenverarbeitung sein. Diese wurde notwendig, weil das Verfahren für den gesamten Bereich der Landesverwaltung nach einheitlichen Merkmalen bei Dataport als Auftragnehmer betrieben werden soll. Aufgabe der zentralen Stelle ist es, die technischen und fachlichen Anforderungen für das Land als Auftraggeber gegenüber Dataport zu definieren und anschließend deren Einhaltung zu kontrollieren und zu dokumentieren.

Die zentrale Stelle wurde inzwischen per Rechtsverordnung auf der Grundlage des Landesdatenschutzgesetzes bei der Staatskanzlei eingerichtet. Damit erfolgt eine organisatorische Trennung zwischen der Verantwortung für das automatisierte Verfahren und der Verantwortung für die Richtigkeit der Daten, die weiter bei den personalverwaltenden Stellen verbleibt. Derartige zentrale Verfahren sind tatsächlich nur beherrschbar, wenn dafür eine zentral verantwortliche Stelle geschaffen wird. Mit der Trennung der Verantwortung entstehen neue Fragen zur Zusammenarbeit zwischen der zentralen und den beteiligten Stellen, zu den Verwaltungsabläufen bei Mängeln im Verfahren sowie zur Verantwortung für Personalentscheidungen gegenüber den Betroffenen. Noch zu erarbeitende Einzelheiten lassen sich in den nach der Landesverordnung für die Errichtung der zentralen Stelle vorgesehenen Nutzungsbestimmungen regeln. Alle Beteiligten sollten sich im Klaren sein, dass hier noch Pionierarbeit zu leisten ist, bei der wir gerne weiterhin beraten.

4.1.7 Übertragung von IT-Dienstleistungen auf einen Zweckverband

Ein Zweckverband wird durch die Übertragung von öffentlich-rechtlichen Aufgaben der angeschlossenen Verbandskommunen zur datenverarbeitenden und damit verantwortlichen Stelle im Sinne des LDSG. Der Aufgabenübergang kann auch „teilweise“ erfolgen. So besteht die Möglichkeit, die Verantwortung für die Ordnungsmäßigkeit eines automatisierten Verfahrens von der Verantwortung für die Richtigkeit der Daten abzutrennen und separat auf den Zweckverband zu übertragen.

Einem Zweckverband waren von den angeschlossenen Kommunen die Erbringung von IT-Dienstleistungen als eigene Aufgabe übertragen worden. Wir prüften zunächst, ob eine Auftragsdatenverarbeitung oder eine Funktionsübertragung vorlag. Eine Auftragsdatenverarbeitung nach dem LDSG kommt nur in Betracht, soweit keine eigene Zuständigkeit bzw. rechtliche Verantwortung für die jeweilige Datenverarbeitung beim Zweckverband besteht. Eine rechtliche Verantwortung setzt nach dem Landesverwaltungsgesetz voraus, dass

Aufgaben der öffentlichen Verwaltung zur Erledigung in den Handlungsformen des öffentlichen Rechts durch Gesetz oder aufgrund eines Gesetzes übertragen werden. Genau dies war im vorliegenden Fall geschehen.

Das Gesetz über die kommunale Zusammenarbeit (GkZ) erlaubt ausdrücklich die Übertragung von Aufgaben der öffentlichen Verwaltung auf einen Zweckverband. Rechte und Pflichten der an einem Zweckverband beteiligten Kommunen gehen zur Erfüllung der Aufgaben der öffentlichen Verwaltung, die dem Zweckverband übertragen werden, einschließlich des Satzungs- und Verordnungsrechts auf den Zweckverband über. Im konkreten Fall lag der für die Aufgabenübertragung bzw. für die Errichtung des Zweckverbandes erforderliche öffentlich-rechtliche Vertrag zwischen den beteiligten Kommunen bereits vor.

Unter dem Begriff „Aufgabenübertragung“ ist die vollständige Erfüllung bestimmter sachlicher Aufgaben (Aufgaben im materiellen Sinn) zu verstehen. Dem Zweckverband wurden jedoch nur die bei der Aufgabenerfüllung anfallenden IT-Dienstleistungen, also eine technische Hilfeleistung für die materielle Aufgabenerfüllung, übertragen. Insoweit sind die beteiligten Kommunen einen neuen Weg der kommunalen Zusammenarbeit gegangen. Dieser wurde erst mit der letzten Änderung des GkZ im Jahr 2012 dadurch eröffnet, dass eine partielle Aufgabenübertragung zugelassen wurde.

Gemäß der Gesetzesbegründung soll die Ergänzung, wonach dem Zweckverband Aufgaben der öffentlichen Verwaltung nunmehr „ganz oder teilweise“ übertragen werden können, der Angleichung der Begrifflichkeit an die Regelungen zu Kommunalunternehmen in der Gemeindeordnung dienen und das Instrument „Zweckverband“ als Form der kommunalen Zusammenarbeit auch für verwaltungsinterne Dienstleistungen nutzbar machen. Hierzu gehöre insbesondere die Unterstützung der öffentlichen Verwaltung durch Informations- und Kommunikationstechniken. Die Kommunen könnten so den Aufgabenbereich des Zweckverbandes flexibel gestalten, sodass dieser auch quasi als „Erfüllungsgehilfe“ für die Kommunen tätig werden kann und die Kommune Aufgabenträger bleibt.

Die Neuregelung verfolgt also weitgehend den gleichen Zweck wie die Regelung über die Einrichtung einer zentralen Stelle im LDSG. In beiden Fällen wird die Verantwortung für die Ordnungsmäßigkeit des automatisierten Verfahrens von der Verantwortung für die gespeicherten Daten getrennt. Der Zweckverband wird für das automatisierte Verfahren zur verantwortlichen Stelle. Die Einzelheiten regelt hier allerdings nicht eine Verordnung, sondern ein öffentlich-rechtlicher Vertrag bzw. die Verbandssatzung. Mit der Gründung des Zweckverbandes geben die beteiligten Kommunen insoweit ihre Zuständigkeit für die Erbringung von IT-Dienstleistungen auf. Damit geht die Verantwortung für die Ordnungsmäßigkeit der automatisierten Verarbeitung personenbezogener Daten vollständig auf den Zweckverband über.

Eine Auftragsdatenverarbeitung durch den Zweckverband kommt in diesem Zusammenhang noch in Betracht, wenn dem Zweckverband nicht angehörende dritte Stellen entsprechende Aufträge erteilen. Es ist z. B. Auftragsdatenverarbeitung, wenn der Zweckverband für angeschlossene Schulträger administrative IT-Dienstleistungen bei Schulgeräten vornimmt, da die Schulen eigenständige datenverarbeitende Stellen sind. Die Verantwortung für die Verarbeitung der personenbezogenen Daten der Schülerinnen und Schüler sowie der Eltern trägt nach der Datenschutzverordnung Schule die Schulleiterin oder der Schulleiter. Ist bei einem Verbandsmitglied ein Schulamt eingerichtet, so ist das Schulamt als untere Landesbehörde ebenfalls eine eigenständige datenverarbeitende Stelle. Die Administration der dortigen EDV-Geräte ist ebenfalls Auftragsdatenverarbeitung. Entsprechendes gilt für die personenbezogene Verarbeitung auf Geräten, die vom Träger des schulpsychologischen Dienstes im Rahmen seiner Verpflichtung nach dem Schulgesetz für die Schulpsychologinnen und Schulpsychologen beschafft wurden.

Was ist zu tun?

Das Modell des Zweckverbandes ist ein geeignetes Instrument zur Errichtung einer zentralen Stelle für zusammen betriebene automatisierte Verfahren im kommunalen Bereich zur Sicherung der Ordnungsmäßigkeit des Verfahrens. Der Zweckverband bedarf dann natürlich nicht nur technischer, sondern auch fachbereichsspezifischer Kompetenz. Das mögliche Einsparpotenzial dieser Zusammenarbeit ist beträchtlich.

4.1.8 Kommunaler Bürgerservice – Nutzung von eIDs

Der neue Personalausweis wird seit über zwei Jahren ohne nennenswerte Probleme ausgegeben. Leider stehen dem noch immer keine ausreichenden Nutzungsmöglichkeiten gegenüber. Öffentliche Stellen mit intensivem Bürgerkontakt wie die Kommunen haben insofern besondere Möglichkeiten und Verpflichtungen. Die Nutzung des elektronischen Identitätsnachweises (eID) kann Vorbild sein für den privaten Bereich und kann die Servicequalität und Datensicherheit deutlich verbessern.

Bis Herbst 2012 wurden in Deutschland mehr als 17 Millionen neue Personalausweise (nPA) mit eID-Funktion ausgegeben. Mit Ausnahme des Verkehrszentralregisters beim Kraftfahrt-Bundesamt findet bis heute praktisch noch keine Nutzung im öffentlichen Sektor statt. Dabei wäre es einfach, erste kleine Schritte zu tun: Statt die Bürgerinnen und Bürger zu relativ unsicheren E-Mail-Kontakten zu ihrer Gemeinde- oder Kreisverwaltung zu verleiten, könnten diese auf ihrer Homepage ein Mitteilungsfenster, vergleichbar einem Webmail-verfahren, integrieren, wo das Anliegen an die Behörde über eine SSL-verschlüsselte Leitung, also auf einem sicheren Übertragungsweg, mitgeteilt werden kann. Würde dieses Vorgehen mit der eID-Funktion des neuen Personalausweises verknüpft, wäre zudem eine zweifelsfreie Identifikation des Absenders für die Behörde möglich. Die Nutzung der eID eröffnet große Potenziale beim E-Government. Anders als bei einer E-Mail könnten darüber verbindliche Anträge, z. B. für die Bereitstellung von Mülltonnen, für die Anforderung von Briefwahlunterlagen, Meldebescheinigungen o. Ä., gestellt werden. Eine persönliche Vorsprache beim Amt wäre oft entbehrlich, was auch die Behörden entlasten würde.

Natürlich erfordert die Integration der eID-Funktion in die kommunale Homepage einen gewissen Aufwand. Dieser kann aber durch eine zentrale Organisation über einen Dienstleister, z. B. durch Dataport, minimiert werden. Vorstellbar ist auch ein zentrales Angebot für alle Kommunen über das bestehende Schleswig-Holstein-Gateway, von wo Nachrichten gesichert an die jeweilige Kommune weitergeleitet werden könnten. Kommunale Dienstleister könnten sich hier ein attraktives neues Geschäftsfeld eröffnen.

Wegen des hohen Sicherheitsstandards dieses Verfahrens würde zugleich eine wesentliche Verbesserung des Datenschutzes und der Datensicherheit erreicht. Insbesondere könnte die bisher praktizierte unverschlüsselte E-Mail-Kommunikation zurückgedrängt werden.

Was ist zu tun?

Dataport sollte ebenso wie private Dienstleister prüfen, ob sie den Kommunen ein Angebot zur Integration der eID-Funktion auf kommunalen Homepages unterbreiten können. Kommunen sollten diese Wünsche an ihren Dienstleister herantragen. Bund und Land sollten über ein Angebot zur Projektförderung nachdenken.

4.1.9 Bürgerbegehren und der Umgang mit Unterschriftenlisten

Bürgerbegehren geben immer wieder Anlass zur Kritik beim Umgang mit den dazugehörigen Unterschriftenlisten. Die maßgeblichen Rechtsvorschriften eröffnen Interpretationsspielräume, die zu Rechtsunsicherheit führen. Das Innenministerium bemüht sich inzwischen um Klarstellungen.

In einem Fall wurde ein Bürgerbegehren mit den dazugehörigen Antragslisten bei der dafür zuständigen Amtsverwaltung abgegeben. In diese Listen sind neben der Unterschrift der Familienname, Vorname, Wohnort mit Postleitzahl, Straße und Hausnummer sowie das Datum der Unterzeichnung einzutragen. Mit diesen Angaben kann festgestellt werden, ob die Unterzeichner am Tag des Eingangs des Antrags bei der Gemeinde dort wahlberechtigt und damit beteiligungsberechtigt waren. Die Amtsverwaltung hatte die Antragslisten zeitnah als zuständige Meldebehörde geprüft. Anschließend wurden sie zuständigkeitshalber an die Kommunalaufsichtsbehörde abgegeben, allerdings nicht ohne vorher zwei Kopien angefertigt zu haben. Eine Kopie war „für den Dienstgebrauch" bestimmt, die andere wurde dem ehrenamtlichen Bürgermeister der Gemeinde zugeleitet. Seitens der Beschwerdeführer wurde zunächst vermutet, dass der Bürgermeister die Daten für eine Kontaktaufnahme mit den Unterstützern des Bürgerbegehrens genutzt habe, um diese zu beeinflussen. Bei unseren Ermittlungen hat sich diese Vermutung allerdings nicht bestätigt.

Dennoch war einiges schiefgelaufen. Nach der Landesverordnung zur Durchführung der Gemeinde-, der Kreis- und der Amtsordnung ist lediglich die Kopie einer einzelnen Antragsliste und eines Einzelantrags, quasi als Muster, der Kommunalaufsichtsbehörde zu übersenden, weil über die Anzahl der Beteiligten und damit über das Erreichen des Quorums die zuständige Meldebehörde entscheidet. Die Kopie sämtlicher Listen „für den Dienstgebrauch" wäre deshalb entbehrlich gewesen.

Für eine Weiterleitung der vollständigen Antragslisten an den ehrenamtlichen Bürgermeister gab es auch keine Notwendigkeit und keine Rechtfertigung. Die Verwendung der Daten ist ausschließlich zum Zweck der Feststellung der Beteiligungsberechtigung und damit zur Ermittlung des Quorums vorgesehen. Das Datenschutzrecht erlaubt eine Kenntnisnahme durch Funktionsträger als eine Form der Verarbeitung personenbezogener Daten nur, soweit dies zur rechtmäßigen Aufgabenerfüllung erforderlich ist. Diese Voraussetzung war hinsichtlich des ehrenamtlichen Bürgermeisters nicht erfüllt.

Die zuständige Kommunalaufsichtsbehörde hatte im vorliegenden Fall bestätigt, dass die von der Amtsverwaltung getroffenen Entscheidungen zum Umgang mit dem Bürgerbegehren im gegenseitigen Einvernehmen getroffen wurden. Sie hatte überflüssigerweise die vollständigen Unterschriftenlisten erhalten und nichts dagegen unternommen. Das Innenministerium als oberste Kommunalaufsichtsbehörde nahm diesen Fall zum Anlass, den Umgang mit Bürgerbegehren anlässlich der jährlichen Dienstbesprechung mit den Kommunalaufsichtsbehörden der Kreise zu erörtern. Im konkreten Fall haben die Beteiligten versichert, dass die eigene Verfahrensweise künftig an die vom Innenministerium dargestellte Rechtslage angepasst wird.

Was ist zu tun?

Kommunen sollten ihre Verwaltungspraxis beim Umgang mit Daten aus Bürgerbegehren sorgfältig prüfen und mit der zuständigen Kommunalaufsichtsbehörde abstimmen. Unter dem Gesichtspunkt der Normenklarheit sollte die Landesverordnung zur Durchführung der Gemeinde-, der Kreis- und der Amtsordnung im Hinblick auf eine Präzisierung der einschlägigen Verfahrensregelungen überprüft werden.

4.1.10 Was bringt das neue Bundesmeldegesetz?

Die Ausweitung automatisierter Datenabrufe durch öffentliche und private Stellen sowie Änderungen bei den Anforderungen für Melderegisterauskünfte im neuen Bundesmeldegesetz (BMG) haben erhebliche Auswirkungen auf die Persönlichkeitsrechte der Meldepflichtigen.

Nach dem Übergang der Gesetzgebungskompetenz für das Meldewesen auf den Bund wurde nach langer politischer Diskussion ein neues Bundesmeldegesetz verabschiedet. Es enthält an zentralen Stellen deutliche Änderungen gegenüber der bisherigen Rechtslage in den Ländern. Aus diesem Grund sollen nachfolgend die wichtigsten Regelungen auf den datenschutzrechtlichen Prüfstand gestellt werden. Es bleibt fraglich, ob die mit den Änderungen verbundenen Belastungen für die Bürgerinnen und Bürger in einem angemessenen Verhältnis zu dem gesetzlich verfolgten Ziel eines Melderechts „als multifunktionale Grundlagen- und Querschnittsverwaltung“ steht.

- Mitwirkung des Vermieters bei der Anmeldung

Die Mitwirkungspflicht des Wohnungsgebers war erst im Jahr 2002 abgeschafft worden. Sie wird jetzt in verschärfter Form wieder eingeführt, in der Hoffnung, Scheinanmeldungen wirksamer verhindern zu können. Bis heute liegen keine belastbaren Daten darüber vor, ob und in welchem Umfang überhaupt solche Scheinanmeldungen in den Melderegistern gespeichert sind. Nennenswerte Probleme sind in dieser Hinsicht jedenfalls in schleswig-holsteinischen Meldebehörden nicht bekannt geworden. Das neue Gesetz verpflichtet den Wohnungsgeber oder eine von ihm beauftragte Person, den Einzug oder Auszug schriftlich oder elektronisch zu bestätigen. Für die Prüfung, ob die von der meldepflichtigen Person gemachten Angaben richtig sind, hat die Meldebehörde den Namen und die Anschrift des Eigentümers der Wohnung und, wenn dieser nicht selbst Wohnungsgeber ist, auch den Namen und die Anschrift des Wohnungsgebers im Melderegister zu speichern. Hinzu kommen Hinweise zum Nachweis der Richtigkeit der Daten.

Die praktischen Auswirkungen dieser Neuregelung sind zunächst ein erheblicher Mehraufwand für Bürger und Verwaltung. Meldepflichtige vergessen häufig bei ihrem ersten Besuch in der Meldebehörde ihre Vermieterbescheinigung. Diese zu beschaffen ist für sie nicht immer einfach, insbesondere wenn der Vermieter nicht vor Ort wohnt oder nicht kurzfristig erreichbar ist. Sukzessive entsteht über die Neuregelung ein vollständiges Wohnungseigentümerverzeichnis im Melderegister. In Mehrfamilienhäusern mit unterschiedlichen Wohnungseigentümern muss eine Zuordnung der Meldepflichtigen über die eigentliche Anschrift hinaus zu einzelnen Wohnungen erfolgen. Auch wegen des für die Kommunen mit den Neuerungen hinzukommenden Aufwands sieht das Innenministerium die Wiedereinführung der Mitwirkungspflicht ebenso wie das ULD kritisch.

- Automatisierte Datenabrufe öffentlicher und privater Stellen

Automatisierte Datenabrufe werden schon heute in den Ländern praktiziert. Sowohl öffentliche als auch private Stellen können damit Melderegisterauskünfte über das Internet einholen. Wichtige Sicherheitsanforderungen, z. B. eine verschlüsselte Auskunftserteilung oder eine umfassende Protokollierung der Abrufe, sind ausdrücklich gesetzlich festgelegt. Gegenüber schriftlichen Auskünften der Meldebehörden per Post ist das automatisierte Abrufverfahren nicht nur effizienter und schneller, sondern auch sicherer. Die Vorteile des automatisierten Verfahrens sind aus unserer Sicht eindeutig: Briefpost kann verloren gehen oder von Unbefugten gelesen werden. Eingabe- und Übertragungsfehler der Meldebehörden sind im automatisierten Verfahren weitgehend ausgeschlossen. Die Einhaltung der Kriterien für die vorgeschriebene Identitätsprüfung hinsichtlich der gesuchten Person kann durch die EDV-Programme bestmöglich sichergestellt werden. Eine umfassende und automatisiert auswertbare Protokollierung der Abrufe gewährleistet ein Höchstmaß an Revisionssicherheit. Quasi als Nebeneffekt ermöglicht diese Protokollierung präzise Auskünfte gegenüber Betroffenen über die Weitergabe ihrer Daten. Vor diesem Hintergrund ist der Wegfall der bisherigen Widerspruchsmöglichkeit für Betroffene gegen Online-Auskünfte an private Stellen konsequent. Damit war aus Sicht des ULD kein Gewinn für ihre Persönlichkeitsrechte verbunden.

- Phonetische Suche bei automatisierten Datenabrufen

Neu eingeführt wird die Möglichkeit, bei Familiennamen, früheren Namen und Vornamen eine phonetische Suche vorzunehmen. Das Gesetz sagt allerdings nicht, was genau unter einer phonetischen Suche zu verstehen ist. Werden aufgrund eines Abrufs einer öffentlichen Stelle die Daten-

sätze mehrerer Personen gefunden, dürfen diese vollständig übermittelt werden, auch wenn klar ist, dass nur eine Person die oder der Gesuchte sein kann, die anderen Datensätze folglich unbeteiligte Dritte betreffen. Bei Auskünften an private Stellen wird selbst bei einer phonetischen Suche gefordert, dass die Identität der gesuchten Person eindeutig festgestellt wird. Dies ist ein Widerspruch in sich. Es bleibt abzuwarten, ob noch zu erlassende Ausführungsbestimmungen für die phonetische Suche für mehr Klarheit sorgen.

- Einfache Melderegisterauskunft an private Stellen

Nach heftiger öffentlicher Kritik an der Beschlussfassung des Deutschen Bundestags hat der Bundesrat deutliche Verbesserungen bei den Anforderungen an die Erteilung einfacher Melderegisterauskünfte vorgeschlagen. Bei Auskünften zu gewerblichen Zwecken müssen diese angegeben und dürfen anschließend nur für diesen Zweck verwendet werden. Danach sind die Daten zu löschen. Werden Daten zur geschäftsmäßigen Anschriftenermittlung für Dritte erhoben, dürfen diese vom Dienstleister nicht für eigene Zwecke weiterverwendet werden. Sollen Daten für Zwecke der Werbung oder des Adresshandels verwendet werden, ist dies nur mit ausdrücklicher Einwilligung der Betroffenen zulässig.

Für das Verbot des Adresspooling sowie für die Bereiche Werbung und Adresshandel dürften die Regelungen eine ausreichende Revisionsfähigkeit gewährleisten. Aufgrund von Eingaben Betroffener oder durch gezielte Auswertung der Protokolldatenbestände hinsichtlich einzelner Empfänger werden „schwarze Schafe“ wohl schnell feststellbar sein. Gegebenenfalls können entsprechende Bußgelder auf der Grundlage der ebenfalls ergänzten Bußgeldvorschriften verhängt werden. Auch der generelle Ausschluss vom automatisierten Verfahren für die Nutzung der einfachen Melderegisterauskunft ist eine mögliche Konsequenz.

4.1.11 Externe Dienstleister als behördliche Datenschutzbeauftragte?

Die Erfahrung zeigt, dass die Bestellung eines behördlichen Datenschutzbeauftragten zu einer wesentlichen Erhöhung des Datenschutzniveaus in den betreffenden Behörden führt. Das ULD unterstützt daher ausdrücklich derartige Bestellungen. An das ULD wird immer wieder die Frage herangetragen, ob wegen der nicht absolut klaren Formulierung in § 10 Landesdatenschutzgesetz auch externe Dienstleister behördliche Datenschutzbeauftragte in Schleswig-Holstein sein dürfen. Wir können jedoch hierbei keine Unklarheit erkennen. Aber auch wegen der umfassend gewährten Kontrollrechte innerhalb einer hoheitlich tätigen Verwaltung muss die Funktion eines behördlichen Datenschutzbeauftragten immer durch einen Beschäftigten oder eine Beschäftigte der datenverarbeitenden Stelle ausgeführt werden. Gemäß § 10 Abs. 1 Satz 2 Landesdatenschutzgesetz ist eine explizite enge Ausnahme vorgesehen: Mehrere datenvverarbeitende Stellen können gemeinsam einen behördlichen Datenschutzbeauftragten bestellen. Private Dienstleister oder sonstige Externe, die nicht Angehörige öffentlicher Stellen sind, dürfen also unzweifelhaft nicht bestellt werden.

Externe Dienstleister können wohl als Sachverständige für allgemeine Fragen der Organisation der Verfahren und für technische Beratungen herangezogen werden. Ein Zugriff auf personenbezogene Daten darf einem externen Berater aber nur unter den Bedingungen des § 17 Abs. 6 LDSG gewährt werden. Die Kontrolle der Datenverarbeitung bei der jeweiligen Stelle obliegt allein der oder dem behördlichen Datenschutzbeauftragten.

4.2 Polizei und Verfassungsschutz

4.2.1 @rtus beschäftigt die Polizei – und das ULD

Seit der Einführung von @rtus als Vorgangsbearbeitungssystem (VBS) der schleswig-holsteinischen Polizei wird an vielen Stellen versucht, Mängel der Anfangsphase zu beseitigen und Optimierungen vorzunehmen. Bei dem laufenden Verfahren bestehen aber auch noch lange währende Unzulänglichkeiten. Aus unserer Sicht muss eine Trennung der Datenbestände, die für unterschiedliche Zwecke gespeichert werden, erfolgen. Hier wie auch in anderen Bereichen, etwa der Weiterentwicklung von @rtus, gibt es positive Entwicklungen.

- @rtus-VBS – unterschiedliche Nutzung durch separate Datenspeicherung

Das Vorgangsbearbeitungssystem @rtus dient der Polizei primär dazu, alles, was in den Akten der Polizei festgehalten wird, elektronisch zu erfassen und für die Bearbeitung zu speichern. Dies erlaubt das Gesetz; dieses sieht aber für eine weitere Speicherung und Nutzung der Daten einschränkende Regelungen vor, nämlich eine Begrenzung der Datenspeicherung und -nutzung für Zwecke der Dokumentation und der Vorgangsverwaltung. Die nötige Trennung der für die Vorgangsbearbeitung gespeicherten Daten von denen, die für die Dokumentation und Vorgangsverwaltung gespeichert werden dürfen, bereitete lange Zeit nicht nur technische Schwierigkeiten. Schon in der Planungsphase legten wir der Polizei nahe, @rtus entsprechend diesen gesetzlichen Vorgaben zu konzipieren. Die Polizei hat nun, auch auf Druck des Innenministeriums, ein Konzept erarbeitet, das im Wege der Zugriffsbeschränkung eine logisch differenzierte Nutzung der Daten aus @rtus-VBS vorsieht. Durch die vorgesehene abgestufte Zugriffsregelung wird in vielen Fällen bereits ein Zustand erreicht, der den bestehenden gesetzesfernen Zustand minimiert.

Die Polizei hat eine erste Aufstellung der Daten vorgelegt, die sie für die Zwecke Vorgangsverwaltung und Dokumentation für erforderlich erachtet. Der diesbezüglich genannte Umfang der Daten ist nach unserer Auffassung noch zu weit. Hierzu sind noch Gespräche mit dem ULD vereinbart. Gleichwohl plant die Polizei, das Gesamtkonzept im Zusammenhang mit der Erstellung der notwendigen Errichtungsanordnung umzusetzen. Das Innenministerium sicherte uns zu, dass mit der vorgesehenen Implementierung der Trennung der Datenbestände die notwendige Abstimmung mit dem ULD weder verhindert noch ausgeschlossen werden soll. Ein Präjudiz für künftige Beteiligungen des ULD sei mit dem hier praktizierten Verfahren ausdrücklich nicht beabsichtigt. Unter diesen Voraussetzungen haben wir uns mit dem Vorgehen einverstanden erklärt. Die Lösungen zu verbleibenden kritischen Fällen sollen nach Abstimmung mit dem ULD dann zeitnah in das Verfahren eingearbeitet werden. Das ULD wird das neue Verfahren baldmöglichst unter rechtlichen und technischen Aspekten durchleuchten.

- @rtus-VBS – Evaluierung notwendig

Das ULD bat nach vorausgegangenen Gesprächen mit dem Innenministerium und der Polizei im Mai 2010 die Polizei, eine Evaluierung des vorhandenen @rtus-VBS-Datenbestandes durchzuführen, um zunächst aus polizeilicher Sicht eine sachgerechte Differenzierung vorzunehmen, welche Daten für andere Zwecke, insbesondere spezifische Auswertungen, erforderlich sind. Gleichzeitig kann dabei nach unserer Empfehlung bei den Datensätzen die festgelegte Dauer der Speicherung überprüft werden. Die Richtwerte für die Speicherungsdauer, die in der Errichtungsanordnung teilweise sehr pauschal festgelegt sind, lassen sich bei der Evaluierung ohne nennenswerten Mehraufwand mit überprüfen. Eine auf Erfahrung und konkrete Feststellungen bei der Evaluierung basierende Korrektur der Fristen könnte die Folge sein. Die Errichtungsanordnung wäre gegebenenfalls anzupassen. Die zurzeit gültige Frist von pauschal fünf Jahren ist aus Datenschutzsicht nicht hinnehmbar. Die zuvor mit dem Innenministerium des Landes vereinbarte differenzierte Aussonderungsprüffrist wurde im Rahmen technischer Umstellungen zur Vorbereitung der Auswertung (siehe unten) absprachewidrig verlängert. Das Innenministerium hat zugesagt, nach erfolgter Evaluierung wieder differenzierte Fristen in @rtus einzuführen.

Soweit neue Verfahren auf der Basis der ursprünglich für den Zweck der polizeilichen Vorgangsbearbeitung erhobenen und gespeicherten Daten beabsichtigt sind, ist stets zu prüfen, ob die geplante weitere Verarbeitung von Daten aus dem Vorgangsbearbeitungssystem durch das Polizei-

recht gedeckt ist. Wenn dabei rechtliche Vorgaben programmtechnisch umgesetzt werden, ist dies aus unserer Sicht zu begrüßen. Das ULD ist weiterhin der Auffassung, dass eine Evaluierung von @rtus-VBS nach etwa sechs Jahren Betrieb dringend angezeigt ist. Die Polizei gewinnt dadurch Rechtssicherheit.

- @rtus-Datenqualität – mehr als nur ein leeres Wort

Eigentlich sollte Datenqualität spätestens seit dem Volkszählungsurteil des Bundesverfassungsgerichts etwas Normales und Selbstverständliches in der elektronischen Welt der Verarbeitung von personenbezogenen Daten sein. Es geht darum, sicherzustellen, dass möglichst alle gespeicherten Daten der Wirklichkeit entsprechen und korrekt gespeichert sind. Daten, deren Wahrheitsgehalt zweifelhaft ist, nutzen der Polizei wenig. Datenqualität ist bereits bei der Aufnahme von Daten relevant und macht bei nicht feststehenden Daten turnusmäße Überprüfungen nötig, wobei die Richtigkeit jedes einzelnen gespeicherten Datums verifiziert werden kann. Nur so kommt man zu verlässlichen Informationen. Bei dem Verfahren @rtus, das für vielfältige Anwendungsbereiche der Polizei zur Verfügung stehen soll, ist die Datenrichtigkeit unerlässlich. Mangelt es hieran, so können gerade in zeitkritischen Situationen, bei denen eine klärende Nachfrage bei der Polizeidienststelle unterbleibt, unberechtigte Eingriffsmaßnahmen bis hin zur Festnahme von Personen nicht ausgeschlossen werden. Das Nachsehen haben dann die von der Maßnahme betroffenen Bürger, aber auch die Polizei, die rechtswidrig und ineffektiv handelt.

Bei einem Verfahren wie @rtus, das aus einer Vielzahl von Komponenten besteht, die alle auf den Bestand des Vorgangsbearbeitungssystems zurückgreifen bzw. diesen teilweise für weitere Verarbeitungen ganz oder teilweise heranziehen, potenziert sich leicht die Gefahr von Fehlern. Das ULD hat daher der Polizei eindringlich geraten, der Datenqualität eine hohe Priorität einzuräumen, auch wenn dies in der Anfangsphase scheinbar zu Mehraufwand führt. Ein nicht verlässlicher Datenbestand verlangt von dem einzelnen Anwender ein hohes Maß an Fehlertoleranz. Zugleich führt er dazu, dass die Akzeptanz des Datenverarbeitungsverfahrens verloren geht.

- @rtus-Recherche – nur ein Hilfsmittel

Unter dem Begriff „@rtus-Recherche“ ist die Gesamtheit der Anwendungen zu verstehen, die eine Selektion personenbezogener Daten für spezielle Bereiche durch Dienststellen der Landespolizei im zentralen Verfahren @rtus ermöglichen. Die aus @rtus auswählbaren strukturierten Daten sollen die Ermittlungstätigkeit der Polizei unterstützen. Die Zugriffe sind entsprechend der Funktion des Bearbeiters begrenzt. Die Polizeien der Länder sind verpflichtet, zu bestimmten Deliktsbereichen Daten an das Bundeskriminalamt (BKA) zu übermitteln. Die Polizei des Landes Schleswig-Holstein hat hierzu den Meldedienst „PolDok“ so umgestellt, dass die Zentralstellen der Landespolizei auf die Datenbestände der Dienststellen zugreifen können. In der Übergangsphase wird @rtus-Recherche von den Zentralstellen der Polizei des Landes Schleswig-Holstein zur Erfüllung der Meldeverpflichtungen gegenüber dem Bundeskriminalamt und zur Unfallanalyse genutzt. Soweit sich das nun implementierte Verfahren „PolDok“ auf die gleichen Daten wie bisher beschränkt, stellt die technische Neuerung letztendlich ein Mehr an Datensicherheit dar. Das Innenministerium hat zugesagt, den Datenumfang erneut zu hinterfragen, um nicht gewollte Veränderungen auszuschließen.

Bei dem Meldedienst „PolDok“ strebt die Polizei des Landes längerfristig an, auf die – grundsätzlich fehleranfällige – doppelte Erfassung der meldepflichtigen Daten zu verzichten. Die Daten sollen künftig unmittelbar aus dem Ursprungsbestand von @rtus-VBS an das BKA abfließen. So gelangen sie schneller, ohne Medienbruch oder mögliche Eingabefehler an das BKA. Das ULD befürwortet grundsätzlich alle Prozesse, die ohne Weiterungen der bisherigen Datenübermittlung mehr Datensicherheit mit sich bringen und auch eine Entlastung in der täglichen Arbeit darstellen.

- @rtus-Auswertung

Zwei Anwendungen sind derzeit bei der Landespolizei in Schleswig-Holstein unter dem Begriff „@rtus-Auswertung“ konzipiert: „Lage“ und „Unfallauswertung“. Diese Anwendungen greifen auf den Datenbestand von @rtus-VBS zu, jedoch sind die Auswertungen so angelegt, dass auf die Verarbeitung und Nutzung von personenbezogenen Daten grundsätzlich verzichtet wird. Die polizeilichen Fragestellungen zielen auf nicht personenbeziehbare Ergebnisse ab.

Die „Lage“ soll einen Überblick über relevante Ereignisse in einer bestimmten Region in einem bestimmten Zeitraum gewähren, um methodische Ansätze zur Verhinderung und Bekämpfung von Straftaten usw. zu erhalten. Es geht nicht um konkrete Angaben zu bestimmten Personen, sondern um einen Überblick über ein bestimmtes

Lageereignis. Auch bei der „Unfallauswertung“ geht es um eine nicht fallbezogene Sachaussage. Diese Auswertung wird derzeit noch über @rtus-Recherche abgebildet.

Was ist zu tun?

Die vertrauensvolle Kooperation mit dem Innenministerium und der Polizei des Landes hat sich bewährt und sollte fortgesetzt werden. Defizite in der Umsetzung müssen abgebaut werden.

4.2.2 Sicherheitsüberprüfungen

Nach wie vor finden bei Großveranstaltungen ohne Rechtsgrundlage Sicherheitsüberprüfungen statt, so im Jahr 2011 im Vorfeld der Ministerpräsidentenkonferenz in SH.

Das ULD hat in der Vergangenheit immer wieder auf die datenschutzrechtlichen Bedenken im Zusammenhang mit Sicherheitsüberprüfungen bei Großveranstaltungen hingewiesen (28. TB, Tz. 4.2.9; 29. TB, Tz. 4.2.5; 30. TB, Tz. 4.2.3). Obwohl Großveranstaltungen wie z. B. die Fußball-WM 2006, die Frauen-Fußball-WM 2010 und 2011, die Veranstaltungen zum Tag der Deutschen Einheit, der Papstbesuch und die Ministerpräsidentenkonferenz 2011 aus polizeilicher Sicht die Überprüfung beteiligter Personen auf Sicherheitsrisiken erfordern, wurde hierfür bisher keine gesetzliche Ermächtigungsgrundlage geschaffen. Wegen der damit verbundenen Eingriffe in das Recht auf informationelle Selbstbestimmung ist diese jedoch notwendig. Das Innenministerium meint dagegen, eine Einwilligung der Betroffenen sei ausreichend.

Das ULD hat wiederholt darauf hingewiesen, dass eine Einwilligung als Rechtsgrundlage aus diversen Gründen für die Sicherheitsüberprüfung nicht genügt (siehe dazu die obigen Nachweise). Wesentlich ist u. a., dass in der Regel nicht von einer Freiwilligkeit der Einwilligung ausgegangen werden kann. Bedienstete bei den Veranstaltern und am Veranstaltungsort, z. B. Hotelangestellte oder Sicherheitsleute, können sich mit gutem Grund in ihrer beruflichen Existenz bedroht sehen, wenn sie sich einer Sicherheitsüberprüfung entziehen möchten.

Die Polizei hält an der Praxis weiterhin fest. Soweit fachlicher Bedarf besteht, müsste eine verhältnismäßige gesetzliche Grundlage einen Ausgleich der beiderseitig betroffenen Interessen herbeiführen. Nur so kann sowohl für die Polizei als auch für die betroffenen Bürgerinnen und Bürger die notwendige Rechtssicherheit und -klarheit geschaffen werden.

Was ist zu tun?

Der Gesetzgeber sollte die Regelungslücke schließen und die erforderliche gesetzliche Rechtsgrundlage schaffen.

4.2.3 Gemeinsames TKÜ-Zentrum Nord

Die Innenminister der norddeutschen Küstenländer haben beschlossen, Telekommunikationsüberwachung künftig in einem gemeinsamen Rechen- und Dienstleistungszentrum durchzuführen. Das Vorhaben wird von den Datenschutzbeauftragten begleitet.

Das von der Innenministerkonferenz der norddeutschen Küstenländer begonnene Projekt zur Realisierung des gemeinsamen Rechen- und Dienstleistungszentrums zur Telekommunikationsüberwachung (RDZ TKÜ) ist zweistufig angelegt. In einer ersten Stufe sollen alle Länder miteinander kooperieren. Dies bedeutet, dass bei Ausfall oder Überlastung der TKÜ-Anlage in Schleswig-Holstein die TKÜ-Anlage in Hamburg oder Niedersachsen die Überwachungsmaßnahme durchführen kann. Diese erste Phase hat bereits begonnen. Die Länder haben mit Hamburg und mit Niedersachsen Auftragsdatenverarbeitungsverträge geschlossen, welche die Rahmenbedingungen für eine tatsächliche Übernahme einer Telekommunikationsüberwachung regeln.

Die technische Infrastruktur für die Kooperation ist ebenfalls eingerichtet. In rechtlicher Hinsicht ist die Zusammenarbeit datenschutzkonform gelöst. Die Projektgruppe konnte allerdings nicht zu unserer Überzeugung darlegen, dass an den Standorten Hamburg und Niedersachsen die erforderliche und vertraglich zugesicherte Datensicherheit gewährleistet wird. Die Dokumentation der Anlagen war bei Vertragsschluss äußerst lückenhaft, sodass wir dem Landeskriminalamt Schleswig-Holstein geraten haben, keine Einzelaufträge für TKÜ-Maßnahmen an die Kooperationspartner zu erteilen, bis die Einhaltung des erforderlichen Sicherheitsniveaus durch Dokumentation der Sicherheitsmaßnahmen nachgewiesen werden kann.

In der zweiten Phase wird ein Konzept für eine vollständige Zentralisierung der TKÜ ab dem Jahr 2016 erstellt. Zu diesem Zeitpunkt soll es ein gemeinsames Zentrum für die fünf beteiligten Länder geben (Hamburg, Niedersachsen, Mecklenburg-Vorpommern, Bremen und Schleswig-Holstein), in dem alle TKÜ-Maßnahmen zentralisiert durchgeführt werden.

Die rechtliche Konstruktion dieses gemeinsamen Zentrums und der Verantwortlichkeit für die Datenverarbeitung steht noch nicht fest. Aus unserer Sicht sollte die Verteilung der Aufgaben und der Verantwortung durch einen Staatsvertrag geregelt werden, damit eine gesetzliche Grundlage für die Zentralisierung geschaffen wird.

Was ist zu tun?

Die Kooperation zwischen den Datenschutzbeauftragten und den Verantwortlichen im Projekt hat sich bewährt und sollte fortgesetzt werden. Für die Zentralisierung der TKÜ sollte ein Staatsvertrag geschlossen werden.

4.2.4 Sicherheitsbehörden in sozialen Netzwerken: Öffentlichkeitsfahndung

War der Beschuldigte zur Tatzeit im Urlaub? Wo arbeitet er? Lebt er allein oder in einer Beziehung? Wer sind seine Freunde? Was macht er in seiner Freizeit? Antworten auf diese Fragen findet man mitunter mit einem Klick – im Profil im sozialen Netzwerk. Kein Wunder, dass soziale Netzwerke als Informationsquelle für Sicherheitsbehörden immer wichtiger werden.

Über die Voraussetzungen und den Umfang zulässiger Recherchen in sozialen Netzwerken besteht in der Praxis große Unsicherheit. Dies liegt nicht zuletzt an einer ganzen Reihe von Abgrenzungen und Abwägungen, die im Einzelfall zu treffen sind. Am Anfang steht die Frage, ob die Polizei überhaupt in Grundrechte eingreift, wenn sie im Internet allgemein zugängliche veröffentlichte Daten erhebt. Dies ist der Fall, wenn die Informationen gezielt zusammengetragen und gespeichert sowie eventuell zusätzlich mit anderen Daten ergänzt werden, insbesondere aber, wenn sie bestimmten Personen zugeordnet werden. Bei gezielten polizeilichen Recherchen zur Strafverfolgung oder Gefahrenabwehr ist dies meist der Fall. Hierfür bedarf es einer Rechtsgrundlage. Werden allgemein zugängliche Daten aus sozialen Netzwerken erhoben, wiegt der Grundrechtseingriff in der Regel nicht besonders schwer. Deshalb können Recherchen im allgemein zugänglichen Bereich sozialer Netzwerke auf der Grundlage der Ermittlungsgeneralklauseln durchgeführt werden. Anders sind dagegen Recherchen in Bereichen zu beurteilen, die nicht jedermann im sozialen Netzwerk offenstehen und aus denen die Polizei nur Informationen erlangen kann, indem sie ein schutzwürdiges Vertrauen des Betroffenen in die Iden-

tität seiner Kommunikationspartner ausnutzt. Hierbei handelt es sich um einen weitaus gewichtigeren Grundrechtseingriff. Die Generalklauseln können nicht mehr angewendet werden, passende spezifische Rechtsgrundlagen gibt es mit Ausnahme der Vorschriften über den Einsatz verdeckter Ermittler nicht.

Schwierigkeiten bereitet die Abgrenzung, ob die Betroffenen in schutzwürdiger Weise darauf vertrauen, dass Informationen im sozialen Netzwerk nur einem abgegrenzten Personenkreis mit bekannter Identität zur Verfügung stehen, oder ob sie an jedermann oder zumindest an Empfänger mit beliebiger Identität gerichtet sind. Dies kann nur im Einzelfall bestimmt werden. Für die Entstehung eines schutzwürdigen Vertrauens spricht es, wenn die oder der Betroffene den Personenkreis, der die Informationen erhalten soll, durch bestimmte Maßnahmen eingegrenzt hat und die Einhaltung dieser Beschränkung durch geeignete Maßnahmen sichert.

Da die Recherchetätigkeit der Polizei vom Betreiber des sozialen Netzwerks registriert werden kann und bei einigen Betreibern auch gezielt ausgewertet wird, sollte die Polizei nicht offen, sondern unter einem Pseudonym recherchieren. Hierfür sollten keine privaten Accounts der Polizeibeamten, sondern polizeieigene, regelmäßig zu wechselnde Pseudonyme verwendet werden.

Ein ausführliches Gutachten zur Zulässigkeit polizeilicher Recherchen in sozialen Netzwerken haben wir auf unserer Webseite veröffentlicht unter:

https://www.datenschutzzentrum.de/polizei/20120312-polizeiliche-recherche-soziale-netzwerke.pdf

Bei der Polizei wird auch über eine aktive Nutzung von sozialen Netzwerken diskutiert, insbesondere zur Öffentlichkeitsfahndung. In Schleswig-Holstein werden Fahndungsaufrufe bislang nicht in sozialen Netzwerken veröffentlicht. Eine solche Veröffentlichung provoziert mehrere Probleme: Die Fahndungsdaten werden bei einem privaten Betreiber gespeichert, der faktisch über deren weitere Verwendung einschließlich der Löschung entscheidet. Bei Betreibern aus den Vereinigten Staaten unterliegen die Fahndungsdaten außerdem dem US-amerikanischen Recht und werden damit dem Zugriff durch US-amerikanische Behörden freigegeben. Dies kann zwar durch eine IFrame-Lösung, bei der die Fahndungsdaten auf einem polizeieigenen Rechner gespeichert sind und im sozialen Netzwerk lediglich angezeigt werden, unterbunden werden. Doch gerade die weltweit agierenden Betreiber wie Facebook registrieren das Verhalten der Nutzer auf ihren Seiten und werten dieses personenbezogen aus (Tz. 7.1.1). Diese Reichweitenanalyse kann auch durch eine IFrame-Lösung nicht abgestellt werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die Innen- und Justizminister der Länder auf diese Probleme hingewiesen. Eine Öffentlichkeitsfahndung ist allenfalls bei privaten Betreibern zulässig, die die Einhaltung des deutschen Rechts gewährleisten.

https://www.datenschutzzentrum.de/facebook/JBOES-2012-2013-Sonderdruck-Weichert.pdf

4.2.5 Umgang mit Auskunftssperren im Melderegister in Strafverfahren

Ein Polizeibeamter und seine Ehefrau wurden Opfer einer Straftat. Daraufhin wurde im Melderegister eine Auskunftssperre eingetragen. Als der Täter seinerseits, um sich zu wehren, einen Strafantrag gegen den Polizisten und dessen Ehefrau stellte und das Ehepaar Einsicht in die Strafakte nahm, wunderten sie sich. Darin war ihre Anschrift eingetragen, nicht aber die Herkunft dieser Information und der Umstand, dass im Melderegister eine Auskunftssperre bestand.

Die Polizei erhält eine Auskunft aus dem Melderegister auch, wenn eine Auskunftssperre eingetragen ist. Es bestehen keine Bedenken dagegen, dass die Strafverfolgungsbehörden für ihre Zwecke die Adresse trotz Auskunftssperre verwenden. Sie müssen dann aber besonders sorgfältig prüfen, ob sie Dritten im Wege der Akteneinsicht oder der Auskunftserteilung die im Melderegister gesperrte Adresse mitteilen. Beantragen Beschuldigte oder Verletzte einer Straftat sowie Dritte Akteneinsicht oder Auskunft aus der Akte, ist stets darauf zu achten, ob schutzwürdige Interessen entgegenstehen. Eine Auskunftssperre im Melderegister ist insofern ein wichtiges Indiz. Zuständig für Akteneinsicht und Auskünfte sind in der Regel die Staatsanwaltschaft oder das Gericht. Damit diese die Interessenabwägung umfänglich vornehmen können, müssen sie über alle relevanten Umstände informiert sein. Dazu gehört auch der Eintrag einer Auskunftssperre beim Melderegister. Die Polizei, die die Adresse ermittelt, muss daher das Bestehen einer Auskunftssperre in der Akte vermerken. Wird die Anschrift direkt beim Betroffenen erhoben, ist

eine zusätzliche Abfrage des Melderegisters nicht erforderlich. Der Betroffene kann in dieser Situation die Polizei selbst darauf hinweisen, dass seine Adresse nicht an Dritte weitergegeben werden soll. Kann die Anschrift nicht beim Betroffenen erhoben werden, ist diese durch Abfrage beim Melderegister zu erheben.

Was ist zu tun?

Wenn Anschriftendaten nicht beim Betroffenen erhoben werden können, sind sie durch Auskunft aus dem Melderegister zu ermitteln. Besteht dort eine Auskunftssperre, ist dies in der Akte zu vermerken und bei einer Auskunftserteilung zu beachten.

4.2.6 Was für die Polizei INPOL ist, ist für die Dienste NADIS – in neuem Gewand

Es scheint die Zeit der Erneuerungen zu sein. Nach der deutschen Polizei haben nun die Verfassungsschutzbehörden des Bundes und der Länder eine neue Datenverarbeitungstechnik erhalten.

Es bedurfte einiger Jahre, um das Ziel der grundlegenden Neugestaltung des Nachrichtendienstlichen Informationssystems (NADIS) von der Idee über ein Konzept hin zur technischen Realisierung und Inbetriebnahme zu erreichen. Zu Recht wurde am Anfang festgestellt, dass das bisherige Verbunddatenverarbeitungssystem NADIS technisch in die Jahre gekommen und gegen ein neues, zukunftssicheres Verfahren auszutauschen sei. Technisch begründete Zwänge eröffnen regelmäßig auch neue Möglichkeiten zur Verarbeitung von Daten. Moderne Datenbanktechnik gepaart mit intelligenten und leistungsfähigen Werkzeugen schafft mehr als Synergieeffekte, Leistungsfähigkeit und Benutzerfreundlichkeit. Veränderungen in der Struktur der Daten, in der Verknüpfbarkeit und in den Analysemöglichkeiten sind bei neuer Technik selbstverständlich, stellen jedoch Datenschützer und letztlich auch die Gesetzgeber vor neue Herausforderungen. Was technisch machbar ist, ist nicht immer rechtlich gewollt und zulässig. Wird etwa durch ein neues Verfahren die Option geschaffen, freitextliche Dokumente in Datenbanken zu erfassen und nach beliebigen Kriterien zu recherchieren, eröffnet sich eine Qualität der Datenverarbeitung, die von den Gesetzgebern bei Erlass der Verfassungsschutzgesetze auf Bundes- wie auf Landesebene nicht im Fokus stand. Die Datenschutzbeauftragten des Bundes und der Länder formulierten im November 2010 frühzeitig ihre Bedenken gegen die Erfassung und Verarbeitung von Freitextdokumenten in Datenbanken der Sicherheitsbehörden (33. TB, Tz. 4.2.7). Die Verfassungsschutzbehörden teilten diese jedoch nicht und genehmigten sich ein Mehr an Datenverarbeitung. Immerhin wurde zugesichert, Namen von Personen, die nicht für die Aufgabenwahrnehmung der Verfassungsschutzbehörde relevant sind, elektronisch zu „schwärzen".

Eine weitere Neuerung von NADIS besteht darin, dass das Bundesamt für Verfassungsschutz (BfV) den Landesbehörden für Verfassungsschutz anbietet, ihren Datenbestand beim BfV verarbeiten, also hosten zu lassen. Für die Länder fallen keine Kosten an, wenn der Umfang der Datenverarbeitung nicht den Rahmen der in Betrieb befindlichen Version von NADIS sprengt und somit keine Aufwände für Zusatzleistungen entstehen. Die Abschottung der einzelnen Datenbestände, Fragen der Benutzerverwaltung, der Datensicherheit, der Protokollierung usw. werden in einer ergänzenden Verwaltungsvereinbarung geregelt.

Offen ist die Frage, auf welcher Rechtsgrundlage das BfV personenbezogene Daten der Landesämter für Verfassungsschutz verarbeitet. Ein Auftragsdatenverarbeitungsverhältnis nach den Bestimmungen des Bundes- bzw. des jeweiligen Landesdatenschutzgesetzes (LDSG) soll jedenfalls nach dem Willen der Verfassungsschutzbehörden durch diese Form der technischen Kooperation nicht begründet werden. Die Alternative wird vom BfV in einer mit den einzelnen Landesbehörden für Verfassungsschutz abzuschließenden Verwaltungsvereinbarung gesehen, die auf die Regelungen über die ausschließliche Gesetzgebungskompetenz des Bundes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes (Art. 73 Nr. 10 b und c GG) in Verbindung mit der entsprechenden Norm im Bundesverfassungsschutzgesetz (§ 1 Abs. 3 BVerfSchG) Bezug nimmt. Das Bereitstellen einer technischen

Plattform durch das BfV stelle eine gegenseitige Unterstützung im Sinne der genannten Regelung des BVerfSchG dar. Die Regelungen über die Auftragsdatenverarbeitung im BDSG bzw. LDSG seien deshalb nicht anzuwenden. Das ULD teilt diese Rechtsauffassung des Bundesministeriums des Innern, der sich die Verfassungsschutzbehörden angeschlossen haben, nicht. Dies haben wir der Behörde für Verfassungsschutz in Schleswig-Holstein, die uns die entsprechenden Unterlagen zur Stellungnahme überlassen hat, ausführlich begründet mitgeteilt.

Wir haben angeregt, die Vereinbarung an die tatsächlichen Rahmenbedingungen für eine Übernahme des Hostings der Amtsdatei anzupassen und den Vertrag im Sinne einer Auftragsdatenverarbeitung nach § 17 LDSG SH zu gestalten.

Was ist zu tun?

Das ULD rät, von einer technischen Kooperation mit dem BfV bis zu einer rechtskonformen Lösung der rechtlichen Fragestellungen Abstand zu nehmen.

4.2.7 Entwicklungen im Verfassungsschutz

- Verlängerung der Antiterrorgesetze

Die Befugnisse, die den Nachrichtendiensten infolge der Anschläge am 11. September 2001 befristet eingeräumt wurden, um den Gefahren des internationalen Terrorismus besser begegnen zu können, sind im Berichtszeitraum größtenteils verlängert worden. Ob sie in der Vergangenheit etwas gebracht haben, blieb dabei weitgehend offen.

Mit dem Terrorismusbekämpfungsgesetz und dem Terrorismusbekämpfungsergänzungsgesetz (29. TB, Tz. 4.2.7) hat der Gesetzgeber die Auskunftsbefugnisse der Nachrichtendienste umfänglich erweitert. Möglich ist etwa die Abfrage von Telekommunikationsdaten, Flugdaten oder Kontodaten. Im Landesrecht sind diese Befugnisse weitgehend übernommen worden (31. TB, Tz. 4.2.6).

Der Gesetzgeber hat mit gutem Grund die Regelungen befristet und für den Fall ihrer Verlängerung eine Evaluierung angeordnet, um die Wirksamkeit der neuen Befugnisse im Verhältnis zu der Schwere der damit verbundenen Eingriffe in die Freiheit der Bürgerinnen und Bürger zu beurteilen.

Die Konferenz der Datenschutzbeauftragten hat Anforderungen an die Evaluierung formuliert: Jede Evaluation, auch die landesrechtlicher Vorschriften, muss auf der Grundlage valider, strukturierter Daten unter Mitwirkung aller relevanten Stellen in einem transparenten Verfahren durch ein unabhängiges Expertengremium erfolgen. Die Nachvollziehbarkeit und Überprüfbarkeit der Evaluierung ist zu gewährleisten. Der Evaluationsbericht muss dem Gesetzgeber eine umfassende Bewertungsgrundlage zur Optimierung bestehender Regelungen zur Verfügung stellen.

http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/79DSK_EvaluierungSicherheitsgesetze.pdf?__blob=publicationFile

http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/82DSK_AntiTerrorgesetze.html?nn=409240

Ob eine solche Evaluierung vorgenommen wurde und ob deren Ergebnisse nachvollziehbar die Notwendigkeit einer Verlängerung der Maßnahmen belegen, konnten wir leider nicht überprüfen. In der Gesetzesbegründung wird auf einen Evaluationsbericht verwiesen; dieser ist aber nicht öffentlich.

- Antiterrordatei und Rechtsextremismusdatei

Mit den Gesetzen zur Antiterrordatei und zur Verbesserung der Bekämpfung des Rechtsextremismus soll die Zusammenarbeit zwischen Diensten und Polizei verbessert werden. Der Datenschutz droht dabei auf der Strecke zu bleiben.

Mit dem Ende Dezember 2006 in Kraft getretenen Antiterrordateigesetz (ATDG) wurde für den Bereich der Terrorismusbekämpfung eine Verbund-

datei geschaffen, die von Polizeien und Nachrichtendiensten gemeinsam genutzt wird. In Anlehnung an das Antiterrordateigesetz trat Ende August 2012 das Gesetz zur Verbesserung der Bekämpfung des Rechtsextremismus (RED-G) in Kraft. Das RED-G wurde infolge der Straftaten des Nationalsozialistischen Untergrundes (NSU) und der sich anschließenden polizeilichen Ermittlungstätigkeiten errichtet. Ziel beider Gesetze ist eine verbesserte Bekämpfung des Terrorismus bzw. des Rechtsextremismus insbesondere durch einen erweiterten Informationsfluss zwischen Polizeien und Nachrichtendiensten. Gegen beide Gesetze bestehen verfassungsrechtliche Bedenken.

Beide Gesetze – also auch das im Laufe der Gesetzesabstimmung wiederholt nachgebesserte RED-G – zeichnen sich durch unbestimmte Rechtsbegriffe aus. Diese führen nicht zu Rechtssicherheit und begründen die Gefahr einer unzulässigen Erweiterung des ohnehin schon sehr weiten Anwendungsbereichs dieser Gesetze. So ist z. B. in beiden Gesetzen das Speichern der Daten von Kontaktpersonen vorgesehen. Bei der Einstufung als Kontaktperson gibt es nur vage Vorgaben und keine klar definierten Parameter. Für den einzelnen Bürger besteht die Gefahr, dass er – nur durch einen unglücklichen Zufall – als Kontaktperson eingestuft, einer Personengruppe zugeordnet und deshalb diskreditiert wird. Dass diese Bedenken nicht nur theoretischer Natur sind, zeigt die Praxis der Antiterrordatei. Für die mündliche Verhandlung des Bundesverfassungsgerichts (BVerfG) im November 2012 hat das ULD die Erfahrungen der Datenschutzbeauftragten aus den Kontrollen der Antiterrordatei zusammengetragen. Dabei ergab sich, dass keine umfassende Kontrolle der Zugriffe auf die in der Datei gespeicherten Daten möglich war. In einigen Fällen wurden die Speicherfristen bei der Erfassung der Antiterrordatei nicht korrekt festgesetzt, teilweise wurden die Betroffenen in eine falsche Personengruppe eingeordnet.

Wegen der datenschutzrechtlichen und verfassungsrechtlichen Bedenken wurde gegen das ATDG eine Verfassungsbeschwerde erhoben. Die Datenschutzbeauftragten des Bundes und der Länder haben zu dem Gesetz Stellung genommen. Themen der mündlichen Verhandlung vor dem BVerfG waren die hinreichende Bestimmtheit der erfassten Personengruppen, die Garantie effektiven Rechtsschutzes und die Möglichkeiten bzw. Grenzen der bestehenden Kontrollrechte der Datenschutzbeauftragten. Die Entscheidung des Gerichts steht noch aus.

Was ist zu tun?

Die aktuelle Diskussion über eine Neustrukturierung des Verfassungsschutzes sollte von einer bisher fehlenden umfassenden unabhängigen Evaluierung aller bislang ergriffenen Maßnahmen einschließlich ihres Zusammenwirkens ausgehen.

4.2.8 Neuorganisation der behördlichen Datenschutzbeauftragten der Polizei

Die bisherige dezentrale Aufgabenwahrnehmung der behördlichen Datenschutzbeauftragten bei den einzelnen Polizeidirektionen, beim Landeskriminalamt und beim Landespolizeiamt wurde aufgegeben. Nun steht eine zentrale Organisationseinheit beim Landespolizeiamt bereit, um die Aufgaben der behördlichen Datenschutzbeauftragten wahrzunehmen.

Die wesentliche Neuerung dieser Organisationsentscheidung des Innenministeriums besteht in einer räumlichen Zusammenführung der bisher bei den einzelnen Behörden tätigen behördlichen Datenschutzbeauftragten. Am Aufgabenzuschnitt, insbesondere an der vom ULD geforderten „Vor-Ort-Betreuung“, soll sich nichts ändern. Der durch diese Zentralisierung erwartete Vorteil besteht in einer besseren Kommunikation und einem besser aufeinander abgestimmten Vorgehen. Die Zuweisung von bestimmten Themenbereichen auf die einzelnen behördlichen Datenschutzbeauftragten kann auch die Qualität der Tätigkeit erhöhen.

Wichtig ist, dass der unmittelbare Kontakt zu den jeweiligen Ämtern und Polizeidirektionen durch die Umorganisation nicht leidet, denn die Gewährleistung von Praxisnähe ist zentral für die Realisierung eines effektiven Datenschutzes bei den

Dienststellen der Polizei. Das ULD hatte zunächst den Weg zur Zentralisierung kritisch gesehen. Erste positive Auswirkungen in der unmittelbaren Zusammenarbeit zeigen, dass die Organisationsentscheidung richtig war.

Was ist zu tun?

Bei all den positiven Effekten der Zusammenfassung der behördlichen Datenschutzbeauftragten ist darauf zu achten, dass die Aufgabenwahrung der behördlichen Datenschutzbeauftragten vor Ort uneingeschränkten Vorrang hat.

4.2.9 Die Polizei als Informant des Arbeitgebers

Wegen Kostenerstattung in einem Ordnungswidrigkeitenverfahren hatte ein Petent das Landespolizeiamt kontaktiert. Die Antwort per E-Mail erhielt nicht nur er selbst, sondern – nachrichtlich (cc) – auch sein Arbeitgeber. Für die Datenübermittlung an die Poststelle des Arbeitgebers gab es weder einen sachlichen Grund noch eine rechtliche Grundlage, weshalb wir diese Datenübermittlung beanstanden mussten.

Was ist zu tun?

Die Behörden sollten ihre Bediensteten in geeigneter Form darauf hinweisen, dass Korrespondenz grundsätzlich nur mit dem Betroffenen selbst zu erfolgen hat.

4.3 Justizverwaltung

4.3.1 Der Staatstrojaner ohne rechtliche Grundlage

Der Einsatz von Spähsoftware auf Computern und anderen informationstechnischen Systemen kann nicht mit der klassischen Telekommunikationsüberwachung gleichgesetzt werden, auch wenn mit beiden Mitteln nur Telefongespräche, E-Mails und ähnliche Kommunikationen überwacht werden.

Im Berichtszeitraum wurde bekannt, dass Strafverfolgungsbehörden in zahlreichen Fällen die Software eines privaten Herstellers eingesetzt haben, um auf den Rechnern von Beschuldigten Telefongespräche und andere Telekommunikation zu überwachen. Für derartige Maßnahmen gibt es im Strafverfahren keine gesetzliche Grundlage. Insbesondere können sie nicht auf die Befugnis zur herkömmlichen Telekommunikationsüberwachung gestützt werden. Der entscheidende Unterschied liegt im Aufbringen eines Überwachungssystems auf dem Rechner des Betroffenen.

Dadurch kann die Strafverfolgungsbehörde im Prinzip Zugriff auf alle dort gespeicherten Inhalte erlangen. Ja, sie kann selbst Aktionen auf dem infiltrierten System ausführen, es gewissermaßen fernsteuern. Beim Aufbringen der Software wird regelmäßig eine Hintertür auf dem Rechner geöffnet. Diese benötigt die Strafverfolgungsbehörde, um z. B. Updates für die installierte Software aufzuspielen. Grundsätzlich kann diese Hintertür auch von Dritten genutzt werden. Damit entsteht eine Vielzahl von Gefahren für die Integrität des infiltrierten Systems und die Vertraulichkeit der

damit verarbeiteten Daten. Diese Gefahren können zwar durch spezifische Maßnahmen der Strafverfolgungsbehörden minimiert werden. So kann die Software so programmiert werden, dass sie nur Daten ausleitet, die Inhalt eines laufenden Telekommunikationsvorgangs sind, und alle übrigen Daten gar nicht erst zur Kenntnis nimmt. Die Hintertür kann gegen die Nutzung durch Dritte gesichert werden.

Quellen-TKÜ

Telefongespräche, E-Mails, Surfen – sämtliche Kommunikation über einen Rechner kann vom Nutzer verschlüsselt werden. Dies hat zur Folge, dass sie von Sicherheitsbehörden mit der herkömmlichen Methode, d. h. durch Ausleiten der Kommunikation, nicht mehr überwacht werden kann. Die Sicherheitsbehörden haben in der Regel keine Möglichkeit, die Nachrichten zu entschlüsseln. Daher greifen sie zur Überwachung der Telekommunikation an der Quelle. Ein Programm wird auf dem Rechner der zu überwachenden Person installiert, das die Telekommunikationsinhalte an die Sicherheitsbehörden ausleitet, noch bevor sie verschlüsselt werden.

Doch alle Sicherheitsvorkehrungen können nicht darüber hinwegtäuschen, dass ein vom Betroffenen genutztes System durch Strafverfolgungsbehörden infiltriert wird. Diese erlangen damit die faktische Herrschaft über das System und können in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme eingreifen. Die Sicherheitsmaßnahmen sind letztlich Selbstbeschränkungen der Strafverfolgungsbehörden, die sie selbst jederzeit wieder aufheben können. Über die grundsätzliche Zulässigkeit der Infiltration von informationstechnischen Systemen sowie ihrer Voraussetzungen und Grenzen kann nicht die Exekutive selbst entscheiden, es bedarf einer Entscheidung des Gesetzgebers.

Dementsprechend gibt es für die Quellen-Telekommunikationsüberwachung zum Zweck der Gefahrenabwehr im Bundesrecht und in einigen Landesgesetzen ausdrückliche Befugnisnormen. In der Strafprozessordnung hingegen fehlt eine Regelung. Die Konferenz der Datenschutzbeauftragten hat hierauf bereits Anfang des Jahres 2011 hingewiesen.

http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/81DSK_Quellen_TKUEV.html?nn=409240

Was ist zu tun?

Für schleswig-holsteinische Behörden gibt es keine gesetzliche Befugnis zur Durchführung von Quellen-Telekommunikationsüberwachungen, weder zur Gefahrenabwehr noch zur Strafverfolgung. Das Mittel darf daher in Schleswig-Holstein nicht eingesetzt werden.

4.3.2 Anordnung von Blutproben – Richtervorbehalt stärken statt abschaffen

Blutentnahmen zur Alkoholkontrolle bei Straftaten oder Ordnungswidrigkeiten im Straßenverkehr müssen grundsätzlich durch den Richter angeordnet werden. Eine Anordnung durch Staatsanwaltschaft und Polizei ist nur bei Gefahr im Verzug möglich. Da die Gerichte hierbei strenge Maßstäbe anlegen, werden immer wieder Zweifel an der Erforderlichkeit des Richtervorbehalts für Blutproben laut.

Bei Alkoholkontrollen im Straßenverkehr muss zügig gehandelt werden, da sich der Blutalkoholgehalt schnell abbaut und bereits ein Promille für die Rechtsfolgen entscheidend sein kann. Dennoch fordern das Bundesverfassungsgericht und ihm folgend die ordentlichen Gerichte, dass die Polizeibeamten vor Ort stets versuchen müssen, die Genehmigung des Gerichts für diese Maßnahme einzuholen, und nicht pauschal davon

ausgehen dürfen, dass für die Entscheidung des Gerichts keine ausreichende Zeit verbleibe oder das Gericht nicht erreicht werden könne. Als Reaktion auf diese Rechtsprechung hat der Bundesrat im Jahr 2010 einen Gesetzentwurf zur Abschaffung des Richtervorbehalts für Blutabnahmen im Straßenverkehr in den Bundestag eingebracht. Damit sollen die Verfahren beschleunigt und Rechtsunsicherheiten beseitigt werden.

Aus unserer Sicht ist das die falsche Antwort auf die Problemlage. Der Richtervorbehalt hat eine wichtige rechtsstaatliche Funktion der unabhängigen vorbeugenden Kontrolle von Exekutivmaßnahmen. Er darf nicht leichtfertig aufgegeben werden. Richtig wäre es, den Richtervorbehalt zu stärken, indem ein 24-stündiger Bereitschaftsdienst eingerichtet wird. Die Entwicklung in Schleswig-Holstein – es wurde ein Bereitschaftsdienst bis 21 Uhr eingerichtet – geht in die richtige Richtung, reicht aber noch nicht aus. Wir haben dem Innen- und Rechtsausschuss des Landtags unsere Bedenken gegen die Abschaffung des Richtervorbehalts für Blutproben im Straßenverkehr deutlich gemacht. Zudem haben wir an das Justizministerium und die Gerichte appelliert, einen 24-stündigen richterlichen Bereitschaftsdienst einzurichten und damit Forderungen nach einem Abbau des Richtervorbehalts die Grundlage zu entziehen.

Was ist zu tun?

Anstatt über eine Abschaffung des Richtervorbehalts und damit über eine Verkürzung des Grundrechtsschutzes zu diskutieren, sollten die Voraussetzungen für gerichtliche Entscheidungen rund um die Uhr geschaffen werden.

4.3.3 MESTA – erste Fortschritte

Seit einigen Jahren berät das ULD den Generalstaatsanwalt im Hinblick auf eine datenschutzgerechte Gestaltung des staatsanwaltschaftlichen Informationssystems MESTA. Inzwischen konnten Verbesserungen erreicht werden, es bleibt jedoch weiterhin einiges zu tun.

Seit Einführung des Verfahrens „Mehrländer-Staatsanwaltschaft-Automation“ (MESTA) in den 90er-Jahren hatte das ULD wiederholt über Mängel berichtet (19. TB, Tz. 4.4.2; 20. TB, Tz. 4.4.1; 21. TB, Tz. 4.4.3; 25. TB, Tz. 4.3.2; 29. TB, Tz. 4.3.2). Das ULD hat in den vergangenen Jahren MESTA im Auftrag des Generalstaatsanwalts eingehend untersucht, insbesondere die einzelnen Datenkategorien, die Zwecke und die Dauer der Speicherung, die Zugriffsberechtigungen, die Schnittstellen zum automatisierten Datenaustausch mit Dritten und die Protokollierung der einzelnen Datenverarbeitungen und der Administratorzugriffe. Hinsichtlich einzelner Datenfelder sowie Zugriffsberechtigungen konnten wir Verbesserungen erreichen. Künftig sollen die Kontaktdaten der Beschuldigten (Telefonnummer, Faxnummer, E-Mail-Adresse usw.) nach Beendigung des Verfahrens gelöscht werden; Besucher von Gefangenen sollen nicht mehr eingetragen werden können; andere Rollen als die der Beschuldigten sollen nicht landesweit recherchierbar sein. In Zusammenarbeit mit uns hat der Generalstaatsanwalt das Verfahren der Auskunftserteilung an Betroffene aus MESTA erheblich verbessert. Bislang erhält der Betroffene eine Auskunft lediglich über einen geringen Teil der in MESTA gespeicherten Daten. Durch eine speziell für die Beantwortung von Auskunftsersuchen gestaltete Abfrage wird der Umfang der Daten, über die im Standardverfahren Auskunft erteilt wird, erheblich erweitert. Der Generalstaatsanwalt hat in Abstimmung mit uns eine Auswahl von relevanten Daten getroffen. Da das System MESTA mehrere hundert Datenfelder enthält (u. a. zahlreiche interne Kennzeichnungen und Geschäftsgangvermerke), wäre eine vollständige Auskunft für den Betroffenen schwer lesbar. Der Betroffene wird darauf hingewiesen, dass neben den mitgeteilten Daten noch weitere Angaben gespeichert sind und er auf Wunsch auch hierüber Auskunft erhalten kann.

Andere Punkte sind noch nicht gelöst. Dies gilt vor allem für die weiterhin unzureichende Protokollierung. Das ULD fordert gemeinsam mit den anderen betroffenen Landesdatenschutzbeauftragten seit der Einführung von MESTA, dass jeder

Systemzugriff protokolliert wird. Staatsanwaltschaften argumentierten dagegen, bei einer Vollprotokollierung aller Zugriffe seien Leistungseinbußen zu befürchten. Nach dem heutigen Stand der Technik hat dieses Argument keine Grundlage mehr. Wir verlangen, dass alle Zugriffe durch Administratoren, mit denen das System verändert wird, z. B. Änderungen an Benutzerrechten, zwingend zu protokollieren sind, ebenso wie die Zugriffe der Benutzer. Zurzeit werden nur das Einfügen, das Ändern und das Löschen von Daten protokolliert. Angesichts der teilweise eingestellten landesweiten Recherchemöglichkeiten halten wir auch eine Protokollierung aller Abrufe für erforderlich. Um den Zweck der Protokollierung zu erfüllen, müssen die Protokolldaten routinemäßig ausgewertet und kontrolliert werden. Der Generalstaatsanwalt zeigte sich gegenüber diesen Vorschlägen aufgeschlossen und prüft gemeinsam mit Dataport deren Umsetzbarkeit.

Was ist zu tun?

In Fortsetzung der konstruktiven Zusammenarbeit zwischen dem ULD und dem Generalstaatsanwalt sind Lösungen für mehr Datenschutz und Datensicherheit bei MESTA, insbesondere bei der Protokollierung, zügig umzusetzen.

4.3.4 Sicherstellung von Datenträgern im Strafverfahren

Zwecks Sicherstellung von Datenträgern als Beweismittel im Strafverfahren werden diese in der Regel vollständig von der Polizei kopiert. Für das Strafverfahren sind aber oft nicht alle kopierten Daten erforderlich. Eine Löschung solcher Daten ist im Nachhinein allerdings schwierig.

Die Beschlagnahme, Auswertung und Verwendung von Datenträgern als Beweismittel im Strafverfahren erfolgen in der Regel in der Weise, dass ein Datenträger nach Sicherstellung oder Beschlagnahme zunächst von der Polizei vollständig gesichert wird; es erfolgt eine Spiegelung, es wird also eine vollständige Kopie des Datenträgers erstellt. Die inhaltliche Auswertung der sichergestellten oder beschlagnahmten Daten erfolgt auf der Grundlage der Kopie. Um die Übereinstimmung der Kopie mit dem Originaldatenträger und die Unversehrtheit und Manipulationsfreiheit der Kopie nachzuweisen, wird ein Hashwert über das gesamte Abbild der Kopie erstellt; die Gesamtheit der kopierten Daten wird also mit einer Prüfsumme gekennzeichnet. Eine Änderung an dem kopierten Datensatz führt zu einer Änderung dieses Hashwertes. Nur durch einen unveränderten Datenbestand mit identischem Hashwert können die Strafverfolgungsbehörden nachweisen, dass sie an dem kopierten Datensatz keine Veränderungen vorgenommen haben.

Dies führt bei einigen der von der Polizei eingesetzten Forensiksoftwareprodukten zu technischen Schwierigkeiten oder zur Unmöglichkeit, Daten nachträglich zu löschen. Das nachträgliche Löschen einzelner Daten aus einem Abbild heraus führt zu einem für die Software inkonsistenten Datenbestand.

Dieser Sachverhalt ist datenschutzrechtlich problematisch. Zwar wird die Integrität der sichergestellten Daten geschützt, was aus Gründen der Datensicherheit geboten ist. Doch führt das Verfahren auch dazu, dass in vielen Fällen weitaus mehr Daten gespeichert bleiben, als für das Strafverfahren erforderlich ist. Darunter können sich die Persönlichkeitsrechte des Betroffenen besonders berührende Daten befinden, etwa private Fotos, Tagebuchaufzeichnungen oder der E-Mail-Verkehr mit Freunden.

Eine Lösung dieses Dilemmas, die sowohl den Grundsatz der Erforderlichkeit der Datenverarbeitung als auch das Schutzziel der Integrität der Daten hinreichend berücksichtigt, kann entsprechend den Anforderungen des Bundesverfassungsgerichts (BVerfGE 113, 29) darin bestehen, dass noch vor der Spiegelung der Daten der Originaldatenträger ausgewertet wird und nur diejenigen Daten gesichert werden, die bei dieser ersten Auswertung für das Strafverfahren als relevant erkannt werden. Diese Daten können mit unterschiedlichen Hashwerten versehen werden. Daten, die nur möglicherweise als beweisrelevant eingestuft werden, können mit jeweils einem

Hashwert über jedes einzelne Verzeichnis oder sogar jede einzelne Datei belegt werden, sodass eine nachträgliche Löschung eines Verzeichnisses oder einer Datei keine Auswirkungen auf den Beweiswert der übrigen gesicherten Daten hat.

Was ist zu tun?

Bei der Sicherstellung oder Beschlagnahme von Datenträgern sollte stufenweise vorgegangen werden. In einer Vorauswertung sollten die für das Verfahren möglicherweise relevanten Verzeichnisse oder Dokumente ausgewählt und nur diese kopiert werden.

4.3.5 Therapieunterbringungsvollzugsgesetz

Der Landtag hat kurz vor Ende der 17. Wahlperiode einen von den Regierungsfraktionen eingebrachten Entwurf für ein Therapieunterbringungsvollzugsgesetz beschlossen. Das Gesetz regelt den Vollzug der Unterbringung psychisch gestörter Gewalttäter in einer geschlossenen Einrichtung.

Das ULD war am Gesetzgebungsverfahren nicht beteiligt worden und erfuhr davon erst durch die Veröffentlichung des Gesetzentwurfs im Landtag. Der Entwurf enthielt eine Reihe von hinterfragungsbedürftigen Regelungen zur Verarbeitung sensibler Daten der Untergebrachten. Die Regelung zum Akteneinsichtsrecht des Betroffenen, die leider unverändert beschlossen wurde, setzt voraus, dass eine Auskunft für die Wahrnehmung der rechtlichen Interessen des Betroffenen nicht ausreicht. Diese Einschränkung des Informationsanspruchs des Betroffenen über die zu seiner Person gespeicherten Daten ist verfassungsrechtlich nicht akzeptabel. Die Akteneinsicht dient wie die Auskunft der Verwirklichung des Rechts auf informationelle Selbstbestimmung als Ausgestaltung des Persönlichkeitsrechts; sie soll dem Betroffenen ermöglichen zu erfahren, welche Informationen über ihn vorhanden sind. Die Nutzung der gespeicherten Informationen zur Verfolgung von Rechtsansprüchen ist allenfalls eine Folge des Auskunfts- und Akteneinsichtsanspruchs, nicht aber dessen eigentlicher Zweck. Warum der Gesetzgeber hier das Akteneinsichtsrecht vom Regelfall – wie es in anderen Gesetzen üblich ist – zum begründungsbedürftigen Ausnahmefall gemacht hat, erschließt sich nicht.

Was ist zu tun?

Das vom Landtag beschlossene Therapieunterbringungsvollzugsgesetz weist einige datenschutzrechtliche Mängel auf. Diese wurden im Gesetzgebungsverfahren entgegen der vom ULD geäußerten Bedenken nicht behoben. Vor dem Erlass von Regelungen zur Verarbeitung personenbezogener Daten, gerade in besonders sensiblen Bereichen, sollte das ULD angehört werden. Das neue Gesetz ist so bald wie möglich zu überarbeiten.

4.3.6 Sicherungsverwahrungsvollzugsgesetz

Positives Gegenbeispiel zum Therapieunterbringungsvollzugsgesetz ist das noch laufende Gesetzgebungsverfahren für ein Sicherungsverwahrungsvollzugsgesetz. Der Gesetzentwurf ist in datenschutzrechtlicher Hinsicht ausgewogen; das ULD wurde frühzeitig beteiligt.

Die Unterbringung in der Sicherungsverwahrung muss nach einem Urteil des Bundesverfassungsgerichts bis Ende Mai 2013 neu geregelt werden. Zum Entwurf des Ministeriums für Justiz, Kultur und Europa wurde das ULD um Stellungnahme gebeten. Der Entwurf orientiert sich an einem von mehreren Bundesländern erstellten Musterentwurf sowie an bereits bestehenden landesrechtlichen Regelungen zum Vollzug der Jugendstrafe und der Untersuchungshaft. Er sieht maßvolle Eingriffe in das Recht auf informationelle Selbstbestimmung der Untergebrachten vor und beschränkt sich weitgehend auf diejenigen Maßnahmen, die zum Vollzug der Unterbringung sowie zur Wahrung der Sicherheit in der Einrichtung unbedingt erforderlich sind. Videoüberwachung wird nicht nur für die Zimmer der Untergebrachten, sondern auch für Gemeinschaftsräume ausgeschlossen. Die Pflicht der tätigen Ärzte zur Offenbarung von medizinischen Daten an die Leitung der Einrichtung wird auf Fälle von Gewicht beschränkt. Die Akteneinsicht ist der Auskunft an den Betroffenen gleichgestellt. In einigen Punkten sind aus unserer Sicht noch Verbesserungen und Klarstellungen nötig. Die Überwachung von Besuchen und Telefongesprächen sollte z. B. nur durch die Leitung der Einrichtung angeordnet werden dürfen. Das Gleiche gilt für die verdeckte Videoüberwachung, bei der außerdem eine umfassende Benachrichtigungspflicht vorgesehen werden muss.

Was ist zu tun?

Der Gesetzentwurf sollte in den vom ULD genannten Punkten nachgebessert werden.

4.3.7 Einführung eines bundesweiten Vollstreckungsportals

Seit dem 1. Januar 2013 sind die bislang bei den Amtsgerichten geführten Schuldnerverzeichnisse über ein zentrales Schuldnerportal bundesweit über das Internet abrufbar.

Mit dem Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung vom Juli 2009 wurden zum Jahresbeginn 2013 wesentliche Neuerungen eingeführt. Jedes Land erhält ab diesem Zeitpunkt ein zentrales Vollstreckungsgericht. In Schleswig-Holstein hat das Amtsgericht Schleswig diese Aufgabe übernommen, wo das landesweite zentrale Schuldnerverzeichnis geführt wird. Über ein gemeinsames Portal sind alle Schuldnerverzeichnisse bundesweit über das Internet abrufbar. Die Einzelheiten zur Umsetzung dieses Vorhabens wurden in einer Verordnung festgelegt. Bei unserer Stellungnahme zu deren Entwurf haben wir besonderes Augenmerk auf die Regelungen zur Identifizierung der Schuldner gelegt. Um den Betroffenen eindeutig zu bestimmen, müssen unseres Erachtens ausreichend viele Suchkriterien angegeben werden. Nicht alle Menschen sind im Schuldnerverzeichnis eingetragen. Mit einem Treffer bei einer Suche nach dem Namen und Vornamen kann nicht mit Sicherheit festgestellt werden, ob es sich bei der eingetragenen Person tatsächlich um die gesuchte Person handelt. Der anfragenden Person müssen also zur Feststellung der Identität des Treffers zusätzlich zum Namen weitere Merkmale wie Anschrift und Geburtsdatum bekannt sein. Der Entwurf für die Verordnung sah dagegen vor, dass bereits nach Eingabe des Namens eine Liste mit allen Daten im Schuldnerverzeichnis des jeweiligen Vollstreckungsgerichts angezeigt wird. Dies ist unzulässig, weil Daten zu Personen übermittelt werden, für deren Kenntnis kein berechtigtes Interesse besteht. Der Entwurf ist in diesem Punkt nachgebessert worden, nachdem die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine eindeutige Trefferanzeige gefordert hatte.

http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/070212_EntschliessungSchuldnerverzeichnis.html?nn=409240

Ein weiterer Kritikpunkt am Verordnungsentwurf war die vorgesehene Möglichkeit, sich unter Angabe von Kreditkartendaten beim Vollstreckungsportal als Nutzer zu registrieren. Wir forderten, die Registrierung allein über den elektronischen Identitätsnachweis des neuen Personalausweises vorzusehen. Die Identifizierung über von privaten Anbietern bereitgestellte Verfahren ist entbehrlich

und gewährleistet nicht das Sicherheitsniveau wie bei der gesetzlich vorgesehenen Identifizierung mit dem neuen Personalausweis.

Erfreulich ist, dass die Suchanfragen im Vollstreckungsportal vollständig protokolliert werden sollen. Damit wird die Revisionsfähigkeit der Datenverarbeitung hergestellt, was für Kontrollzwecke wie auch für Auskunftsersuchen der betroffenen Schuldner wichtig ist. Die im Entwurf vorgesehene Aufbewahrungsdauer der Protokolldaten ist mit sechs Monaten zu kurz; wir haben eine Aufbewahrung für die gesamte Dauer der Speicherung der Grunddaten gefordert.

Was ist zu tun?

Schuldnerdaten sind sensible Informationen. Es muss daher ein hohes Maß an Sicherheit gewährleistet werden, schon bei der Suchanfrage. Diese ist so zu gestalten, dass nur eindeutige Treffer hervorgebracht werden.

4.3.8 Dokumentation von Grundbucheinsicht

Die unterbliebene Dokumentation einer Grundbuchauskunft führte in einem Fall dazu, dass die Grundstückseigentümer nicht erfuhren, ob und welche Informationen ihr Nachbar aus dem Grundbuch über sie erhalten hatte. Sie konnten gerichtlich nicht gegen die Grundbuchauskunft vorgehen, da sie nichts beweisen konnten.

Der Nachbar eines Ehepaars hatte über dieses offenbar Auskünfte aus dem Grundbuch erhalten. Die Eheleute wollten nun wissen, welche Auskunft ihr Nachbar erhalten hatte und ob diese rechtmäßig war. Auf die Anfrage beim Grundbuchamt hin erhielten sie die Mitteilung, dass im Nachhinein nicht mehr zu ermitteln sei, welche Auskünfte der Nachbar erhalten habe. Den Eigentümern stehe die Möglichkeit der Beschwerde zu. Dafür wäre von ihnen aber genau zu bezeichnen, welche Angaben der Nachbar vom Grundbuchamt erhalten habe.

Auf unsere Nachfrage hin erhielten wir vom Amtsgericht eine ähnliche Auskunft. Alle Einsichtnahmen von Dritten in Grundbücher würden auf einem Formular dokumentiert, mündlich erteilte Auskünfte durch Mitarbeiter des Grundbuchamts dagegen nicht. Da der Nachbar offenbar nur eine mündliche Auskunft erhalten und nicht selbst Grundbucheinsicht genommen habe, sei keine Dokumentation darüber vorhanden. Diese Praxis widerspricht dem Datenschutzrecht. Datenverarbeitende Stellen müssen gewährleisten, dass der Zeitpunkt und Umfang der Datenverarbeitung festgestellt werden kann. Die Betroffenen haben einen Anspruch auf Auskunft darüber, an welche Dritte welche Daten übermittelt wurden. Demgemäß schreibt ein Erlass des Justizministeriums vor, dass alle Einsichtnahmen in das Grundbuch oder in Grundakten unter Angabe des Tages der Einsicht und des Namens sowie der Anschrift des Einsichtnehmenden dokumentiert werden müssen. Dies gilt auch, wenn Mitarbeiter des Grundbuchamts Einsicht nehmen, um Dritten Auskünfte zu erteilen.

Was ist zu tun?

Die Einsichtnahme in das Grundbuch und in Grundakten ist zu dokumentieren, unabhängig davon, ob sie unmittelbar durch Dritte erfolgt oder ob Mitarbeiter des Grundbuchamts Einsicht nehmen, um Dritten Auskünfte zu erteilen.

4.3.9 Gerichtsvollzieher-Durchsuchungen in Abwesenheit des Schuldners

Darf ein Mitbewohner einem Gerichtsvollzieher erlauben, die Wohnräume des Schuldners zu durchsuchen? Wir und das nun geltende Recht sagen: Nein.

Für eine Zwangsvollstreckung suchte ein Gerichtsvollzieher die Wohnung des Schuldners auf. Er traf dort nur den Vater des Schuldners an, der mit diesem in einer gemeinsamen Wohnung lebte. Der Gerichtsvollzieher eröffnete dem Vater den Vollstreckungsauftrag und fragte ihn, ob er mit einer Durchsuchung der Wohnung einverstanden sei. Nach einem Telefonat mit seinem Sohn verneinte der Vater sein Einverständnis und der Gerichtsvollzieher musste die Vollstreckung vorläufig einstellen. Der Sohn bat das ULD um Überprüfung, ob der Gerichtsvollzieher die Informationen über den Vollstreckungsauftrag dem Vater mitteilen durfte.

Die damals geltende Geschäftsanweisung für Gerichtsvollzieher erlaubte dem Gerichtsvollzieher die Durchsuchung der Wohnung eines Schuldners, wenn ein Gericht dies angeordnet oder der Schuldner eingewilligt hat, wobei die Einwilligung in die Wohnungsdurchsuchung bei Abwesenheit des Schuldners auch von einem Hausgenossen erteilt werden konnte. Demgemäß war das Vorgehen des Gerichtsvollziehers nicht zu beanstanden.

Wir meinen aber, dass die Regelung in der Geschäftsanweisung nicht mit dem Grundrecht auf Unverletzlichkeit der Wohnung vereinbar ist. Dieses persönliche Recht soll die freie Entfaltung des Betroffenen in einem persönlichen Rückzugsraum schützen. Auf diesen Schutz kann nur der Betroffene selbst verzichten, nicht aber ein Mitbewohner. Wir baten das Justizministerium um eine Änderung der bundesweit einheitlichen Geschäftsanweisung für Gerichtsvollzieher. Nach dessen Mitteilung ist dies mittlerweile erfolgt. Nun darf nur noch der Schuldner selbst über eine Wohnungsdurchsuchung entscheiden.

4.3.10 Protokollierung (auch) der lesenden Zugriffe im Justizvollzug

Im Justizvollzug sind im Interesse einer lückenlosen Transparenz auch lesende Zugriffe auf das Datenverarbeitungsprogramm zu protokollieren.

Die bislang fehlende Protokollierungsmöglichkeit bei lesenden Zugriffen auf die in dem Programm gespeicherten personenbezogenen Daten hatte wiederholt dazu geführt, dass derartige Zugriffe von Dritten auf Gefangenendaten erfolgen konnten, ohne dass bekannt wurde, welche Daten durch wen abgefragt worden sind. In einem Fall wurde einem Wissenschaftler in einer Justizvollzugseinrichtung zu Forschungszwecken für einen eng begrenzten Zeitraum ein Zugriff auf das Datenverarbeitungsprogramm gewährt. Mangels Zugriffsprotokoll war es im Nachhinein nicht möglich nachzuvollziehen, welche Daten der Wissenschaftler zur Kenntnis genommen hat. In einem anderen Fall wurde nach Aufforderung eines Mitarbeiters einer Justizvollzugsanstalt ein Ausdruck aus dem Datenverarbeitungssystem angefertigt. Ursprungsdaten wurden gelöscht und die Daten einer dritten Person eingesetzt; der derart geänderte Ausdruck wurde missbräuchlich für einen „internen Scherz“ verwendet.

Um derartige Zugriffe zukünftig nachvollziehbar zu machen, zu unterbinden oder zu erschweren und ahnden zu können, sind die Vorgänge umfassender zu dokumentieren. Nötig ist nicht nur eine Protokollierung der verändernden, sondern auch der lesenden Zugriffe auf die in dem Datenverarbeitungsprogramm gespeicherten personenbezogenen Daten. Der im Strafvollzugsgesetz geregelte Schutz der Akten und Dateien vor unbefugtem Zugang und Gebrauch durch die technischen und organisatorischen Maßnahmen verlangt eine entsprechende Dokumentation. Die Dokumentation dient u. a. der nachträglichen Kontrolle, ob der Zugriff auf die entsprechenden personenbezogenen Daten des Gefangenen zur Aufgabenerfüllung erforderlich war. Deshalb müssen die Zugriffe auf Daten, die vorgenommenen Veränderungen und gegebenenfalls auch die Begründung der Einsichtnahme in einer nachvollziehbaren Form dokumentiert werden.

Was ist zu tun?

Die systemtechnisch mögliche Protokollierung von lesenden Zugriffen sollte umgesetzt und die weiteren erforderlichen Maßnahmen für die praktische Durchführung einer derartigen Protokollierung sollten veranlasst werden.

4.4 Ausländerverwaltung

4.4.1 Visa-Warndatei

Mit dem vom Bundestag Ende 2011 beschlossenen Visa-Warndateigesetz wird eine Datei errichtet, in der Missbrauchsfälle gespeichert werden. Alle Personen, die mit einem Visumantrag im Zusammenhang stehen, sollen mit der Antiterrordatei abgeglichen werden.

Seitdem vor einigen Jahren Missbrauchsfälle in Visumverfahren bekannt wurden, wird diskutiert, wie die Visumbehörden durch ein Frühwarnsystem Missbrauch besser verhindern können. Die beschlossene Lösung einer Visa-Warndatei ist von den vielen Vorschlägen noch eine der grundrechtsfreundlichen. In der Visa-Warndatei sollen nur tatsächliche Missbrauchsfälle gespeichert werden. Der Zugriff auf die Daten bleibt auf den Zweck des Visumverfahrens und die daran beteiligten Behörden beschränkt. Frühere Vorschläge sahen vor, dass jeder Einlader, Verpflichtungsgeber und jede sonstige Referenzperson in einer Einladerdatei gespeichert werden sollten. Hierauf sollten auch die Sicherheitsbehörden Zugriff erhalten.

Doch auch die jetzige Ausgestaltung der Visa-Warndatei ist zu kritisieren. Wir haben in der Sachverständigenanhörung im Innenausschuss des Bundestags die Erforderlichkeit einer eigenen Datei generell infrage gestellt, da der überwiegende Teil der darin zu speichernden Informationen bereits in anderen zentralen und dezentralen Registern gespeichert ist, insbesondere im Bundeszentralregister und im europäischen Visa-Informationssystem. Die parallele Speicherung der Daten in der Visa-Warndatei erfordert die Herstellung und Aufrechterhaltung einer Kongruenz des Datenbestands der Visa-Warndatei einerseits und der anderen Register andererseits. Dies verursacht Aufwand durch Informationspflichten, aber auch unnötig Gefahren für das Recht auf informationelle Selbstbestimmung. Letztere entstehen, wenn der Informationsfluss zwischen den Registern und der Visa-Warndatei gestört ist und deshalb z. B. Tilgungen in den Registern in der Visa-Warndatei nicht nachvollzogen werden.

Noch weitaus gravierender sind unsere Bedenken gegen den eingeführten Abgleich aller am Verfahren beteiligten Personen mit der Antiterrordatei. Dieser Abgleich stellt einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung der hiervon Betroffenen dar. Das Bundesverfassungsgericht hat wiederholt hervorgehoben, dass die Streubreite einer Maßnahme von maßgebender Bedeutung für das Gewicht des Grundrechtseingriffs ist: „Werden Personen, die keinen Erhebungsanlass gegeben haben, in großer Zahl in den Wirkungsbereich einer Maßnahme einbezogen, können von ihr auch allgemeine Einschüchterungseffekte ausgehen, die zu Beeinträchtigungen bei der Ausübung von Grundrechten führen können. Die Unbefangenheit des Verhaltens wird insbesondere gefährdet, wenn die Streubreite von Ermittlungsmaßnahmen dazu beiträgt, dass Risiken des Missbrauchs und ein Gefühl des Überwachtwerdens entstehen.“ Der Anlass für den Abgleich ist hier die Einreise eines visumpflichtigen Ausländers nach Deutschland. Dies ist nicht per se eine Gefährdung der öffentlichen Sicherheit, sondern legales und für ein weltoffenes Land gesellschaftlich adäquates, in weiten Teilen sogar gesellschaftlich notwendiges Verhalten, beispielsweise für international tätige Organisationen oder Unternehmen. Der vorgesehene Abgleich aller Personen mit der Antiterrordatei begründet die Gefahr, dass sowohl Ausländerinnen und Ausländer als auch in Deutschland lebende Einlader, Verpflichtungsgeber und Referenzpersonen auf

eine Einreise nach Deutschland bzw. auf die Mitwirkung daran vermehrt verzichten. Die Anlässe für eine Speicherung in der Antiterrordatei sind weit gefasst; die Möglichkeit von fehlerhaften Treffermeldungen bei Unbescholtenen und sich daraus ergebenden weiteren Grundrechtseingriffen ist groß. Eine Begründung der Erforderlichkeit fehlte im Entwurf gänzlich.

Die Frage nach der Erforderlichkeit drängt sich hier besonders auf, da für den angegebenen Zweck bereits das Konsultationsverfahren nach § 73 Aufenthaltsgesetz existiert. Die in den vergangenen Jahren stets erweiterte Vorschrift ermächtigt zu einer umfassenden Überprüfung von Visumantragstellern sowie Einladern, Verpflichtungsgebern und sonstigen Referenzpersonen auf etwaige Sicherheitsbedenken. An diesem Verfahren sind Polizeibehörden und Nachrichtendienste beteiligt. Das Verfahren wird allerdings nur bei Staatsangehörigen bestimmter Staaten angewendet. Der Gesetzentwurf legte weder abstrakt noch anhand von konkreten Auswertungen und Beispielsfällen dar, dass sich das Konsultationsverfahren nicht als ausreichend erwiesen hat.

4.4.2 Daten über EU-Bürger im Ausländerzentralregister

Das EuGH-Urteil aus dem Jahr 2008, das eine Speicherung der Daten von Unionsbürgerinnen und -bürgern im Ausländerzentralregister nur eingeschränkt erlaubt, ist endlich gesetzlich umgesetzt.

Die Einrichtung der Visa-Warndatei wurde zügig beschlossen; ein datenschutzrechtlich dringendes Gesetzgebungsvorhaben im Ausländerbereich hat dagegen lange auf sich warten lassen. Vor zwei Jahren berichteten wir über den Gesetzentwurf zur Einschränkung der Speicherung von Daten über EU-Bürgerinnen und -Bürger im Ausländerzentralregister (33. TB, Tz. 4.9.1). Seitdem sind einige Verbesserungen bzw. Präzisierungen an dem Gesetzentwurf vorgenommen worden. Sowohl die Speicheranlässe als auch der Umfang der Daten, die über Unionsbürgerinnen und -bürger gespeichert werden dürfen, sind abschließend beschrieben. Der Entwurf wurde kurz vor Redaktionsschluss endlich beschlossen.

4.5 Soziales

4.5.1 Das Ende von ELENA

Nach langen Diskussionen über eine mögliche verbotene Vorratsdatenspeicherung hat der Deutsche Bundestag im September 2011 entschieden, das Verfahren des elektronischen Entgeltnachweises – ELENA – zu beenden.

Begründet wurde das Aus für ELENA mit Problemen der qualifizierten elektronischen Signatur und des notwendigen Sicherheitsniveaus. Das ULD hatte bereits im Jahr 2007 sein Unverständnis zum Ausdruck gebracht, dass für ein datenschutzrechtlich äußerst bedenkliches Projekt jahrelang große Geldsummen aus dem Staatshaushalt ausgegeben wurden. Wir kritisierten immer wieder die unzulässige Vorratsdatenspeicherung sowie weitere Aspekte, etwa die Nichterteilung von Auskünften an die Betroffenen (z. B. 33. TB, Tz. 4.5.2). In einem Aufhebungsgesetz wurden die Anforderungen zur Abwicklung des ELENA-Verfahrens festgelegt, wozu auch die Löschung der bisher gespeicherten ELENA-Daten gehört. Diese Datenlöschung wurde vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und vom Bundesamt für die Sicherheit in der Informationstechnik überprüft und bestätigt.

4.5.2 ULD kein Ansprechpartner für AOK, MDK und Jobcenter mehr – und nun?

Es war einmal … da war das ULD für die Datenschutzkontrolle beim Medizinischen Dienst der Krankenversicherung (MDK) und bei der AOK Schleswig-Holstein zuständig. Wir überwachten die vielen ARGEn bzw. Jobcenter in Schleswig-Holstein. Der MDK fusionierte mit Hamburg, die AOK mit Westfalen-Lippe, und für die Jobcenter reichte ein Satz im Gesetz. Nun müssen Schleswig-Holsteiner ihre Anliegen im fernen Bonn, Düsseldorf oder Hamburg vortragen (33. TB, Tz. 4.5.1, 4.5.4). In Sozialleistungsverfahren geht es für die Betroffenen oft um sehr viel, etwa deren Gesundheit oder finanzielle Existenz. Nicht immer entscheiden die Behörden positiv; nicht immer sind Entscheidungen fehlerfrei. Hat ein Antragsteller das Gefühl, in seinen Datenschutzrechten verletzt worden zu sein, wird oft die gesamte Entscheidung nicht akzeptiert. Eine datenschutzrechtliche Beratung oder Prüfung hilft sowohl den Behörden als auch den Antragstellern.

Die Datenschutzaufsicht um Hilfe zu bitten, kostet den Mitarbeitern der Behörden als auch den Antragstellern oft Überwindung. Wir haben gelernt, dass es nicht reicht, Hilfe nur anzubieten, sondern dass wir dafür sorgen müssen, dass diese auch angenommen wird. Dementsprechend hat sich das ULD in den letzten Jahren Vertrauen bei den Behörden und Betroffenen erarbeitet. Gerade in dem sensiblen Bereich der Sozialleistungen ist es für Ratsuchende unverständlich, wenn ihr ULD ihnen nicht mehr wirksam helfen darf. Was können die Kollegen im fernen Bonn oder Düsseldorf machen, wenn die Probleme in Heide, Mölln oder Plön zu klären sind? Fragen werden nicht mehr gestellt; Rat wird nicht mehr eingeholt; Konflikte bleiben ungelöst. Für uns bedeutet dies nicht weniger Arbeit. Ungezählte Briefe müssen weitergeleitet und Anrufe beantwortet werden.

Wie wird es weitergehen? Derzeit prüfen die Gerichte, ob nicht auch die IKK Nord in die Zuständigkeit des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gehört. Bei der Landwirtschaftlichen Sozialversicherung wechselte die Zuständigkeit zum Jahresbeginn 2013. Das ULD kann immer weniger Schleswig-Holsteinern in ihren Sozialangelegenheiten wirksam helfen. Wir könnten und wollten es gern tun, wenn wir dürften.

Was ist zu tun?

Es war und ist keine Kostenersparnis und keine Verwaltungseffizienz, wenn in Sozialangelegenheiten Bürgernähe abgebaut wird. Dies ließe sich vom Bundesgesetzgeber rückgängig machen.

4.5.3 Arbeitslosengeld II – Kopien von Kontoauszügen und Personalausweisen

Wer Arbeitslosengeld II beantragt, muss seine Identität und seine wirtschaftliche Situation nachweisen. Zu Recht wird die Vorlage von Ausweispapieren, Mietverträgen, Einkommensnachweisen und Kontoauszügen verlangt. Doch darf die Behörde alle Unterlagen pauschal in Kopie zur Akte nehmen? Nein!

Vorgelegte Unterlagen dürfen nach dem Gesetz nur dann in Kopie zur Akte genommen werden, wenn die in diesen Unterlagen enthaltenen Daten für die weitere Aufgabenerfüllung der Behörde erforderlich sind. Was erforderlich ist, muss im konkreten Einzelfall von der Behörde entschieden werden. Doch was ist erforderlich?

Eine Kopie des Personalausweises ist nicht erforderlich! Das Personalausweisgesetz regelt restriktiv, wann überhaupt Kopien vom neuen Personalausweis gemacht werden dürfen. Die Sammelei der Jobcenter erfüllt diese Voraussetzungen nicht. Hat die Behörde Zweifel an der Identität einer Person, so sollte sie nicht auf alte Kopien in der Akte zurückgreifen, sondern den Betroffenen auffordern, sich aktuell auszuweisen.

Kontoauszüge beinhalten eine Vielzahl von Informationen: Wann wurde wie viel Geld am Automaten abgehoben, bei welchem Discounter wurde mit Karte gezahlt und bei welchem Versandhandel wurde etwas bestellt. Die Daten müssen nicht über

viele Jahre, wenn nicht gar Jahrzehnte in den Jobcentern gesammelt werden. Selbstverständlich dürfen Jobcenter Kontoauszüge einsehen, um festzustellen, ob der Antragsteller vollständige und richtige Angaben gemacht hat. Werden aber keine Auffälligkeiten festgestellt, dann sind die vorgelegten Kontoauszüge wieder auszuhändigen, ohne dass zuvor Kopien für die Akte gefertigt werden. Ein kurzer Vermerk in der Akte genügt in solchen Fällen.

https://www.datenschutzzentrum.de/material/themen/bekannt/kontoaus.htm

Was ist zu tun?

Die Jobcenter dürfen nur im Rahmen der Erforderlichkeit Kopien von vorgelegten Unterlagen zur Akte nehmen. Bei der Aufforderung zur Vorlage von Kontoauszügen sind die Gemeinsamen Hinweise der Landesbeauftragten für Datenschutz der Länder Berlin, Brandenburg, Hamburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und Schleswig-Holstein zu beachten.

4.5.4 TK-Ärztezentrum – ein störrischer Patient

Fast 100 Ärztinnen und Ärzte beraten rund um die Uhr Versicherte der Techniker Krankenkasse (TK). Hunderttausende haben diesen telefonischen Service bereits genutzt und Fragen über ihre Erkrankungen, Behandlungsmöglichkeiten und zu Medikamenten gestellt. Gespeichert wird, wer angerufen hat und warum. Eine riesige Datenbank ist entstanden. Bei dem TK-Ärztezentrum handelt es sich um einen externen Dienstleister, die ife Gesundheits-AG mit Sitz in Gut Nehmten. Die Vorschriften zur ärztlichen Schweigepflicht sind zu beachten. Im November 2008 besuchten wir die ife Gesundheits-AG und stellten akuten Handlungsbedarf fest (33. TB, Tz. 4.5.5). Wir forderten, dass zu Beginn eines Telefonates jeder Anrufer darüber informiert wird,

- dass sich hinter dem TK-Ärztezentrum ein externer Dienstleister verbirgt,
- welche Daten gespeichert und
- welche Daten an die TK übermittelt werden sowie
- dass grundsätzlich alle 100 Ärzte Zugriff auf die Aufzeichnungen haben.

Diese Forderungen wurden vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit auch an die TK als verantwortlichen Auftraggeber gerichtet. Für die ife Gesundheits-AG bzw. die TK ist dies anscheinend eine bittere Pille. Anders lässt sich nicht erklären, dass die Umsetzung unserer Forderungen stockend verläuft und uns Anrufer immer wieder berichten, dass sie die erforderlichen Informationen nicht erhalten hätten. Die ife Gesundheits-AG ist auf einem guten Weg, aber noch nicht geheilt. Sollte sich dieser störrische Patient künftig nicht an unseren Rat halten, wird ein weiterer Hausbesuch erfolgen!

Was ist zu tun?

Um den datenschutzrechtlichen Anforderungen – insbesondere im Hinblick auf die Vorschriften zur ärztlichen Schweigepflicht – gerecht zu werden, muss die TK bzw. die ife Gesundheits-AG gegenüber allen Ratsuchenden zu Beginn eines Telefonates die zu erwartende Datenverarbeitung darstellen.

4.5.5 Kindervernachlässigung in Segeberg – Wer kontrolliert das Jugendamt?

Im September 2012 berichtete die Presse über einen besonders dramatischen Fall einer Kindeswohlgefährdung in Segeberg. Das öffentliche Interesse war groß. Ein externer Gutachter sollte klären, ob das Jugendamt Fehler gemacht hatte. Aber wer durfte das Gutachten erhalten, um über die Arbeit des Jugendamtes zu urteilen?

Der externe Gutachter prüfte die Falldokumentation, las die Gesprächsvermerke und bewertete gewissenhaft das Vorgehen der einzelnen Mitarbeiter des Jugendamtes. Wieso wurde nicht bemerkt, was die Eltern ihren Kindern antaten und warum? Was hätte verhindert und was getan werden können? Das Gutachten zeigte auch Versäumnisse des Jugendamtes auf. Viele Gremien, Fachleute und Politiker verlangten nach dem Gutachten und übersahen dabei, dass das Gutachten auch eine Vielzahl sensibelster Sozialdaten der Eltern und der betroffenen Kinder beinhaltete, also Daten, die dem strengen Schutz des Sozialgeheimnisses unterliegen und daher grundsätzlich zu schützen sind. In einer öffentlichen Stellungnahme legten wir detailliert dar, welche Gremien in welchem Umfang in derartige Gutachten Einblick nehmen dürfen.

https://www.datenschutzzentrum.de/sozialdatenschutz/20121119-kindeswohl-segeberg.pdf

Es verstößt nicht gegen das Sozialgeheimnis, wenn dem Jugendhilfeausschuss des Kreises das vollständige Gutachten zur Verfügung gestellt wird. Aufgabe dieses Ausschusses ist es, die Arbeit des Jugendamtes zu überwachen. Dazu bedurfte es der Kenntnis des vollständigen Gutachtens. Die sonstigen Mitglieder des Kreistages dürfen dagegen nur die Informationen des Gutachtens zur Kenntnis bekommen, die nicht dem Sozialgeheimnis unterliegen. Durch eine Schwärzung der entsprechenden Passagen des Gutachtens wird sichergestellt, dass der Kreistag seine Aufgaben wahrnehmen kann und trotzdem die betroffene Familie gleichzeitig geschützt bleibt. Nachdem kritisiert worden war, dass die Landrätin zu viel geschwärzt habe, war auch der Hauptausschuss des Kreistages gefordert, da diesem die Dienstaufsicht über die Tätigkeit der Landrätin obliegt. Das Innenministerium des Landes Schleswig-Holstein übt die Rechtsaufsicht über die Jugendhilfe des Kreises aus. Es bestehen keine Bedenken an einer Überlassung, soweit ein rechtsaufsichtliches Verfahren durchgeführt wird.

Im konkreten Fall war zunächst streitig, welche Passagen des Gutachtens dem Sozialgeheimnis unterliegen. Die Aufgabe dieser Klärung kam dem Kreis zu, wobei konkret die Kreisverwaltung mit dem Jugendhilfe- und dem Hauptausschuss kooperierten. Das ULD unterstützte diesen Prozess beratend. Dem Sozialausschuss des Landtages und dem Ministerium für Soziales, Gesundheit, Familie und Gleichstellung durfte das vollständige Gutachten nicht ungeprüft zur Verfügung gestellt werden. Diese sind weder für eine Fach- noch eine Rechtsaufsicht zuständig. Eine Übermittlungsbefugnis in Bezug auf Sozialgeheimnisse besteht nicht, sodass nur die Weitergabe eines geschwärzten Gutachtens zulässig war.

Was ist zu tun?

Auch wenn das öffentliche Interesse an einer lückenlosen Offenlegung derartiger Fälle verständlich ist, darf die Übermittlung von Falldaten nur im Rahmen der strengen gesetzlichen Vorschriften, insbesondere des Sozialdatenschutzrechts, erfolgen.

4.5.6 Leumundsanfrage bei Tagesmüttern und ärztliches Attest von Pflegeeltern

Tagesmütter und Pflegeeltern dürfen nur dann Kinder betreuen, wenn diese im Sinne des Gesetzes „geeignet“ sind. Wer eine Pflegeerlaubnis beantragt, wird daher zu Recht vom Jugendamt überprüft. Wie weit darf dabei die Datenerhebung gehen?

In einem Bewerbungsbogen sollen Antragsteller detaillierte Angaben zu ihrer Person, ihrem schulischen und beruflichen Werdegang, ihren finanziellen Verhältnissen und ihrer Wohnsituation machen. Erweiterte polizeiliche Führungszeugnisse und ärztliche Atteste für alle im Haushalt lebenden Personen sind ebenso vorzulegen wie ein Lebenslauf, Nachweise über den Schulabschluss und die Berufsausbildung sowie Einkommensnachweise. Bevor die Erlaubnis erteilt wird, erfolgt außerdem ein Hausbesuch.

Eine angehende Tagesmutter und eine erfahrene Pflegefamilie ärgerten sich über eine Leumundsanfrage und über die Aufforderung, vom Hausarzt ein Attest vorzulegen, das bestätigt, dass man nicht psychisch erkrankt sei. Bei unseren Recherchen stellten wir fest, dass bei der Datenerhebung nicht unterschieden wurde, ob die Erteilung einer Pflegeerlaubnis für Tagesmütter oder eine Vermittlung von Kindern in eine Pflegefamilie erfolgen soll. Den Antragstellern wurden keine erläuternden Hinweise gegeben, und es erfolgte keine Unterscheidung zwischen Pflicht- und freiwilligen Angaben. Viele Fragen, z. B. nach dem Geburtsort, waren entbehrlich oder zu pauschal, etwa nach Vorstrafen, Erkrankungen oder Behinderungen. Die verwendeten Einwilligungserklärungen entsprachen nicht den gesetzlichen Anforderungen.

Die Leumundsanfrage zeigt deutlich, dass Daten teilweise ohne Sinn und Verstand gesammelt wurden. Die Wohnortgemeinde wurde gefragt, ob Bedenken gegen die Erteilung der Pflegeerlaubnis bestehen würden. Manchmal antwortete der Bürgermeister persönlich, häufiger jedoch irgendein Mitarbeiter der Gemeinde, und schilderte, was aus dortiger Sicht über den Antragsteller berichtenswert war. Nicht eine der erteilten spannenden Antworten enthielt Informationen, die für das Bewilligungsverfahren relevant gewesen wären.

Auch die Aufforderung, doch bitte für jedes Familienmitglied vom Hausarzt bestätigen zu lassen, dass keine ansteckenden, psychischen oder Suchterkrankungen bestehen, ist weder hilfreich noch zulässig. Wenn überhaupt, ist der Amtsarzt mit einer aktuellen Einschätzung zu beauftragen. Wir forderten das Jugendamt auf, das Verfahren inklusive der Vordrucke zu überarbeiten und datenschutzgerecht zu gestalten. Die Leumundsanfrage wurde sofort nach unserem ersten Beratungsgespräch eingestellt.

Was ist zu tun?

Bei der Prüfung der Geeignetheit von Tagespflegepersonen und Pflegefamilien dürfen Daten nur zielgerichtet und soweit es für die Durchführung des Bewilligungsverfahrens erforderlich ist erhoben werden.

4.5.7 Wiener Übereinkommen: Daten vom Jugendamt fürs Konsulat

Das Wiener Übereinkommen über konsularische Beziehungen ist keine Rechtsgrundlage für die Übermittlung personenbezogener Daten durch Jugendämter.

Das Wiener Übereinkommen über konsularische Beziehungen regelt, dass die konsularische Vertretung eines Landes benachrichtigt werden muss, sofern die Bestellung eines Vormundes, Pflegers oder Betreuers für einen minderjährigen Staatsangehörigen des jeweiligen Staates erwogen wird. Dabei handelt es sich fraglos um besonders sensible personenbezogene Daten, die von öffentlichen Stellen an Dritte gehen. Die zuständige Behörde hierfür ist jedoch nicht das Jugendamt, sondern das Familiengericht. Dieses betreibt die Verfahren zur Anordnung einer Vormund- bzw. Pflegschaft von Amts wegen, die Jugendämter regen derartige Verfahren lediglich an.

4.5.8 Willkommensbesuche des Jugendamtes bei Familien mit Neugeborenen

Welche Daten dürfen Meldeämter zu welchen Zwecken an Jugendämter übermitteln? Wie ist das Recht auf informationelle Selbstbestimmung im Spannungsverhältnis zum Datenabgleich zum Wohle Neugeborener zu werten? Datenschutz ist hier oft zugleich Kinderschutz.

Nachdem Fälle öffentlich bekannt wurden, in denen Neugeborene, Säuglinge und Babys in ihren Familien durch Verschulden der Eltern zu Schaden gekommen waren, wollen Jugendämter den Eltern Neugeborener Hilfestellungen im Rahmen sogenannter Willkommensbesuche anbieten, die über die Pflichtuntersuchungen der Kinder beim Arzt nach dem Kinderschutzgesetz hinausgehen. Hierbei dürfen aber die Eltern nicht pauschal unter den Verdacht gestellt werden, nicht für das Wohl ihrer Kinder zu sorgen. Auch Neugeborene haben ein Recht auf informationelle Selbstbestimmung, die Verarbeitung von deren Daten bedarf einer Rechtsgrundlage.

Für die Willkommensbesuche wären die Meldedaten der Neugeborenen nützlich. Das geltende Melderecht enthält aber keine Regelung zur Datenübermittlung an Jugendämter für diesen Zweck. Um einerseits die Interessen der Neugeborenen und andererseits die Vorgaben des Datenschutzrechts zu wahren, ist daher im Kreis Segeberg beabsichtigt, die Willkommensbesuche des Jugendamtes zu realisieren, ohne hierbei auf die Übermittlung von Meldedaten zurückgreifen zu müssen. Das Angebot des Jugendamts zu Willkommensbesuchen kann den Eltern über Anschreiben der Krankenhäuser gemacht werden, in denen die Kinder zur Welt kommen. Datenschutzkonform und praktikabel ist auch eine Zusammenarbeit des Kreises mit Frauenärzten, die ebenfalls den werdenden Müttern das Kreisangebot unterbreiten können, oder mit Kinderärzten, die die Pflichtuntersuchungen der Kinder nach dem Kinderschutzgesetz vornehmen.

Grobablauf des kontrollierenden Einladungs- und Meldewesens nach dem Kinderschutzgesetz Schleswig-Holstein:

- Landesamt für soziale Dienste erhält von Meldebehörden Kinderdaten
- Einladungen zu U4 bis U9
- Rückmeldung durch Kinderarzt
- Bei Fehlanzeige Erinnerung
- Abgabe an Kreis: Gesundheitsamt schreibt Eltern an
- Bei Fehlanzeige Abgabe an Jugendamt
- Telefonische/briefliche, dann Vor-Ort-Kontaktaufnahme

4.5.9 Aufbewahrung von Betreuungsakten

Für den Umgang mit Betreuungsakten bei gerichtlich bestellten Betreuern bestehen aus Datenschutzsicht Regelungslücken. Diese sollen durch die folgenden Empfehlungen des ULD für Betreuer geschlossen werden.

Der Betreuer hat als verantwortliche Stelle im Sinne des Datenschutzrechts die technisch-organisatorischen Maßnahmen zu treffen, um den Schutz der personenbezogenen Daten zu gewährleisten. Dies gilt sowohl für die Führung und Aufbewahrung von Papierunterlagen wie für elektronische Akten. Der Betreuer muss deshalb dafür sorgen, dass der Zugang zu Unterlagen und zu deren Inhalten von ihm unter Kontrolle bleibt. Ist das Verfahren abgeschlossen, ist die Akte zu schließen, sicher aufzubewahren und nach Ende der Aufbewahrungspflichten datenschutzkonform zu vernichten. Aufzubewahren sind Betreuungsakten nach Abschluss des jeweiligen Verfahrens so lange, wie dies fachlich erforderlich ist. Dies legt im Prinzip die verantwortliche Stelle, der Betreuer, selbst fest. Für Betreuungsgerichte gilt eine 10-jährige Aufbewahrungspflicht. Hieran sollte sich der gerichtlich bestellte Betreuer orientieren. Sofern für Teile der Akte aus steuerrechtlichen Gründen andere Aufbewahrungsfristen gelten, sind nur die hierfür tatsächlich erforderlichen Teile der Akten aufzubewahren.

Nach Ende der Aufbewahrungspflicht sind die Akten zu vernichten. Dies kann von speziellen, zertifizierten Fachfirmen durchgeführt werden. Der Betreuer kann die Akten auch beim zuständigen Amtsgericht vernichten lassen. In jedem Fall muss die Vernichtung der Akten datenschutzgemäß erfolgen; ein bloßes Entsorgen in der Papiertonne ist nicht ausreichend.

4.6 Schutz des Patientengeheimnisses

4.6.1 Hausarztzentrierte Versorgung

Hausarztzentrierte Versorgung im Land Schleswig-Holstein beschäftigte das ULD auch in den Jahren 2011 und 2012 (33. TB, Tz. 4.5.3).

Nachdem die Anordnung des ULD zur Regelung der Datenverarbeitung im Rahmen der hausarztzentrierten Versorgung (HzV) durch das Verwaltungsgericht und das Oberverwaltungsgericht (OVG) Schleswig im einstweiligen Rechtsschutz überprüft worden ist und beide Gerichte festgestellt haben, dass die geltenden HzV-Verträge gegen materielles Datenschutzrecht verstoßen, sind diese Verträge im Land Schleswig-Holstein nicht in Kraft getreten. Im August 2011 trat mit § 295a Abs. 1 SGB V eine Neuregelung zur Abrechnung der hausarztzentrierten Versorgung in Kraft. Danach sind nicht mehr die Ärzte verantwortliche Stelle für die von ihnen in die Abrechnung gegebenen Daten. Die Hausarztverbände wurden gesetzlich zu verantwortlichen Stellen bestimmt. Aufgrund dieser Regelung sind die Hausarztverbände der Länder befugt, einen Vertragspartner mit der Verarbeitung der entsprechenden abrechnungsrelevanten Daten zu beauftragen. Dies ist in den meisten Fällen das Rechenzentrum der Hausärztlichen Vertragsgemeinschaft – HÄVG-RZ.

Das ULD bemängelt, dass die Datenverarbeitung im Rahmen der HzV-Verträge gesetzgeberisch „geheilt" wurde. Das OVG Schleswig hat im Januar 2011 in seinem Beschluss festgestellt, dass eine von privaten Stellen durchgeführte Abrechnung und Datenverarbeitung im Rahmen der gesetzlichen Krankenversicherung rechtswidrig ist. Damit hat es eine Entscheidung des Bundessozialgerichts vom Dezember 2008 bestätigt. Mit der gesetzlichen Neuregelung erfolgte eine Teillegalisierung des bisherigen Rechtsverstoßes. Dies ändert aber nichts daran, dass die Datenweitergabe an private Stellen im Rahmen der HzV-Verträge im Rahmen der gesetzlichen Krankenversicherung systemwidrig bleibt. Das Gesetz enthält nun eine Erlaubnisnorm für die bisher ausdrücklich nicht erlaubte Datenverarbeitung. Bei dessen Anwendung müssen aber weiterhin das Grundrecht auf informationelle Selbstbestimmung, das Patientengeheimnis der Leistungserbringer und das Sozialgeheimnis gewahrt bleiben. Die andauernden Verhandlungen mit den Hausarztorganisationen zeigen, dass dort bis heute immer noch nicht die damit verbundene Verantwortung bewusst zu sein scheint.

4.6.2 Privatärztliche Verrechnungsstelle und Einwilligung der Patienten

Vermehrt beschweren sich privat versicherte Patienten beim ULD, weil sie ohne Einwilligung in die Übermittlung ihrer personenbezogenen Daten Rechnungen für die privatärztlichen Leistungen von privatrechtlich organisierten Abrechnungszentren erhalten.

Privatärztliche Verrechnungsstellen erheben, verarbeiten und nutzen honorarrelevante medizinische Behandlungsdaten. Diese werden üblicherweise von den behandelnden Ärzten an die Verrechnungsstellen übermittelt. Es gibt mindestens zwei verschiedene Formen der Dienstleistungen der Verrechnungsstellen. Entweder erstellt die Verrechnungsstelle auf Grundlage der vom behandelnden Arzt übermittelten relevanten Patientendaten eine Abrechnung für den jeweiligen Arzt, die an den Patienten versandt wird. Die Verrechnungsstelle kontrolliert den Zahlungseingang und mahnt den fälligen Betrag nach Ablauf der Zahlungsfrist an. Sollte der Patient nicht zahlen, obliegt es dem jeweiligen Arzt, den ausstehenden Betrag einzuklagen.

Oder – und dies ist inzwischen wohl die verbreitetere Dienstleistung – die Verrechnungsstelle kauft die Forderung des Arztes auf und zahlt diesen Betrag sofort nach Abzug einer Risiko- und Gewinnspanne aus. Die Verrechnungsstelle erhält wie im ersten Fall die Behandlungs- bzw. Abrechnungsziffern des jeweiligen Behandlungsverlaufs, führt oft eine Bonitätsabfrage durch, erstellt die Rechnung und kontrolliert den Zahlungseingang. Dieses Mal ist die Verrechnungsstelle aber selbst Forderungsinhaberin. Sie handelt nun in eigenem Namen und auf eigene Rechnung und unterliegt beim weiteren Forderungseinzug nicht den Weisungen des Arztes. Die Entscheidung darüber, wie

die Forderung geltend gemacht wird, obliegt allein der Verrechnungsstelle. Kommt es zu einem Streit über die Zahlungspflicht, z. B. wegen eines Behandlungsfehlers, so beschafft sich die Verrechnungsstelle die forderungsbegründenden Daten, also die Details über die Behandlung.

Gesundheitsdaten dürfen nur unter den Voraussetzungen des § 28 Abs. 6 Nr. 1-4 BDSG für eigene Geschäftszwecke erhoben, verarbeitet und genutzt werden, wenn dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung der Gesundheitsdaten überwiegt. Liegen diese Voraussetzungen nicht vor, ist für die Erhebung, Nutzung und Verarbeitung dieser Daten eine Einwilligung des Patienten erforderlich. Zusätzlich ist § 203 Abs. 1 Nr. 1 StGB zu berücksichtigen, der die unbefugte Offenbarung von Patientengeheimnissen unter Strafe stellt. Eine Weitergabe von Patientendaten an eine praxisfremde Verrechnungsstelle ist unbefugt, wenn eine Einwilligung des betroffenen Patienten nicht vorliegt und keine Rechtsgrundlage für die Weitergabe vorhanden ist. Der Bundesgerichtshof hat bereits im Jahre 1991 festgestellt, dass der Arzt ein ihm anvertrautes Patientengeheimnis offenbart, wenn Patientendaten den Bereich seiner Praxis verlassen, ohne dass eine wirksame Schweigepflichtentbindungserklärung vorliegt. Allein dies sichere das Recht auf informationelle Selbstbestimmung des Patienten. Lediglich ärztlichen Gehilfen und Personen, die zur Vorbereitung auf den Beruf einer ärztlichen Tätigkeit teilnehmen, dürfen die Patientendaten im Zusammenhang mit der konkreten Behandlungssituation offenbart werden.

Ein Arzt bedarf insoweit für die Weitergabe von Patientengeheimnissen einer Offenbarungsbefugnis. Der Patient allein hat die Berechtigung zu entscheiden, an wen der Arzt die Daten zu seiner Person weitergeben darf. Eine Offenbarung der Patientendaten an eine Verrechnungsstelle ist nur zulässig, wenn der Patient ausdrücklich seine Einwilligung zur Offenbarung der Patientendaten erklärt hat. Eine konkludente Einwilligung ist hier nach ständiger Rechtsprechung nicht zulässig. Der Arzt muss dem Patienten dabei mitteilen, welche Daten er zu welchem Zweck an welches Unternehmen weiterleitet. Es ist weiterhin darauf zu achten, dass die Einwilligung freiwillig erteilt wird. Dies bedeutet, dass dem Patienten eine Alternativmöglichkeit zur Abrechnung gegeben werden sollte. Ärzte müssen beim Forderungsverkauf darauf achten, dass sie verpflichtet sind, die dafür erforderlichen Unterlagen, also Behandlungsdokumente mit den entsprechenden Gesundheitsdaten, an den Forderungskäufer zu übermitteln. Dies muss von der Einwilligungserklärung umfasst sein.

Was ist zu tun?

Ärzte müssen, wollen sie sich bei der Abrechnung privatärztlicher Forderungen Dritter bedienen, bei den Behandelten wirksame schriftliche Einwilligungen und Schweigepflichtentbindungserklärungen einholen.

4.6.3 Nationales Krebsregister

Der Entwurf eines Gesetzes zur Weiterentwicklung der Krebsfrüherkennung und zur Qualitätssicherung durch klinische Krebsregister (KFRG) liegt seit August 2012 dem Bundestag zur Beratung vor.

Entsprechend dem Gesetzentwurf soll ein nationales klinisches Krebsregister aufgebaut werden. Bisher gibt es in Schleswig-Holstein ein epidemiologisches Krebsregister und seit Juli 2012 ein klinisches Krebsregister (Tz. 4.6.4). Das epidemiologische Krebsregister dient in erster Linie dazu, die Häufigkeit von Erkrankungen und die Ursachen sowie beeinflussende Faktoren zu erfassen. Mithilfe dieser Daten werden wissenschaftliche Untersuchungen durchgeführt, z. B. auch um zu erkunden, ob Früherkennungsangebote und Vorbeugungsmaßnahmen helfen, die Zahl von Krebserkrankungen zu verringern.

Daneben gibt es sogenannte klinische Krebsregister in den verschiedenen Ländern und in Krankenhäusern. Mit den dort erfassten Daten können

Wissenschaftler untersuchen, welchen Einfluss einzelne Krebstherapien auf die Prognose und die Lebensqualität der Betroffenen haben. Die Qualität der Behandlung und der einzelnen Einrichtungen kann damit überprüft werden. Zusätzlich werden die Daten von niedergelassenen Ärzten und Laboren erfasst und zusammengeführt. Diese können auch behandelnden Therapeuten zur Verfügung gestellt werden. Mit klinischen Krebsregistern kann so auch eine Qualitätskontrolle der individuellen Krebstherapie durchgeführt werden.

Das neue Krebsfrüherkennungs- und -registergesetz schreibt die verpflichtende Einführung eines klinischen Krebsregisters in jedem Bundesland vor. Damit werden bundesweite Standards für die einheitliche Erfassung in Krebsregistern gesetzt, was auch die Vergleichbarkeit der Versorgungsqualität der einzelnen Kliniken zum Ziel hat. Datenschutzrechtliche Brisanz hat dieses nationale klinische Krebsregister, weil neben den Stammdaten zu einer Person auch die Art des Tumors, Sitz und Ausbreitung des Tumors und Stadium der Erkrankung aufgeführt werden. Von den Ärzten werden genaue Angaben zur Diagnose, Therapie und zum Verlauf der Krebserkrankung sowie zur Nachsorge und zur Lebensqualität des Patienten aufgenommen. Das Gesetz schreibt vor, dass alle Identifikationsangaben wie Name, Geburtsdatum und Adresse des jeweiligen Patienten von den krankheitsbezogenen Daten getrennt werden. Beide Datensätze werden jeweils verschlüsselt gespeichert. Damit soll ein Erkennen der gemeldeten Personen verhindert werden. Anders als in den meisten Bundesländern vorgesehen, soll beim nationalen klinischen Krebsregister nicht die Möglichkeit eines Widerspruchs gegen die Aufnahme der Daten eröffnet werden. In einer Stellungnahme hat sich das ULD hiermit kritisch auseinandergesetzt.

Was ist zu tun?

Im laufenden Gesetzgebungsverfahren muss darauf hingewirkt werden, dass eine Aufnahme der Daten in das klinische Krebsregister nur nach Einwilligung der Patientin oder des Patienten zulässig ist.

4.6.4 Klinisches Krebsregister Schleswig-Holstein

Seit dem 1. Juni 2012 gibt es in Schleswig-Holstein ein klinisches Krebsregister. Dieses wird von einem eingetragenen Verein beim Universitätsklinikum Schleswig-Holstein betrieben. Das klinische Krebsregister dokumentiert in erster Linie den Krankheitsverlauf und die therapeutischen Maßnahmen, um so die Qualität der Tumorbehandlung zu fördern. Daher sollen im klinischen Krebsregister neben den Angaben zur Person des Patienten die krankheitsbezogenen Daten – wie Art und Stadium der Krebserkrankung, durchgeführte Operationen, Chemotherapien, Strahlentherapien usw. – erfasst werden. Diese erfassten Daten sollen dann für eine übergreifende und gemeinsame Tumordokumentation aller beteiligten Ärztinnen und Ärzte die Behandlung sichern und effektiver gestalten. Damit kann die Organisation der Behandlung und Nachsorge unterstützt und eine Auswertung aller gesammelten Daten zugunsten der Versorgungsqualität erreicht werden.

Das klinische Krebsregister beruht auf der Einwilligung des jeweiligen Patienten. Jederzeit kann ohne Nennung von Gründen und ohne Nachteil für die Behandlung eine Einwilligung in die Speicherung der personenbezogenen Gesundheitsdaten widerrufen werden. In diesem Fall werden die personenbezogenen Daten im klinischen Krebsregister gelöscht und die Unterlagen mit personenbezogenen Daten vernichtet. Da die Informationen bei allen beteiligten Ärzten jeweils einzeln zu deren Dokumentation weiterhin vorliegen, ist den Dokumentationspflichten nach § 10 Musterberufsordnung der Ärzte Genüge getan.

4.6.5 Apothekerverband und Clearingstelle

Gesetzlich Versicherten wird oftmals vorgegeben, von welchem Hersteller sie ein benötigtes Medikament erhalten dürfen. Dies liegt daran, dass Krankenkassen Rabattvereinbarungen mit einzelnen Pharmaunternehmen abschließen, um so die Kosten zu senken. Die Apotheken übernehmen für ihre Kunden die Prüfung, welche Krankenkasse welches Medikament von welchem Hersteller bezahlt. Auch bei verordneten Hilfsmitteln müssen Apotheken zunächst feststellen, welche Vorgaben die jeweilige Krankenkasse macht. Dies ist ein nicht unerheblicher Verwaltungsaufwand. Es ist nachvollziehbar, dass Apotheken hier nach Auswegen suchen. Dies darf aber nicht zulasten des Patientengeheimnisses gehen.

Es ist ein verlockendes Angebot des Apothekerverbandes Schleswig-Holstein bzw. des Hamburger Apothekervereins: Eine dort eingerichtete Clearingstelle übernimmt für die Apotheke die erforderliche Prüfung von Hilfsmittelverordnungen und klärt im konkreten Einzelfall, ob bzw. von welchem Hersteller die Krankenkasse das benötigte Hilfsmittel bezahlt. Das Rezept wird schnell an die Clearingstelle gefaxt, die alles Weitere klärt. Doch gibt es da einen Haken: Apotheken bzw. Apotheker müssen neben dem allgemeinen Datenschutzrecht ihre besondere berufliche Schweigepflicht beachten und benötigen für eine Offenbarung von Patientendaten eine ausreichende Befugnis. Dies bedeutet, dass das Rezept mit den Versicherten- und Arztdaten nur an die Clearingstelle gefaxt werden darf, wenn die Patientin bzw. der Patient zuvor wirksam und möglichst schriftlich eingewilligt hat. Nichts soll ohne Wissen und gegen den Willen der Versicherten passieren.

Kann oder will die Apotheke die Einwilligung der oder des Versicherten nicht einholen, so müssen die Rezeptdaten vor der Übermittlung an die Clearingstelle ausreichend pseudonymisiert werden. Die Mitarbeiter in der Clearingstelle dürfen nicht die Möglichkeit haben festzustellen, um welche oder welchen Versicherten es sich handelt. Dafür reicht es nicht, nur den Namen wegzulassen. Auch Geburtsdatum, Anschrift und Versichertennummer lassen Rückschlüsse auf die konkrete Person zu. In Absprache mit dem Hamburgischen Beauftragten für den Datenschutz und die Informationsfreiheit forderten wir von dem Apothekerverband Schleswig-Holstein ein datenschutzgerechtes Verfahren.

Was ist zu tun?

Vor einer Übermittlung bzw. Offenbarung von Kundendaten an eine externe Clearingstelle müssen Apotheken die Einwilligung der betroffenen Kunden einholen oder aber die Versicherten- bzw. Arztdaten ausreichend pseudonymisieren.

4.6.6 Patientenarmbänder – Sicherheit auf Kosten des Patientengeheimnisses?

Immer mehr Krankenhäuser in Schleswig-Holstein verwenden Patientenarmbänder für die eindeutige Identifizierung der Patientinnen und Patienten, um so insbesondere die Verwechslung von Patienten auszuschließen.

Dies trägt sicherlich zur Patientensicherheit bei. Aus datenschutzrechtlicher Sicht sind jedoch folgende Aspekte zu beachten:

Zielsetzung definieren

Dient das Patientenarmband ausschließlich der Patientenidentifikation oder auch weiteren organisatorischen Zwecken, wie z. B. der Zuordnung der Verpflegung, Unterscheidung von privat und gesetzlich Versicherten …?

Verwendungsbereich festlegen

Sollen die Armbänder an alle Patientinnen und Patienten ausgehändigt werden, oder werden einzelne Klinikbereiche wie die Psychiatrie ausgenommen?

Freiwilligkeit sicherstellen und die Einwilligung der Betroffenen einholen

Die Patienten sollten bereits bei der Aufnahme über den Sinn und Zweck der Armbänder aufgeklärt werden. Nur Patienten, die ihre Einwilligung (schriftlich) erteilen, wird ein Armband ausgehändigt. Bei Minderjährigen sind die Sorgeberechtigten zu fragen.

Inhalte der Armbänder festlegen

Grundsätzlich genügt die Aufnahme von Name, Vorname, Geschlecht, Geburtsdatum und einer Fallnummer bzw. gegebenenfalls einem Barcode.

Farbliche Gestaltung

Soweit möglich sollte auf eine unterschiedliche farbliche Gestaltung der Armbänder verzichtet werden, um eine Diskriminierung durch andere Patienten auszuschließen.

Einschaltung von Dienstleistern

Werden externe Firmen mit der Herstellung, Beschriftung oder Vernichtung beauftragt, ist zu prüfen, inwieweit diesen Patientendaten zur Kenntnis gelangen könnten und ob hierfür eine ausreichende Befugnis vorliegt.

Vorgang der Identifizierung

Erfolgt eine optische Prüfung durch einzelne Mitarbeiter oder der Einsatz von Lesegeräten?

Einschätzung von Missbrauchsszenarien

Wie könnten Unbefugte an die Armbänder gelangen, die Daten auslesen und unberechtigt verwenden? Welche Sicherheitsvorkehrungen sind zu treffen?

Dienstanweisung/Verfahrensanweisung

Die zuvor aufgezeigten Punkte sind vor dem Einsatz von Patientenarmbändern schriftlich in einer für alle Mitarbeiterinnen und Mitarbeiter verbindlichen Dienstanweisung festzulegen.

4.6.7 Elektronische Gesundheitskarte – Was kann sie wirklich?

Die elektronische Gesundheitskarte (eGK) ist ein bundesweites Projekt, für das viel Geld aus dem Staatshaushalt ausgegeben wurde und das (noch?) nicht die gewollte Wirkung erzielt.

Nach langem Diskutieren kam man im April 2010 überein, dass die elektronische Gesundheitskarte (eGK) zwar eingeführt werden soll, aber nicht mit den ursprünglich vorgesehenen Merkmalen. Auf der eGK sollen lediglich die Versichertenstammdaten und im Falle einer Einwilligung freiwillig ein sogenannter Notfalldatensatz gespeichert werden. Die gesetzlichen Krankenkassen mussten bis Ende des Jahres 2012 70 % ihrer Versicherten mit der eGK ausgestattet haben. Gemäß § 291 SGB V muss die Versichertenkarte ein Foto der oder des Versicherten enthalten. Weiter gehende Anforderungen an das Foto enthält das Gesetz nicht. Vorläufig enthält die neue eGK bis auf das aufgedruckte Foto keine weiter gehenden Daten als die bisherige Krankenversichertenkarte.

Die neue elektronische Gesundheitskarte enthält jedoch einen Mikroprozessor, der es möglich macht, künftig sensible Gesundheitsdaten verschlüsselt und gegen unberechtigten Zugriff geschützt zu speichern. Im Laufe der nächsten Jahre soll es mit der Einwilligung des Patienten möglich sein, neben der Aufnahme von Notfalldaten auch eine Arzneimitteldokumentation, eine Impfdokumentation, eine Aussage zur Organspendebereitschaft und den Zugang zu einer elektronischen Patientenakte zu ermöglichen. Verwaltungsdaten der Versicherten sollen online aktualisiert werden können. Damit wäre es z. B. nicht mehr erforderlich, bei Adressänderungen die Karte auszutauschen. Auch eine sichere Kommunikation zwischen Ärzten soll durch die eGK ermöglicht werden, z. B. die Übermittlung von Arztbriefen und Befunden.

Gesetzlich verpflichtend ist auf der Gesundheitskarte lediglich die Speicherung von Verwaltungsdaten. Dies sind Angaben zur Person wie Name, Geburtsdatum, Geschlecht und Anschrift sowie Angaben zur Krankenversicherung. Unter Angaben zur Krankenversicherung sind die Krankenversichertennummer, der Versicherungsstatus und der Zuzahlungsstatus aufzuführen. Alle weiter gehenden Daten werden nur mit Einwilligung des Versicherten gespeichert. Ein Zugriff von Dritten auf die elektronische Gesundheitskarte ist nicht zulässig. Die auf der elektronischen Gesundheitskarte gespeicherten Daten dürfen nur zum Zweck der medizinischen Versorgung verwendet werden.

4.7 Wissenschaft und Bildung

Schulen hinkten über Jahre hinweg hinsichtlich des Einsatzes von Informationstechnik (IT) der übrigen Verwaltung und der Wirtschaft hinterher. Dies hat sich mit der massiven Verbreitung insbesondere von mobilen IT-Geräten wie Smartphones bei Schülerinnen und Schülern sowie bei den Lehrkräften schlagartig geändert (Tz. 4.7.3). Der enorme Bedarf nach Einsatz von mehr Social Media in den Schulen veranlasste das ULD, sich im Februar 2011 an das Bildungsministerium mit einer Liste zu bewältigender Aufgaben zu wenden. Heikle Vorfälle an Schulen in Schleswig-Holstein bestätigten, dass neue Regeln sowie eine Modernisierung und Standardisierung beim IT-Einsatz einschließlich besserer Sicherungsmaßnahmen dringend nötig sind.

Schon ein Jahr später bestand Anlass, die Skizze „personenbezogene Datenverarbeitung der Schulen" zu überarbeiten und zu veröffentlichen, verbunden mit der erneuten dringenden Bitte an das Bildungsministerium, ordnend tätig zu werden. Diese Bitte fand bei dem neu besetzten Bildungsministerium Gehör. Das ULD einigte sich im November 2012 mit dem Staatssekretär des Bildungsministeriums, die in der Skizze genannten Problempunkte gemeinsam systematisch abzuarbeiten.

https://www.datenschutzzentrum.de/schule/20120417-strategiepapier-schulen.html

4.7.1 Schulen und Facebook

Das ULD wurde darauf aufmerksam gemacht, dass Facebook als Kommunikationsplattform zwischen Lehrkräften und Schülerinnen und Schülern über private Facebook-Profile genutzt wird. Dies ist datenschutzrechtlich wie pädagogisch infrage zu stellen.

Teilweise wurden Schulausfälle wegen Schnee, Hausaufgaben und Seminaraufgaben nur über Facebook-Profile der Lehrkräfte bekannt gegeben. Da es sich dabei um eine schulinterne bzw. unterrichtserforderliche – also dienstliche – Kommunikation handelt, ist eine Nutzung von Facebook als Kommunikationsplattform unzulässig.

Für die Verarbeitung von Schülerdaten finden die Vorschriften des § 30 Schulgesetzes (SchulG) und der Datenschutzverordnung Schule (DSVO Schule) Anwendung. Nach § 4 Abs. 1 DSVO Schule ist für die Verarbeitung der personenbezogenen Daten der Schülerinnen und Schüler sowie der Eltern die Schulleiterin oder der Schulleiter verantwortlich. Der Umfang der personenbezogenen Daten, die nach § 30 Abs. 1 SchulG von der Schule verarbeitet werden dürfen, ist dort und ergänzend in der Anlage zu § 4 der DSVO Schule abschließend aufgeführt. Als Telekommunikationsdaten dürfen nur die Telefonnummern und die E-Mail-Adressen der Eltern erhoben und weiterverarbeitet werden. Die Erhebung und Weiterverarbeitung von eigenen Telekommunikationsadressen der Schülerinnen und Schüler ist in diesen Vorschriften nicht vorgesehen. Aus Sicht des ULD ist gegen die Nutzung solcher Daten durch die Lehrkräfte im Grundsatz nichts einzuwenden, wenn es dem Unterrichtszweck dient. Doch darf von den Vorgaben der oben genannten Vorschriften nicht abgewichen werden. Die erforderlichen Daten werden von der Schulleitung zur Verfügung gestellt. Die Nutzung von Facebook-Accounts – und damit auch die Erhebung durch die Lehrkräfte – ist selbst mit der Einwilligung der Schülerinnen und Schüler im Rahmen ihrer schulischen Tätigkeit nicht zulässig, da die Schule diese Daten generell nicht erheben darf.

Das Ministerium für Bildung und Wissenschaft des Landes Schleswig-Holstein hat sich mit einem Schreiben vom November 2012 an alle Schulen dieser Bewertung angeschlossen. Das Ministerium hält eine direkte dienstliche Kommunikation über Facebook für unzulässig. Das Ministerium weist zu Recht darauf hin, dass Schülerinnen und Schüler keinen Nachteil dadurch erfahren dürfen, dass sie an einer Kommunikation schulisch relevanter Themen über Facebook nicht teilnehmen.

Bezüglich der Nutzung einer Facebook-Fanpage durch Schulen verweisen wir auf unsere allgemeinen Ausführungen zu öffentlichen Stellen (Tz. 1.5). Das Ministerium für Bildung und Wissenschaft schlägt für den Bereich der Schulen vor, auf den Betrieb von Fanpages auf Facebook zu verzichten.

4.7.2 LanBSH mausert sich zur „Allzweckwaffe“ für mehr Effizienz

Das LanBSH eröffnet immer mehr Möglichkeiten, personenbezogene Daten von Schülerinnen und Schülern sicher im Landesnetz zu übermitteln. Für die Schulen ist dies eine Arbeitserleichterung. Wiederkehrende gesetzliche Aufgaben können so automatisiert bearbeitet werden.

Im Jahre 2011 wurde erstmalig die jährliche Schulstatistik größtenteils über das LanBSH abgewickelt. Das Statistische Amt für Hamburg und Schleswig-Holstein erhielt so wesentlich schneller die erforderlichen statistischen Daten als zuvor. Möglich wurde dies durch die genaue Abstimmung bestimmter Schulverwaltungsprogramme auf die Schnittstellendefinition für die Erzeugung der schulstatistischen Daten.

Alle Schulen, die diese Programme einsetzten und bereits am LanBSH angeschlossen waren, konnten schnell valide Daten an das Statistische Amt übermitteln. Schulverwaltungen ohne Anschluss zum LanBSH und ohne kompatible Schulverwaltungsprogramme mussten ihre statistischen Daten über aufwendigere andere Wege zur Verfügung stellen.

Über das LanBSH wird zukünftig auch die Mitteilung der Schulabgängerinnen und Schulabgänger aus den allgemeinbildenden Schulen und Förderzentren an die beruflichen Schulen in automatisierter Form erfolgen. Auch in diesem Fall ist ein kompatibles Schulverwaltungsprogramm und der LanBSH-Anschluss Voraussetzung. Ein flächendeckender Einsatz wird den Verwaltungsaufwand der allgemeinbildenden und der beruflichen Schulen in dieser Hinsicht spürbar minimieren.

Die Effizienzsteigerung durch solche automatisierten Vorgehensweisen trägt auch zur Wirtschaftlichkeit bei. Damit wird den Anmerkungen des Landesrechnungshofes Rechnung getragen, der einen weiteren Ausbau des LanBSH und die Vereinheitlichung der Schulverwaltungsprogramme gefordert hat.

Was ist zu tun?

Das Land sollte unter Federführung des Bildungsministeriums den Anschluss der noch nicht an das LanBSH angeschlossenen Schulen forcieren und einheitliche Vorgaben für datenschutzkonforme Schulverwaltungsprogramme festlegen.

4.7.3 Neue Möglichkeiten des EDV-Einsatzes in der Schule – neue Fragen

Smartphones und Tablets halten Einzug in den Schulen bei Schülerinnen und Schülern wie bei Lehrkräften. Letztere nutzen ihre privaten Geräte auch für die Verarbeitung von dienstlichen Schülerdaten. Dies wirft Fragen auf, die schnellstmöglich beantwortet werden müssen.

Das ULD erreicht eine Vielzahl von Anfragen von Schulleitungen und Lehrkräften, ob der Einsatz dieser Geräte zur Verarbeitung von Schülerdaten in der Schule zulässig ist. Insbesondere die Anwendung „TeacherTool“, die derzeit nur auf Geräten der Firma Apple lauffähig ist, ermöglicht diesbezüglich viele Nutzungen. Die Verwaltung von Klassenlisten und Fotos der Schülerinnen und Schüler, aber auch von Noten ist vorgesehen. Diese Anwendung ersetzt den traditionellen Papierlehrerkalender. Die geltenden bereichsspezifischen Regeln erlauben den Lehrkräften eine personenbezogene Datenverarbeitung mit privaten informationstechnischen Geräten mit Genehmigung der Schulleitung ausschließlich in ihrem häuslichen Bereich. Eine Verwendung von Smartphones und Tablets zur Verarbeitung personenbezogener Daten in der Schule ist durch diese Vorschrift nicht abgedeckt. Die Datensicherheit dieser Geräte ist derzeit nicht hinreichend gewährleistet. Das ULD rät deshalb im Moment von der Nutzung dieser Geräte und der genannten Anwendung ab.

Dessen ungeachtet kann der Einsatz solcher neuen Geräte den Arbeitsalltag der Lehrkräfte künftig auch im Hinblick auf die Verarbeitung personenbezogener Daten erleichtern. Eine solche Nutzung

in datenschutzkonformer Weise setzt aber eine Überarbeitung der Rechtsgrundlagen voraus, die Anforderungen an eine sichere Verarbeitung der Daten, etwa zum Schutz vor dem Zugang Unbefugter, festlegen.

Was ist zu tun?

Das Bildungsministerium sollte darüber befinden, ob und unter welchen Voraussetzungen Lehrkräften die Nutzung privater Smartphones und Tablets zur Verarbeitung personenbezogener Daten der Schülerinnen und Schüler sowie der Eltern erlaubt werden soll. Das Ergebnis muss Eingang in die Rechtsgrundlagen und Verfahrensregeln finden sowie in die Anforderungen hinsichtlich der Datensicherheit dieser Geräte.

4.7.4 Handreichung für die Schulsozialarbeit

Die Handreichung des ULD für die Schulsozialarbeiterinnen und Schulsozialarbeiter erweist sich als sinnvolle Hilfe bei der täglichen Arbeit.

Im letzten Tätigkeitsbericht (33. TB, Tz. 4.7.7) berichteten wir über die datenschutzrechtlichen Herausforderungen für Schulsozialarbeiterinnen und Schulsozialarbeiter in ihrer täglichen Praxis. Um ihnen im datenschutzrechtlichen Bereich Handlungssicherheit zu geben, haben wir zusammen mit dem Sozialministerium und dem Bildungsministerium im Jahr 2011 wie angekündigt eine Broschüre fertiggestellt, zu der wir zahlreiche positive Rückmeldungen erhalten. Unsicherheiten hinsichtlich der Zusammenarbeit zwischen Schule und Schulsozialarbeit bleiben aber weiterhin bestehen. Dies mag am Fehlen hinreichend präziser Rechtsvorschriften liegen. Weder im Schulgesetz noch in der Datenschutzverordnung Schule finden sich bisher hierzu Vorgaben.

Was ist zu tun?

In der Datenschutzverordnung Schule sollten vom Bildungsministerium zur Datenverarbeitung hinsichtlich der Zusammenarbeit zwischen Schulsozialarbeit und Schule eindeutige Regelungen verankert werden.

4.7.5 Regeln für die Videoüberwachung in Schulen

Schulen und Schulträger wünschen sich häufig aus Sicherheitsgründen den Einsatz von Videoüberwachungstechnik in den Schulen. Mit einem Erlass des Bildungsministeriums wurde nun Rechtssicherheit geschaffen.

In den letzten Jahren wurden wir immer intensiver von Schulen und Schulträgern um datenschutzrechtliche Beratung zur Installation von Videoüberwachungsanlagen gebeten. Schulen wollten Kameras in und an den Gebäuden installieren, um z. B. vermehrt auftretende Diebstähle von Schuleigentum oder von Sachen der Schülerinnen und Schüler aufzuklären bzw. zu verhindern. Schulträger äußerten vorrangig ihr Interesse am Schutz ihrer Schulgebäude, insbesondere vor Graffiti und anderen Sachbeschädigungen. Das ULD sieht aus Datenschutzsicht die Installation von Videoüberwachungskameras in Schulgebäuden kritisch, das Bildungsministerium hat bildungspolitische Vorbehalte. Doch lassen sich die Argumente für mehr visuelle Kontrolle nicht pauschal zurückweisen.

Deshalb haben das ULD und das Bildungsministerium in Absprache mit den die Schulträger vertretenden kommunalen Landesverbänden eine Erlasslösung entwickelt, die dem informationellen Selbstbestimmungsrecht der betroffenen Schülerinnen und Schüler, Eltern und Lehrkräften Rechnung trägt und andererseits den Bedürfnissen der Schulträger entgegenkommt. Der Erlass (NBl. MBK. Schl.-H. 2010, S. 145) gibt klare Hinweise, für welche Zwecke und an welchen Örtlichkeiten Videokameras installiert werden dürfen. Ferner werden Vorgaben für den Beginn und das Ende der Videoaufzeichnungen sowie die maximale Speicherungsdauer für die Videosequenzen und den Zugriff auf die Bilder festgelegt.

4.7.6 Tausche Fingerabdruck gegen Schulmittagessen

Schulen bieten ihren Schülerinnen und Schülern Mittagsverpflegung in eigenen Mensen an. Dabei finden auch elektronische Systeme Anwendung, die die Verwaltung der Essenausgabe über die Fingerabdrücke der Schülerinnen und Schüler steuern.

Besorgte Eltern informierten uns, dass Schulen zur Organisation ihrer Mittagsverpflegung die Fingerabdrücke der betroffenen Schülerinnen und Schüler einscannen. Seitens der Schule waren ihnen die technischen Prozesse nur ungenügend erklärt worden. Wir schauten uns deshalb das Verfahren und die damit verbundene Verarbeitung personenbezogener Daten an und konnten hier Entwarnung geben. Bei dem Verfahren werden keine kompletten Fingerabdrücke eingescannt und gespeichert, sondern nur bestimmte Punkte eines Fingerabdrucks in einen mathematischen Wert, einen Hashwert, umgerechnet. Der Fingerabdruck erzeugt immer denselben Hashwert und ermöglicht so eine Zuordnung zu den bestellten Mittagessen.

Das von uns geprüfte Programm verarbeitet die personenbezogenen Daten der Schülerinnen und Schüler sowie die Hashwerte separat vom Mensaverpflegungsprogramm. Die Firma, die die Mittagsverpflegung herstellt, erhält also keine Kenntnis von diesen Daten. Unter diesen Bedingungen haben wir das Verfahren als datenschutzrechtlich zulässig erachtet. Der Vorgang zeigte, wie wichtig es ist, vor der Einführung solcher Systeme eine umfassende Aufklärung der Elternschaft vorzunehmen.

Was ist zu tun?

Schulen, die die Einführung eines auf Fingerabdrücken basierenden Essenausgabesystems für ihre Mensen planen, sollten vorher prüfen, ob das System den Datenschutzanforderungen genügt. Über die technischen und organisatorischen Gegebenheiten sollte vor der Einführung umfassend informiert werden.

4.7.7 Zwischen Schule und Beruf – datenschutzkonformes Übergangsmanagement

Kreise und kreisfreie Städte haben in den letzten Jahren Projekte aufgelegt, um minderjährigen Schulabgängerinnen und Schulabgängern, die keinen Ausbildungsplatz erhalten haben, den Übergang in die Berufsausbildung zu erleichtern.

Diese Projekte möchten von den Schulen die personenbezogenen Daten der Schulabgängerinnen und Schulabgänger erhalten, um diese gezielt anzusprechen. Projektleitungen wandten sich an uns und baten um Beratung. Wir mussten mitteilen, dass eine Übermittlung der personenbezogenen Daten von den allgemeinbildenden Schulen und den Förderzentren nur mit der Einwilligung der betroffenen Schülerinnen und Schüler bzw. deren Eltern möglich ist. Gemeinsam konnten aber dennoch Wege gefunden werden, die Projektarbeit erfolgreich durchzuführen. Eine enge Zusammenarbeit der Projekte mit den betroffenen Schulen erlaubt es, ohne größere Schwierigkeiten

und ohne Vorabübermittlungen die nötigen Einwilligungserklärungen zu erhalten. Entscheidend sind eine klar strukturierte Planung der Vorgehensweise vor Beginn des Projekts und Transparenz gegenüber den Betroffenen.

4.8 Steuerverwaltung

4.8.1 Die Steuerverwaltung ohne Auskunftsanspruch

Die Finanzverwaltung verweigert in Schleswig-Holstein weiterhin immer wieder Betroffenen Auskunft bzw. Einsicht zu Informationen in der eigenen Steuerakte.

In der Abgabenordnung (AO) ist ein Auskunftsanspruch bezüglich der eigenen Steuerakte bisher nicht gesetzlich festgeschrieben. Daraus folgert die Finanzverwaltung des Landes Schleswig-Holstein, dass dieser Anspruch aufgrund einer „absichtsvollen Nichtregelung in der Abgabenordnung" auch nicht bestünde. Ein Anspruch auf Einsicht in die eigene Steuerakte sei insbesondere dann ausgeschlossen, wenn der Steuerpflichtige Auskunft begehrt, um zivilrechtliche Ansprüche gegen den Bund oder ein Land durchzusetzen, sprich, wenn der Finanzverwaltung ein Fehler unterlaufen sein könnte und diese Auskunft der Vorbereitung eines Amtshaftungsverfahrens dient.

Diese Position des Finanzministeriums ist schlicht verfassungswidrig und bürgerfeindlich und ignoriert gerichtliche Entscheidungen: Das Bundesverfassungsgericht (BVerfG) hat mit seiner Entscheidung vom 10. März 2008 ausdrücklich festgestellt, dass natürliche Personen einen grundrechtlich geschützten Anspruch aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG und Art. 19 Abs. 4 GG auf die Information zu den sie betreffenden gesammelten Daten haben (BVerfG, Beschluss vom 10.03.2008, Az: 1 BvR 2388/03). Die Gewährleistung eines tatsächlich effektiven Rechtsschutzes setzt die Kenntnis derartiger Informationen voraus. Der Gesetzgeber muss unter Beachtung der Grundrechte der Betroffenen hinreichende Kenntnischancen gewährleisten. Ein Auskunftsanspruch tritt nur in den Hintergrund, wenn die Aufgabenerfüllung und eine gleichmäßige Festsetzung und Erhebung von Steuern gefährdet würde, wobei dann in jedem Fall die widerstreitenden Interessen abgewogen werden müssen.

Das BVerfG hat im Hinblick auf eine Bundessteuerbehörde § 19 Bundesdatenschutzgesetz als Entscheidungsmaßstab für einen Informationszugang im Bereich der Steuerverwaltung herangezogen. Das Fehlen eines Akteneinsichts- und Auskunftsrechts in der AO könne nicht als fortbestehende planvolle Negativregelung interpretiert werden. Die Anwendung der Datenschutzgesetze könne nicht ausgeschlossen werden. Die Entscheidung des BVerfG ist mit Verweis auf § 27 LDSG auf die Finanzämter des Landes Schleswig-Holstein im laufenden Steuerverfahren übertragbar.

Gemäß § 27 Abs. 3 Nr. 1 LDSG darf eine Auskunftserteilung oder Gewährung von Einsicht nur unterbleiben, wenn eine Prüfung ergibt, dass dadurch die Erfüllung der Aufgaben der datenverarbeitenden Stelle, einer übermittelnden Stelle oder einer empfangenden Stelle gefährdet würde. Das LDSG sieht keine Darlegungsverpflichtung eines berechtigten Interesses des Betroffenen vor. Insoweit steht ein Schreiben des Bundesministeriums für Finanzen (BMF) vom 17.12.2008 im Widerspruch zur Entscheidung des BVerfGs und zum Grundrecht des Betroffenen auf informationelle Selbstbestimmung. Die Forderung vom Auskunftsersuchenden, ein berechtigtes Interesse darlegen zu müssen, steht im Widerspruch zu unserem Grundgesetz. Auch in § 27 LDSG wird den Behörden bei der Auskunftserteilung kein Ermessen eingeräumt.

Diese Verfassungsrechtsprechung wurde von der Verwaltungsgerichtsbarkeit übernommen. So bestätigte das VG Potsdam einen Auskunftsanspruch eines Betroffenen im Rahmen eines Besteuerungsverfahrens und nahm Bezug auf eine Regelung, die dem § 3 Informationszugangsgesetz Schleswig-Holstein (IZG-SH) entspricht (VG Potsdam, Urteil vom 27.04.2010, Az: 3 K 1595/05, Tz. 41). Von einer planvollen Nichtregelung des Akteneinsichtsrechts könne keine Rede sein. Eine Weisung des BMF, also eine exekutive Verwaltungsvorschrift, kann den grundrechtlich begründeten Auskunftsanspruch nicht infrage stellen.

Die Nichterteilung der Auskunft, z. B. des Finanzamtes Kiel-Süd, wird deshalb immer wieder durch das ULD beanstandet. Das Oberverwaltungsge-

richt (OVG) Schleswig schloss sich mit einem Urteil vom 6. Dezember 2012 dem Urteil des OVG Nordrhein-Westfalen vom 15. Juni 2011 an und bejahte einen Anspruch auf Akteneinsicht aus dem IZG-SH im laufenden Steuerverfahren gegenüber dem Finanzamt. Zusätzlich hat das OVG Schleswig einen datenschutzrechtlichen Auskunftsanspruch bejaht. Mit dem Urteil des OVG Schleswig ist hoffentlich der langjährige Streit mit der Finanzverwaltung des Landes Schleswig-Holstein beendet.

Was ist zu tun?

Die Finanzverwaltung muss endlich ihre Verweigerungspraxis bei Auskunftsansprüchen von Betroffenen beenden.

4.8.2 Zusendung falscher Steuerunterlagen

Erneut informierten Steuerpflichtige mehrfach das ULD, dass ihnen vom Finanzamt Steuerunterlagen fremder Personen zugesandt wurden (32. TB, Tz. 4.8.3).

Konkret betroffen waren das Finanzamt Ratzeburg, das Finanzamt Flensburg, das Finanzamt Stormarn und das Finanzamt Kiel-Süd. Es handelte sich jeweils um von Steuerpflichtigen eingereichte Steuerbelege, also Kontoauszüge, Arztrechnungen, Überstundennachweise usw. Diese Unterlagen sind nach Prüfung durch das Finanzamt üblicherweise an die Steuerpflichtigen zurückzusenden. In allen dem ULD bekannten Fällen sind diese sensiblen Daten an andere Steuerpflichtige versandt worden. Der Grund war jeweils eine falsche Befüllung von Briefumschlägen. Dass eine hohe Arbeitsbelastung zu Fehlern im Arbeitsablauf führen kann, ist dem ULD bekannt. Bei den Steuerunterlagen handelt es sich aber um besonders schutzbedürftige und rechtlich geschützte Daten. Hier kann besondere Sorgfalt erwartet werden.

Was ist zu tun?

Die Leitungen der Finanzämter müssen organisatorische Vorkehrungen treffen, dass die Mitarbeiterinnen und Mitarbeiter bei der Bearbeitung von Steuerunterlagen Sorgfalt walten lassen und Verwechslungen vermeiden.

05

KERNPUNKTE

Versicherungen

Finanzdienstleistungen

Cloud Computing

5 Datenschutz in der Wirtschaft

5.1 Datenschutz in der Versicherungswirtschaft

Das ULD hat den Vorsitz der Arbeitsgruppe (AG) Versicherungswirtschaft des Düsseldorfer Kreises inne, der das Koordinierungsgremium der deutschen Datenschutzaufsichtsbehörden im nicht öffentlichen Bereich ist.

Die AG Versicherungswirtschaft hat im Berichtszeitraum die Verhandlungen mit dem Gesamtverband der Deutschen Versicherungswirtschaft (GDV) zum Hinweis- und Informationssystem (HIS) sowie zur Einwilligungs- und Schweigepflichtentbindungserklärung zur Verwendung von Gesundheitsdaten abgeschlossen. Ebenfalls konnten die Verhandlungen zu einer Verhaltensregel für die Versicherungswirtschaft nach § 38a Bundesdatenschutzgesetz (BDSG) abgeschlossen werden.

5.1.1 Hinweis- und Informationssystem der Versicherungswirtschaft (HIS)

Nach langen Verhandlungen der AG Versicherungswirtschaft mit dem GDV hat im April 2011 das neue Hinweis- und Informationssystem der Versicherungswirtschaft (HIS) als Warndienst den Betrieb aufgenommen. Betreiber ist die informa Insurance Risk and Fraud Prevention GmbH (IIRFP) mit Sitz in Baden-Baden. IIRFP ist ein Teil der infoscore-Gruppe. Zu dieser gehört auch eine der größten deutschen Auskunfteien, die infoscore Consumer Data GmbH (ICD). Die Datenbanken der ICD und der IIRFP sind streng voneinander getrennt. Einziger Geschäftszweck der IIRFP ist der Betrieb des HIS.

HIS dient der Bekämpfung und Verhinderung von Versicherungsbetrug und -missbrauch. Gemeldet werden können Personen wie Versicherungsnehmer oder Geschädigte sowie Objekte wie Fahrzeuge und Gebäude. Meldungen in HIS erfolgen nur, wenn bestimmte Auffälligkeiten bestehen. Diese werden bei besonderen Schadenfolgen, atypischen Schadenhäufigkeiten, Auffälligkeiten im Schadens- bzw. Leistungsfall und besonderen Risiken angenommen.

- Unter besonderen Schadenfolgen werden Fälle wie die fiktive Abrechnung eines Fahrzeugschadens auf Gutachterbasis ab einer bestimmten Höhe verstanden, wenn also keine Reparatur erfolgt. Es soll verhindert werden, dass derselbe Schaden etwa bei einem Wechsel der Versicherung nochmals eingereicht wird.
- Atypische Schadenhäufigkeiten beziehen sich auf einen bestimmten, nach Versicherungssparte unterschiedlichen Zeitraum. In der Rechtsschutzversicherung erfolgt eine Meldung beispielsweise regelmäßig, wenn innerhalb von zwölf Monaten vier oder mehr Versicherungsfälle eingetreten sind.
- Auffälligkeiten des Schadensfalls stellen Auffälligkeiten des Schadenhergangs, -bildes oder -umfangs dar, die nach den Erfahrungen der Betrugsaufklärung und der Rechtsprechung Hinweiskriterien für Betrugsfälle darstellen. Hierunter fallen z. B. Hinweise auf banden- oder gewerbsmäßigen Versicherungsbetrug. Diese können vorliegen, wenn wiederholt Verkehrsunfälle vorgetäuscht werden, wobei Bandenmitglieder jeweils in unterschiedlichen Rollen – als Fahrer, Zeuge, Anspruchsteller – in Erscheinung treten.
- Erschwerte Risiken sind z. B. beim Abschluss einer Lebensversicherung eine risikoerhebliche Vorerkrankung oder ein gefährlicher Beruf. Der konkrete Beruf oder die konkrete Krankheit sowie andere Gesundheitsdaten dürfen nicht an das HIS gemeldet werden. Damit Versicherungen Überversicherungen eines Kunden erkennen können, werden ab einer bestimmten Höhe Versicherungssummen und Rentenhöhen in HIS gemeldet. Von einer Überversicherung geht die Versicherungswirtschaft aus, wenn beispielsweise eine Rentensumme versichert ist, die das Interesse an der Vermeidung des Versicherungsfalls mindern kann.

Das neue HIS ersetzt das vom GDV seit 1993 genutzte alte HIS, das auch als „Uniwagnis"-System bezeichnet wurde (30. TB, Tz. 5.1). Dieses entsprach in vielfacher Hinsicht nicht den datenschutzrechtlichen Vorgaben und war deshalb von den Aufsichtsbehörden als unzulässig beanstandet worden.

Das neue HIS wurde in Abstimmung zwischen der Versicherungswirtschaft und den Datenschutzaufsichtsbehörden konzipiert (31. TB, Tz. 5.5.2). Die Bereiche zur Antrags- und Leistungsfallbearbeitung sind streng voneinander getrennt. Eine strikte Versicherungsspartentrennung ist vorgesehen. Damit wird sichergestellt, dass dem Sachbearbeiter einer Versicherung jeweils nur die erforderlichen Daten übermittelt werden. Auskünfte werden nur an Versicherungen, nicht an Unternehmen anderer Branchen erteilt. Eine Auskunft erfolgt nur, wenn ein berechtigtes Interesse der Versicherung an der Auskunft im Einzelfall vorliegt und keine schutzwürdigen Interessen des Betroffenen entgegenstehen. Abfragen von Versicherungen aus dem HIS werden protokolliert. In einem Stichprobenverfahren wird überprüft, ob diese Abfragen in zulässiger Weise erfolgt sind.

Die Versicherungen informieren bei Vertragsschluss über die Existenz, die Zwecke und die wesentlichen Funktionen des HIS. Bei Einmeldung von Informationen in HIS werden die Betroffenen – also neben Versicherungskunden beispielsweise auch Zeugen oder Geschädigte in einem Versicherungsfall – benachrichtigt. Dies ermöglicht, dass Betroffene frühzeitig bei der IIRFP eine Selbstauskunft einholen können. So lassen sich Fehler im Datenbestand des HIS oder Fehleinschätzungen bei der Einmeldung erkennen und aufklären. Mindestens einmal jährlich können Bürgerinnen und Bürger unentgeltlich eine Selbstauskunft verlangen.

Die regelmäßige Speicherfrist in HIS beträgt vier Jahre und beginnt mit dem Jahr, das der erstmaligen Speicherung folgt. Die Speicherdauer kann sich bei erneuten Einmeldungen innerhalb der vierjährigen Speicherfrist verlängern. Die maximale Speicherdauer beträgt zehn Jahre. Sollten unrichtige Daten in HIS gespeichert sein, müssen diese berichtigt werden. Unzulässig gespeicherte Daten sind zu löschen. Es geht nun darum, darauf zu achten, dass Einmeldungen in HIS nur erfolgen, wenn es zur Verhinderung von Versicherungsbetrug und Versicherungsmissbrauch erforderlich ist, und dass Abrufe aus HIS nur stattfinden, wenn ein berechtigtes Interesse an der Kenntnis der Information glaubhaft dargelegt worden ist und keine schutzwürdigen Interessen des Betroffenen entgegenstehen.

Was ist zu tun?

Von den Aufsichtsbehörden muss kontrolliert werden, ob der Betrieb des HIS entsprechend dem entwickelten Konzept und im gesetzlichen Rahmen erfolgt.

5.1.2 Einwilligungs- und Schweigepflichtentbindungserklärung

Die Aufsichtsbehörden haben mit der Versicherungswirtschaft eine Musterklausel zur Einwilligung in die Erhebung und Verwendung von besonders sensiblen Daten wie Gesundheitsdaten und zur Schweigepflichtentbindung entwickelt.

Mit Beschluss vom 17. Januar 2012 hat der Düsseldorfer Kreis die Mustereinwilligung angenommen. Versicherungsunternehmen müssen nun so schnell wie möglich die vom Bundesverfassungsgericht bereits 2006 für rechtswidrig erklärten Pauschaleinwilligungen (30. TB, Tz. 5.1) ersetzen.

In der Versicherungswirtschaft kann die Erhebung und Verwendung von Gesundheitsdaten erforderlich sein. Naheliegend ist dies bei Kranken- und Lebensversicherungen. Aber auch bei anderen Versicherungen wie der Kfz-Haftpflichtversicherung ist es bei der Bearbeitung eines Unfallschadens unter Umständen notwendig, Gesundheitsdaten zu verwenden. Gesundheitsdaten sind äußerst sensible und deshalb besonders geschützte Daten, deren Verwendung nur unter engen Voraussetzungen erlaubt ist. Da keine allgemeinen gesetzlichen Erlaubnisse für die Erhebung und Verwendung durch Versicherungen bestehen,

benötigen Versicherungen datenschutzrechtliche Einwilligungen. Um wirksam zu sein, müssen diese freiwillig und informiert erteilt werden. Darüber hinaus benötigen Versicherungen Schweigepflichtentbindungserklärungen, um Gesundheitsdaten bei schweigepflichtigen Stellen wie Ärzten erheben zu dürfen, was beispielsweise bei der Prüfung eines Schadens erforderlich sein kann. Lebens- und Krankenversicherungen sind darüber hinaus selbst schweigepflichtig. Um Gesundheitsdaten oder weitere nach § 203 Strafgesetzbuch geschützte Daten wie die Tatsache, dass ein Vertrag mit dieser Versicherung besteht, weitergeben zu dürfen, muss ebenfalls eine wirksame Schweigepflichtentbindungserklärung erteilt worden sein.

In jedem Bundesland besteht eine Behörde, die die Aufsicht über die dort ansässigen Unternehmen führt. Für Schleswig-Holstein nimmt das Unabhängige Landeszentrum für Datenschutz (ULD) die Aufgaben der Aufsichtsbehörde wahr. Sind datenschutzrechtliche Fragen zu klären, die überregional beispielsweise branchenweit eine Vielzahl von Unternehmen, Verbrauchern oder Beschäftigten betreffen, so erfolgt ein Austausch im sogenannten Düsseldorfer Kreis. Hierdurch wird eine einheitliche Linie in der Aufsichtspraxis angestrebt.

http://www.datenschutz.de/aufsicht_privat/

Die Musterklausel wurde als Baukastensystem entwickelt. Für die Versicherungen und ihre Mitarbeiterinnen und Mitarbeiter wurden Hinweise für die Anwendung der Musterklausel erstellt.

- Ein Baustein betrifft die Erhebung, Speicherung und Nutzung von Gesundheitsdaten durch die Versicherung, die der Betroffene selbst mitgeteilt hat. Die Musterklausel bezieht sich dabei ausdrücklich nur auf solche Daten, die erforderlich sind zur Prüfung eines Versicherungsantrags oder zur Begründung, Durchführung oder Beendigung eines Versicherungsvertrages.

Die Erhebung von Gesundheitsdaten durch Versicherungen bei Stellen wie Ärzten ist in § 213 Versicherungsvertragsgesetz (VVG) grundlegend geregelt:

(1) Die Erhebung personenbezogener Gesundheitsdaten durch den Versicherer darf nur bei Ärzten, Krankenhäusern und sonstigen Krankenanstalten, Pflegeheimen und Pflegepersonen, anderen Personenversicherern und gesetzlichen Krankenkassen sowie Berufsgenossenschaften und Behörden erfolgen; sie ist nur zulässig, soweit die Kenntnis der Daten für die Beurteilung des zu versichernden Risikos oder der Leistungspflicht erforderlich ist und die betroffene Person eine Einwilligung erteilt hat.

(2) Die nach Absatz 1 erforderliche Einwilligung kann vor Abgabe der Vertragserklärung erteilt werden. Die betroffene Person ist vor einer Erhebung nach Absatz 1 zu unterrichten; sie kann der Erhebung widersprechen.

(3) Die betroffene Person kann jederzeit verlangen, dass eine Erhebung von Daten nur erfolgt, wenn jeweils in die einzelne Erhebung eingewilligt worden ist.

(4) Die betroffene Person ist auf diese Rechte hinzuweisen, auf das Widerspruchsrecht nach Absatz 2 bei der Unterrichtung.

- Der zweite Baustein betrifft die Abfrage von Gesundheitsdaten bei anderen Stellen. Bei diesen Stellen handelt es sich vor allem um Ärztinnen und Ärzte sowie Krankenhäuser. Eine solche Abfrage kann zur Risikoprüfung im Antragsfall notwendig sein. Außerdem kann es zur Prüfung der Leistungspflicht einer Versicherung erforderlich sein, Angaben eines Versicherten über seinen Gesundheitszustand zu überprüfen. Für diese Einwilligung enthält die Musterklausel eine Wahlmöglichkeit. Die Einwilligung kann für jede Abfrage in der Zukunft „pauschal“ erteilt werden. In diesem Fall wird der Versicherte vor jeder Datenabfrage bei Dritten wie Ärzten unterrichtet. Die Unterrichtung muss darüber informieren, von wem und zu welchem Zweck Daten erhoben werden sollen. Außerdem ist der Versicherte auf sein Widerspruchsrecht und die Möglichkeit, die erforderlichen Unterlagen selbst beizubringen, hinzuweisen. Der Versicherte kann aber auch die Möglichkeit wählen, in jedem Einzelfall zu entscheiden, ob er der konkreten Abfrage von Gesund-

heitsdaten zustimmt oder die erforderlichen Unterlagen beispielsweise aus seiner Krankenakte selbst beibringt.

- Der dritte Abschnitt der Mustereinwilligung betrifft die Weitergabe von Gesundheitsdaten durch Versicherungen.

  Ein Baustein erfasst die Datenweitergabe an medizinische Gutachter. Dies kann für die Prüfung des Risikos bei Antragstellung oder zur Prüfung einer Leistungspflicht erforderlich sein. Der Betroffene ist über eine solche Weitergabe zu unterrichten.

  Ein anderer Baustein betrifft die Übertragung von Aufgaben wie Risikoprüfungen, Leistungsfallbearbeitungen oder telefonische Kundenbetreuung an andere Stellen außerhalb der Versicherung. Die Versicherung hat eine aktuelle Liste über die Unternehmen, an die solche Aufgaben ausgelagert worden sind, mit der Einwilligung zur Verfügung zu stellen. Zudem muss auch später, nach Erteilung der Einwilligung, immer eine aktuelle Liste beispielsweise über das Internet verfügbar sein.

§ 3a Bundesdatenschutzgesetz (BDSG)

Datenvermeidung und Datensparsamkeit

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

Ein weiterer Baustein wurde zur Datenweitergabe an Rückversicherungen entwickelt. Versicherungen schalten Rückversicherungen ein, damit diese das Versicherungsrisiko ganz oder teilweise übernehmen. Rückversicherungen schalten teilweise ihrerseits Rückversicherungen ein. Wegen der verhältnismäßig geringen Zahl an Rückversicherungsunternehmen ist das Risiko hoch, dass Daten aus verschiedenen Versicherungsverhältnissen sich bei dem Rückversicherer konzentrieren und Profilbildungen ermöglichen. Gerade bei sensiblen Gesundheitsdaten sind die schutzwürdigen Interessen der Versicherten besonders zu wahren. Deshalb sind grundsätzlich anonymisierte oder gegebenenfalls pseudonymisierte Daten zu verwenden. Dies entspricht den Grundsätzen der Datenvermeidung und Datensparsamkeit. Nur im Ausnahmefall, wenn eine besondere Erforderlichkeit für die Übermittlung personenbezogener Gesundheitsdaten an Rückversicherer besteht, kann diese zulässig sein. Der Betroffene wird über die Übermittlung seiner Gesundheitsdaten an Rückversicherungen unterrichtet.

Ein weiterer Baustein wurde zur Meldung von Daten an das Hinweis- und Informationssystem der Versicherungswirtschaft (HIS, Tz. 5.1.1) entwickelt. An HIS werden Auffälligkeiten, die auf Versicherungsbetrug hindeuten könnten, und erhöhte Risiken, aber keine Gesundheitsdaten gemeldet. Die Musterklausel enthält ausdrücklich keine Einwilligung zur Weitergabe von Gesundheitsdaten.

§ 203 Strafgesetzbuch (StGB)

Verletzung von Privatgeheimnissen

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt (...),
2. Berufspsychologen (...),
3. Rechtsanwalt (...),
6. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung (...)

anvertraut worden oder sonst bekannt geworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Es wurde nur eine Schweigepflichtentbindungserklärung für schweigepflichtige Versicherungen wie Kranken- und Lebensversicherungen geschaffen. Denn bereits die Information, dass eine Person mit einer solchen Versicherung einen Versicherungsvertrag geschlossen hat, unterfällt nach der Rechtsprechung des Bundesgerichtshofs der strafbewährten Schweigepflicht.

Ein letzter Baustein erfasst die Datenweitergabe an selbstständige Versicherungsvermittler wie beispielsweise Makler. Für die Beratung kann es erforderlich sein, dass der Vermittler Informationen darüber erhält, ob eine Versicherung einen Antrag der Kundin oder des Kunden nur mit Risikozuschlag annimmt oder bestimmte Risiken ausgeschlossen werden. Soweit es erforderlich ist, erfährt der Vermittler, dass und mit welchem Inhalt der Vertrag abgeschlossen wurde. Dabei erfährt er auch, ob Risikozuschläge oder Ausschlüsse bestimmter Risiken vereinbart wurden. Wechselt der betreuende Vermittler, etwa wegen Geschäftsaufgabe, ist die oder der Versicherte vor der Weitergabe von Gesundheitsdaten an einen anderen Vermittler zu informieren und auf die Widerspruchsmöglichkeit hinzuweisen.

- Der vierte Abschnitt der Musterklausel betrifft die Speicherung und Verwendung von Gesundheitsdaten für den Fall, dass der Vertrag nicht zustande kommt. Die Speicherfrist beträgt drei Jahre. Hintergrund ist vor allem die Betrugs- und Missbrauchsprävention, für die die Speicherung und der Austausch über nicht zustande gekommene Verträge von der Versicherungswirtschaft für erforderlich gehalten wird.

Was ist zu tun?

Versicherungen, die Gesundheitsdaten verwenden, haben diesen Datenumgang unverzüglich auf eine tragfähige Rechtsgrundlage zu stellen. Hierfür können sie die von dem GDV gemeinsam mit den Aufsichtsbehörden entwickelte Mustererklärung verwenden. Die Versicherungen müssen die in der Mustererklärung vorgegebenen Prozesse zur Unterrichtung des Betroffenen umsetzen. Die Aufsichtsbehörden begleiten und überprüfen das Umsetzungsverfahren.

5.1.3 Verhaltensregeln – der „Code of Conduct“

Die Versicherungswirtschaft ist in Deutschland die erste Branche, die zur Förderung der Beachtung datenschutzrechtlicher Regelungen nach § 38a BDSG förmlich anerkannte Verhaltensregeln erlassen hat.

Die Arbeit der Datenschutzaufsichtsbehörden und der Versicherungswirtschaft an den Verhaltensregeln der Versicherungswirtschaft (Code of Conduct; 31. TB, Tz. 5.5.1) sind im Berichtszeitraum wieder aufgenommen und 2012 abgeschlossen worden. Der Berliner Beauftragte für den Datenschutz und die Informationsfreiheit hat deren Vereinbarkeit mit dem Datenschutzrecht festgestellt. Die Verhaltensregeln sollen die abstrakten Regelungen der Datenschutzgesetze mit Blick auf die Abläufe in der Versicherungsbranche konkretisieren und ergänzen. Versicherungsunternehmen sollen hinsichtlich der gesetzlichen Erlaubnisse zur Verwendung von Versichertendaten Sicherheit gewinnen. Der Einsatz von Einwilligungen soll, wo nicht erforderlich, ausgeschlossen werden. Erforderlich ist er bei der Verarbeitung von besonders sensiblen Daten wie Gesundheitsdaten (Tz. 5.1.2), bei der Werbung sowie der Markt- und Meinungsforschung.

Die Verhaltensregeln enthalten Vorgaben zur Qualität der Datenerhebung, zur Datenerhebung beim Betroffenen und zur Erhebung ohne dessen Mitwirkung, zu den jeweiligen Informationspflichten, zu Transparenzvorgaben und Einwilligungen, zu gemeinsamen Datenverarbeitungen innerhalb von Unternehmensgruppen, zum Datenaustausch mit anderen Versicherern, zum Hinweis- und Informationssystem, zu Datenübermittlungen an selbstständige Vermittler sowie an Rückversicherer, zur Auftragsdatenverarbeitung und Funktionsübertragung, zur Markt- und Meinungsforschung, zur Aus-

kunft, Berichtigung, Löschung und Sperrung, zur Datensicherheit sowie zur Meldung von Datenlecks, der sogenannten Breach Notification. Die Verhaltensregeln enthalten keine Konkretisierungen zu Werbung, Bonitätsabfragen und Scoring in der Versicherungswirtschaft.

Was ist zu tun?

Die Vorgaben der Verhaltensregeln für die Versicherungswirtschaft sollten branchenweit umgesetzt werden. So wird für die Versicherungen wie auch für die Betroffenen ein Mehrwert an Rechtssicherheit geschaffen.

5.2 Geldkarten mit Funkchips

Seit August 2012 geben schleswig-holsteinische Sparkassen die „SparkassenCard kontaktlos“ an Kundinnen und Kunden aus. Diese Geldkarten sind mit Funkchips ausgestattet. Das ULD sieht vor allem in Hinblick auf die Datensicherheit Nachbesserungsbedarf.

Mithilfe der Funkchips soll die sogenannte Near Field Communication (NFC), also die kontaktlose Kommunikation, ermöglicht werden. Einsatzbereich soll wie bei den klassischen Geldkartenfunktionalitäten vorrangig das Bezahlen von Kleinbeträgen, z. B. beim Kauf von Fahrkarten, sein. Kundinnen und Kunden sollen ihre Geldkarten nicht mehr in ein Kartenlesegerät stecken müssen; es genügt, diese nahe an ein Lesegerät zu halten. Das ULD sieht die Einführung der NFC-Technologie u. a. durch schleswig-holsteinische Banken kritisch. Auch in anderen Bundesländern erfolgte im Jahr 2012 die Einführung. Zwar scheint die Kommunikation für die Bezahltransaktionen als solche ausreichend abgesichert zu sein. Die Informationen, wann ein Karteninhaber wo kontaktlos eingekauft hat, sind nach dem derzeitigen Stand aber weitgehend ungeschützt. Eine vollständige Technikfolgenabschätzung wurde selbst nach dem Start der Einführung nicht vorgelegt. Von den verantwortlichen Stellen kann so nicht auf eine verbindliche Datenschutzkonzeption verwiesen werden.

Das ULD kritisiert folgende Mängel in Bezug auf die technische und organisatorische Sicherheit der Geldkarten mit NFC-Funktion:

- Die auf den Geldkarten mit NFC-Funktion gespeicherten Transaktionsdaten (Logs der letzten drei Lade- bzw. Entlade- und der letzten 15 Abbuchungs- bzw. Rückbuchungstransaktionen mit Datum, Zeit, Händlerkartennummer, gezahltem Betrag und Restbetrag) und eine eindeutige Kartennummer können ohne zusätzliche Prüfung einer Zugriffsberechtigung und ohne eine explizite Autorisierung durch die Inhaberin oder den Inhaber der Geldkarte (PIN-Code, Schlüssel, Kennwort …) ausgelesen werden. Der Abruf der Daten wird durch die Karte selbst nicht protokolliert, sodass auch eine nachträgliche Überprüfung und Feststellung der Datenübermittlungen und der empfangenden Stellen durch die Inhaberin oder den Inhaber der Karte nicht möglich ist. Die gesetzlichen Vorgaben für die Verarbeitung personenbezogener Daten verpflichten grundsätzlich dazu, jeweils die Abrufberechtigung zu prüfen und die erfolgten Abrufe zu protokollieren. Diese Vorgaben werden nicht eingehalten. Dies ist für das ULD nicht nachvollziehbar, weil die verwendeten Kartensysteme durchaus zur Durchführung kryptografisch sicherer Datenverarbeitung und -übermittlung in der Lage sind und bereits Mechanismen zur vorherigen Autorisierung der Datenverarbeitung durch die Karteninhaberin oder den Karteninhaber vorsehen.
- Gegen das unbefugte Auslesen der Transaktionsdaten und der eindeutigen Kartennummer durch Dritte werden seitens der Banken lediglich Maßnahmen genannt, die die Nutzung der NFC-Schnittstelle behindern oder einschränken. Sowohl die – aktuell noch nicht zur Verfügung stehende – Möglichkeit, dass Kundinnen und Kunden die NFC-Schnittstelle auf den Karten selbst deaktivieren oder fallweise aktivieren

können, als auch die Nutzung von Metallschutzhüllen, die ein unbefugtes Auslesen über die NFC-Schnittstelle erschweren, verringern nur teilweise die Risiken, die aus dem nicht ausreichenden technischen Zugriffsschutz entstehen. Eine Stellungnahme, die auf nachvollziehbaren Tests mit aktuell zur Verfügung stehender Infrastruktur wie spezialisierte Antennen, höherer Feldstärke oder passives Mitschneiden eines stattfindenden Auslesevorgangs basiert, sowie eine Bewertung seitens der Banken liegt nicht vor.

In Kenntnis der aktuellen Datenschutz- und Sicherheitskonzeption der Geldkarten mit NFC-Schnittstellen kommt das ULD zu den folgenden Schlussfolgerungen und Empfehlungen:

- Die Geldkarte mit NFC-Funktion ist gegen das unbefugte Auslesen der Transaktionsdaten und der eindeutigen Kartennummer nicht ausreichend gesichert. Inhaberinnen und Inhaber von Geldkarten mit NFC-Funktion sollten daher mit der Geldkarte nur Transaktionen durchführen, die nicht weitere Rückschlüsse auf Sachverhalte der Intim- oder Privatsphäre zulassen. Selbst wenn die NFC-Funktion nicht für Transaktionen eingesetzt wird, bleibt die eindeutige Kartennummer auslesbar.
- Die weitere Produktion von Geldkarten mit NFC-Schnittstelle ohne verbesserte Absicherung der Transaktionsdaten und der eindeutigen Kartennummer sollte unterbleiben. Stattdessen sollten in einer hinreichend langen Pilotphase in einem begrenzten Gebiet Lösungen insbesondere unter den Gesichtspunkten der Kunden- und Datenschutzfreundlichkeit gesucht und entwickelt werden. Die Banken müssen schnellstmöglich eine Erweiterung der Geldkarten um eine von der Inhaberin oder dem Inhaber der Geldkarte explizit zu autorisierende Auslesemöglichkeit und Löschmöglichkeit der Transaktionen ergänzen. Diese Funktion sollte auch bei Geldkarten ohne NFC-Schnittstelle im Rahmen des regelmäßigen Austausches der Geldkarten nachgerüstet werden.
- Für die aktuell produzierten oder bereits im Einsatz befindlichen Geldkarten mit NFC-Schnittstelle muss den Inhaberinnen und Inhabern unaufgefordert eine Darstellung der mit der Nutzung verbundenen Risiken und der empfohlenen Schutzmaßnahmen sowie technische Funktionen zur fallweisen Aktivierung der NFC-Schnittstelle oder übergangsweise physikalische Schutzmaßnahmen gegen das unberechtigte Auslesen, z. B. metallene Schutzhüllen, zur Verfügung gestellt werden.
- Die Banken müssen die bisher fehlende Risikoanalyse und -bewertung nachholen und sollten diese mit den Aufsichtsbehörden der Länder diskutieren. Zusätzlich sollten die Banken zukünftig frühzeitig bereits in der Designphase und vor allem vor Aufnahme der Produktion eine datenschutzrechtliche sowie sicherheitstechnische Bewertung von Zahlungssystemen veranlassen und mit den Datenschutzaufsichtsbehörden abstimmen. Dies gilt insbesondere auch für andere in der Planung oder bereits im Betrieb befindliche Zahlungssysteme unter Nutzung der NFC-Schnittstelle, z. B. Bezahlung per NFC-Schnittstelle mit Smartphones oder Verwendung der NFC-Schnittstelle bei Kreditkarten.

Was ist zu tun?

Beim Einsatz von „Near Field Communication“ (NFC)-Technologie in Geldkarten und anderen Zahlungssystemen muss insbesondere bezüglich der Datensicherheitsvorkehrungen durch die verantwortlichen Stellen, wie z. B. die Banken, deutlich nachgebessert werden.

5.3 Elektronisches Lastschriftverfahren – der Kunde bezahlt mit seinen Daten

Beim Elektronischen Lastschriftverfahren sammeln die von den Händlern beauftragten Netzbetreiber Daten zum Einkaufsverhalten, um vermeintlich „riskante Kunden" zu identifizieren und Rücklastschriften sowie betrügerische Handlungen zu verhindern.

Wir berichteten über die langen Kassenzettel im Elektronischen Lastschriftverfahren (ELV), die Kundinnen und Kunden z. B. an Supermarktkassen zur Unterschrift vorgelegt werden (33. TB, Tz. 5.3). Diese Kassenzettel und die sich dahinter verbergenden Datenverarbeitungsverfahren stießen auf Kritik bei Verbraucher- und Datenschützern. Das ULD hält die derzeit eingesetzten Verfahren weder für datenschutzrechtlich zulässig noch für alternativlos.

Beim Lastschriftverfahren trägt der Händler das Risiko, dass das Konto der Kundin bzw. des Kunden nicht gedeckt ist. Allerdings ist es für die Händler gegenüber dem EC-Cash-Verfahren kostengünstiger, bei dem durch die Eingabe der PIN eine Online-Überprüfung des Kartenkontos stattfindet und bei ausreichender Kontodeckung und Kartengültigkeit eine Zahlungsgarantie für den Händler erteilt wird. Die Abwicklung erfolgt in beiden Fällen über Dienstleister, sogenannte Netzbetreiber. Diese haben Systeme zur Identifizierung des Risikos von Forderungsausfällen geschaffen. Diese Systeme nutzen vor allem Daten aus ELV-Zahlungsvorgängen. Im ELV werden aus der EC-Karte bei Transaktionen Bankleitzahl, Kontonummer, Kartenverfallsdatum und die sogenannte Kartenfolgenummer ausgelesen und zusammen mit Daten zu der Transaktion – u. a. Höhe der Forderung, Zeitpunkt und Ort der Zahlung – an den jeweiligen Netzbetreiber zur Zahlungsabwicklung übermittelt. Nach den Erkenntnissen der Aufsichtsbehörden gleichen Netzbetreiber die ihnen von den Händlern übermittelten Datensätze zu Zahlungsvorgängen mit bei ihnen vorliegenden Datenbeständen ab und treffen eine Aussage darüber, welche Zahlungsempfehlung – Lastschrift- oder EC-Cash-Verfahren – dem Händler gegeben wird.

Sammelt eine zentrale Stelle Informationen zu Transaktionen bei unterschiedlichen Händlern, um sie für die Übermittlung an weitere Unternehmen wie Händler zu nutzen, nimmt die Stelle die Funktion einer Auskunftei wahr. Für die sogenannte Einmeldung von Negativdaten wie Informationen über Rücklastschriften im ELV müssen die gesetzlichen Voraussetzungen erfüllt sein.

§ 28a Bundesdatenschutzgesetz (BDSG)

Datenübermittlung an Auskunfteien

(1) Die Übermittlung personenbezogener Daten über eine Forderung an Auskunfteien ist nur zulässig, soweit die geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist, die Übermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten erforderlich ist und

1. die Forderung durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden ist oder ein Schuldtitel nach § 794 der Zivilprozessordnung vorliegt,

2. die Forderung nach § 178 der Insolvenzordnung festgestellt und nicht vom Schuldner im Prüfungstermin bestritten worden ist,

3. der Betroffene die Forderung ausdrücklich anerkannt hat,

4.

a) der Betroffene nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist,

b) zwischen der ersten Mahnung und der Übermittlung mindestens vier Wochen liegen,

c) die verantwortliche Stelle den Betroffenen rechtzeitig vor der Übermittlung der Angaben, jedoch frühestens bei der ersten Mahnung über die bevorstehende Übermittlung unterrichtet hat und

d) der Betroffene die Forderung nicht bestritten hat oder

5. das der Forderung zugrunde liegende Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und die verantwortliche Stelle den Betroffenen über die bevorstehende Übermittlung unterrichtet hat.

…

Es muss sich insbesondere um eine fällige Forderung handeln, die beispielsweise durch ein Urteil festgestellt oder u. a. zweimal schriftlich angemahnt worden ist. Diese Voraussetzungen erfüllt die bloße Rücklastschrift nicht. Netzbetreiber dürfen also generell keinen Pool von Negativinformationen unterschiedlicher Händler ansammeln.

Die händlerübergreifende Sammlung von Positivdaten zum Einkaufsverhalten von Kundinnen und Kunden, die aus Zahlungen mittels ELV stammen, kann erst recht nicht datenschutzrechtlich zulässig sein. Hierdurch werden alle Kundinnen und Kunden unter einen Generalverdacht gestellt. Es wird zwar behauptet, diese Datensammlung diene nur der Missbrauchsbekämpfung im ELV. Diese Behauptung ist aber zum einen nicht belegt. Zum anderen kann dieser Zweck mit anderen Mitteln erreicht werden. Der Einsatz gestohlener EC-Karten könnte z. B. über stichprobenhafte Personalausweiskontrollen an der Kasse erkannt und auch präventiv abgewehrt werden. Unstreitig ist, dass Händler die polizeiliche KUNO-Datei zu verloren gegangenen EC-Karten nutzen dürfen. Der Gefahr ungedeckter Konten kann durch einen zufälligen Wechsel zwischen dem EC-Cash- und dem Elektronischen Lastschriftverfahren begegnet werden. Die Entscheidung darüber, welches Bezahlverfahren der Händler der Kundin bzw. dem Kunden anbietet, kann auch von dem zu bezahlenden Betrag abhängig gemacht werden. Diese Betragsgrenze könnte beispielsweise abhängig von Filialstruktur, Wochentag und Uhrzeit unterschiedlich gesetzt werden. Unbenommen bleibt, dass Händler ihre eigenen Rücklastschrifterfahrungen so lange nutzen und die Kundin bzw. den Kunden für das riskante Lastschriftverfahren sperren, bis die Forderung beglichen ist (33. TB, Tz. 5.3).

Kundinnen und Kunden müssen in jedem Fall vor einer Datenverarbeitung zuverlässig Kenntnis darüber erhalten können, welche Daten zu welchem Zweck verwendet werden. Eine Information allein auf der Rückseite des Kassenbelegs, der beim ELV erst nach der Entscheidung für ein Bezahlverfahren und nach der Datenverarbeitung ausgehändigt wird, erfüllt diese Voraussetzungen nicht. Die Kundeninformation hat in einer verständlichen Sprache zu erfolgen.

Von den Netzbetreibern müssen weniger datenverarbeitungsintensive Verfahren realisiert werden. Über die letztlich verantwortlichen Händler, die auf dem Markt ihren Netzbetreiber und dessen Dienstleistungen auswählen, kann auf deren Angebot Einfluss genommen werden. Auch die Kundinnen und Kunden können durch die Wahl des Bezahlwegs Einfluss nehmen; bei Bargeldzahlungen fallen keine elektronischen Spuren an.

Was ist zu tun?

Das Elektronische Lastschriftverfahren und die Systeme zur Identifizierung von Forderungsausfallrisiken müssen grundlegend überarbeitet und rechtskonform gestaltet werden.

5.4 Geldwäsche nicht um jeden Preis

Ein Regierungsentwurf zur Änderung des Geldwäschegesetzes hätte zum Ausschluss des anonymen elektronischen Einkaufens und Bezahlens geführt. Eine derart tief greifende Geldwäscheprävention stünde zu den festgestellten Risiken außer Verhältnis.

Mit einem Gesetzentwurf zur „Optimierung der Geldwäscheprävention“ plante die Bundesregierung, dass die Nutzenden von elektronischem Geld verpflichtet werden, sich zu identifizieren, auch wenn eine elektronische Aufladung von Bagatellbeträgen erfolgt. Verkaufsstellen waren als Adressaten einer neuen Regelung vorgesehen, die im Falle der Herausgabe von Coupons, Chips, Gutscheinen sowie Prepaidkarten gegen Bargeld eine Identifizierung der Käuferin bzw. des Käufers vornehmen sollten. Im Gesetzentwurf war hierfür kein Schwellenwert festgelegt; die Verkäufer wären verpflichtet worden, eine Identifizierung bereits ab einem Cent vorzunehmen. Die Aufnahme einer solchen Bestimmung wäre aus Datenschutzsicht unverhältnismäßig gewesen.

Der Verzicht auf jeglichen Schwellenwert wird selbst von Fachleuten für Geldwäscheprävention

nicht gefordert. Die Financial Action Task Force on Money Laundering (FATF), ein zwischenstaatliches Gremium bei der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD), erarbeitet internationale Standards zur Bekämpfung der Geldwäsche und Terrorismusfinanzierung und entwickelt diese weiter. Die FATF wies in einem Report darauf hin, dass sogenannten New Payment Products erhöhte Aufmerksamkeit geschenkt werden muss, da diese neue Zahlungsmethoden nutzen. Das Bundeskriminalamt (BKA) hatte in seinem Jahresbericht für das Jahr 2009 lediglich 63 Tatverdächtige der Geldwäsche ermittelt, die internetbasierte Zahlungssysteme und deren anonyme Nutzungsmöglichkeiten verwendeten. Vor diesem Hintergrund empfahl das BKA gerade nicht, Geldwäscheprävention bereits beim Einsatz von Bagatellbeträgen zu praktizieren.

Ein Wegfall von Schwellenwerten ist auch nicht europarechtlich gefordert. So wird durch die gültige Richtlinie eine Identifizierung von Käufern nicht für zwingend erachtet, sofern der auf dem Datenträger gespeicherte Betrag – falls der Datenträger nicht wieder aufgeladen werden kann – nicht mehr als 150 Euro beträgt oder sofern – falls der Datenträger wieder aufgeladen werden kann – sich der in einem Kalenderjahr insgesamt abgewickelte Betrag auf nicht mehr als 2.500 Euro beläuft, außer wenn ein Betrag von 1.000 Euro oder mehr in demselben Kalenderjahr von dem Inhaber zurückgetauscht wird.

Der Regierungsentwurf stand auch im Widerspruch zum Telemediengesetz. Anbieter von Leistungen via Internet haben demnach die Verpflichtung, die Nutzung ihrer Angebote und deren Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Hierüber sind die Internetnutzer von dem Anbieter der Leistungen zu unterrichten. Die Anbieter können ihrer gesetzlichen Verpflichtung zur Ermöglichung einer anonymen Bezahlweise nicht mehr nachkommen, wenn sie grundsätzlich eine Identifizierung und die kontinuierliche Überwachung der Geschäftsbeziehung sicherstellen sollen.

https://www.datenschutzzentrum.de/presse/20110701-geldwaeschepraevention.htm

Unsere Kritik am Regierungsentwurf wurde im Gesetzgebungsverfahren aufgenommen. Es wurde eine Ausnahme von der Identifizierungspflicht vorgesehen, soweit die E-Geldbeträge 100 Euro pro Kalendermonat oder weniger betragen und sichergestellt ist, dass das ausgegebene E-Geld nicht mit dem E-Geld eines anderen E-Geld-Inhabers verbunden werden kann, die Identifizierungspflichten ab Überschreiten eines Betrags von 20 Euro beim Rücktausch in Bargeld eingehalten werden und beim Wiederaufladen des E-Geld-Trägermediums pro Kalendermonat die Höchstbetragsgrenze von 100 Euro eingehalten wird. Die Bekämpfung von Geldwäsche macht keinen Sinn, wenn selbst bei Centbeträgen eine Identifizierung der Käuferin oder des Käufers und eine Überwachung der Geschäftsbeziehungen erfolgen müssten. Ein Verzicht auf Schwellenwerte verstößt gegen das verfassungsrechtlich verankerte Gebot, anonyme und pseudonyme Online-Dienste zu ermöglichen.

Was ist zu tun?

Der Gesetzgeber ist aufgerufen, sich auch künftig für den Schutz von Schwellenwerten einzusetzen.

5.5 Der gläserne Mietinteressent

Hinsichtlich der Einholung von Informationen über Mietinteressenten vor der Vermietung von Wohnraum inklusive Bonitätsabfragen ist eine bundesweite Gesamtlösung noch nicht in Sicht.

Das ULD ist schon länger mit der Praxis der Wohnwirtschaftsbranche befasst, vor der Wohnraumvermietung eine Bonitätsauskunft über den Mietinteressenten bei Auskunfteien einzuholen (33. TB, Tz. 5.4). Die Auskunft zu einem Mietinteressenten darf erst dann eingeholt werden, wenn der Abschluss des Mietvertrags mit diesem Bewerber nur noch vom positiven Ergebnis der Bonitätsprüfung abhängt. Grundsätzlich haben Vermieter ein berechtigtes Interesse, solche Auskünfte einzuholen, um das Risiko der Zahlungs-

unfähigkeit oder -unwilligkeit des Mietinteressenten bereits vor Vertragsabschluss abschätzen zu können. Datenschutzrechtlich unzulässig ist es aber, zu einer Vielzahl von Mietinteressenten solche Auskünfte parallel einzuholen, ohne dass ein konkreter Vertragsschluss ins Auge gefasst wird.

Die Aufsichtsbehörden für den Datenschutz haben im November 2011 mit Vertretern der Wohnwirtschaftsbranche und der Auskunfteien die Praxis der Bonitätsabfragen eingehend erörtert. Wir machten dabei deutlich, dass ein Datenabruf nicht pauschal zu einer Mehrheit von Mietinteressenten erfolgen darf. Abrufe zu weiteren Interessenten sind erst dann zulässig, wenn die Bonitätsabfrage zu dem zuerst ausgewählten Bewerber ein negatives Ergebnis zutage fördert. Die Wohnwirtschaftsbranche hat den Aufsichtsbehörden bis heute keine akzeptable Gesamtlösung für das gesamte Bundesgebiet vorgelegt, welche die datenschutzrechtlichen Forderungen der Aufsichtsbehörden berücksichtigt. Das ULD wird unabhängig davon die Auswahlpraxis der Wohnwirtschaftsunternehmen bezüglich der Mietinteressenten auch weiterhin kontrollieren.

Was ist zu tun?

Vermieter haben kein berechtigtes Interesse, Bonitätsinformationen zu einer nicht näher bestimmbaren Anzahl von Mietinteressenten bei den Auskunfteien zu erfragen. Die Vermieter müssen gegebenenfalls ihre Geschäftsmodelle an das geltende Datenschutzrecht anpassen.

5.6 Einwilligungen, Bonitätsabfragen und öffentlicher Personennahverkehr

Bonitätsabfragen durch Verkehrsbetriebe des öffentlichen Personennahverkehrs sind zumeist nicht zulässig.

Überzogene Bonitätsabfragen sind in vielen Wirtschaftsbereichen eine weitverbreitete Unart (Tz. 5.5; 33. TB, Tz. 5.4, 5.5; 32. TB, Tz. 5.4, 5.7.8). In dem von einem verantwortlichen Nahverkehrsbetrieb erstellten Antragsformular für eine Abonnementkarte war eine Einwilligungserklärung enthalten, in der sich der Antragsteller per Unterschrift damit einverstanden erklärte, dass seine personenbezogenen Daten zwecks Bonitätsabfrage an ein Inkassounternehmen übermittelt werden.

Diese vorformulierte Einwilligungserklärung stellte keine wirksame Legitimation für die Verwendung der personenbezogenen Daten dar. Eine datenschutzrechtlich wirksame Einwilligung muss freiwillig abgegeben werden. Die Freiwilligkeit war wegen der Kopplung verschiedenartiger Erklärungen hier nicht gegeben. Bei der verantwortlichen Stelle handelt es sich um ein Unternehmen, das im öffentlichen Personennahverkehr für die Sicherstellung einer ausreichenden Versorgung der Bevölkerung verantwortlich ist. Der sich daraus ergebende gesetzliche Auftrag der Daseinsvorsorge stand der gekoppelten Einwilligungserklärung entgegen.

Es gibt auch keine gesetzliche Rechtsgrundlage für die Bonitätsabfrage. Die nach dem Bundesdatenschutzgesetz in Betracht kommenden Regelungen setzen voraus, dass die Bonitätsabfrage erforderlich ist. Folgende Aspekte waren für die Bewertung des ULD ausschlaggebend:

- Allgemeines Geschäftsrisiko: Ein gewisser Zahlungsausfall stellt für sich genommen ein allgemeines Geschäftsrisiko dar, das keine Bonitätsabfrage rechtfertigt. Eine Bonitätsabfrage bei einer Auskunftei ist gesetzlich nur vorgesehen, wenn das Unternehmen eine wesentliche Vorleistung erbringt und damit ein finanzielles Ausfallrisiko hat und zugleich die schutzwürdigen Interessen der Betroffenen nicht überwiegen (32. TB, Tz. 5.7.8). Dabei ist zu berücksichtigen, dass die Unternehmen durch die Gestaltung der Geschäftsmodelle, der Abläufe und der Vertragsbedingungen den Umfang der Vorleistung steuern können. Unternehmen können einem finanziellen Ausfallrisiko durch die Verkleinerung von Vorleistungen entgegenwirken,

z. B. durch Vorabkasse für quartalsweise verschickte Monatskarten.

- Nachteile für den Betroffenen: Die Bonitätsabfragen können Nachteile für den Betroffenen begründen: Jede Abfrage hinterlässt Informationen bei der Auskunftei über den Betroffenen, die wiederum auf spätere Abfragen einwirken können. Eine hohe Anzahl von Abfragen allein kann schon zu dem unzutreffenden Schluss führen, die oder der Betroffene sei nicht in der Lage, Verbindlichkeiten zu erfüllen. Das kann zur Folge haben, dass die oder der Betroffene – etwa beim Scoring – grundlos schlechter bewertet wird und z. B. eine Finanzierung oder Vertragsschlüsse verweigert bekommt.
- Gesetzlicher Auftrag: Die verantwortliche Stelle nimmt mit Beförderungsleistungen aus dem Grundgesetz abzuleitende staatliche Pflichten zur Daseinsvorsorge wahr. Die Sicherstellung einer ausreichenden Versorgung der Bevölkerung mit Verkehrsleistungen im öffentlichen Personennahverkehr steht tendenziell einer Bonitätsabfrage entgegen.
- Bagatellbereich: Ein finanzielles Risiko der verantwortlichen Stelle im Bagatellbereich ist verhältnismäßig und damit hinnehmbar. Über die geltenden Tarifbestimmungen kann eine verantwortliche Stelle ihr Recht wahren, den Vertrag im Falle der Nichtzahlung fristlos zu kündigen.
- Ungeeignetheit: Bonitätsabfragen sind oft nicht geeignet, ein angenommenes Risiko zu unterbinden. Es kann auch bei den Antragstellern, die mit einer positiven Bonität ausgewiesen wurden, zu ausbleibenden Zahlungen kommen.

Die verantwortliche Stelle hat dem ULD zugesichert, keine Bonitätsabfragen mehr durchführen zu wollen. Das Verfahren ist abgeschlossen.

Was ist zu tun?

Bonitätsabfragen durch Unternehmen, die Leistungen im Bereich des öffentlichen Personennahverkehrs erbringen, sind bei überwiegenden schutzwürdigen Interessen der Betroffenen nicht zulässig.

5.7 Orientierung in der Datenwolke

Durch eine über Netze verbundene Rechnerlandschaft wird die unternehmensinterne Datenverarbeitung im Wege des Cloud Computing ausgelagert. Eine Orientierungshilfe für die Privatwirtschaft präzisiert die datenschutzrechtlichen Anforderungen für Cloud Computing.

Oft werden eine oder mehrere IT-Dienstleistungen – Infrastruktur, Plattformen, Anwendungssoftware – aufeinander abgestimmt, schnell dem tatsächlichen Bedarf angepasst und nach tatsächlicher Anwendung abrechenbar über ein Netz bereitgestellt. Von Vorteil sind die gezielte Nutzung von Rechenkapazitäten, die verbrauchsabhängige Abrechnung, die Einsparpotenziale durch Verzicht auf teure Hardware und die globale Verfügbarkeit der Dienstleistungen. Durch die Auslagerung der Datenverarbeitung an sogenannte Cloud-Anbieter, die im Auftrag der Cloud-Anwender die Datenverarbeitung übernehmen, entstehen Fragen zur Wahrung der Rechte von Betroffenen, z. B. der Rechte auf Berichtigung oder Löschung unrichtiger personenbezogener Daten, Fragen zur Einhaltung der Datensicherheit oder zu den Anforderungen einer zulässigen internationalen Datenverarbeitung.

Das ULD hat zusammen mit einigen anderen Datenschutzaufsichtsbehörden eine Orientierungshilfe für die Privatwirtschaft erarbeitet und darin die Risiken, Chancen und datenschutzrechtlich relevanten Aspekte des Cloud Computing dargestellt. Wesentlich ist zunächst die Feststellung, dass der Cloud-Anwender als Auftraggeber für die Wahrung der Betroffenenrechte, für die Durchführung von Datensicherheitsmaßnahmen – letztlich für die gesamte Datenverarbeitung – verantwortlich bleibt. Verstöße der Cloud-Anbieter gegen datenschutzrechtliche Vorschriften muss er sich zurechnen lassen.

Zwischen Cloud-Anwender und Cloud-Anbieter liegt in der Regel eine Auftragsdatenverarbeitung vor, wobei der Cloud-Anbieter sorgfältig ausgewählt werden muss. Da die Auswahl mit haftungsrechtlichen Risiken verbunden ist und auch nach der Auswahl eine ständige Kontrolle des Cloud-Anbieters erfolgen muss, sollte der Anbieter geeignete Nachweise für seine Fachkompetenz und Zuverlässigkeit vorlegen, wie etwa Nachweise zu Zertifizierungen bzw. Datenschutz-Gütesiegel.

Die Datenverarbeitung in einer innereuropäischen Cloud ist gegenüber der in einer außereuropäischen Cloud vorzuziehen. In der außereuropäischen Cloud kann die Einhaltung europäischen Datenschutzrechts schwerer kontrolliert werden, Datenschutzstandards beim Anbieter sind möglicherweise nicht gewährleistet, sodass für die Cloud-Anwender höhere Haftungsrisiken bestehen (Tz. 11.3).

Die Orientierungshilfe ist abrufbar unter:

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

Was ist zu tun?

Der für die gesamte Datenverarbeitung verantwortlich bleibende Cloud-Anwender muss bei der Auswahl der Cloud-Anbieter einen hohen Sorgfaltsmaßstab anwenden und sich geeignete Nachweise zur Einhaltung der Anforderungen an Datenschutz und Datensicherheit vorzeigen lassen.

5.8 Dopingbekämpfung

Die Dopingbekämpfung bei Spitzensportlerinnen und -sportlern steht zum Datenschutz in einem Spannungsverhältnis, da die Anwendung der weltweit geltenden Regeln in Deutschland beim Meldesystem, bei den Tests wie bei Verstößen wenig Rücksicht auf informationelle Selbstbestimmung nimmt.

Schleswig-Holstein ist in einigen Sportarten nicht nur in Deutschland, sondern weltweit an der Spitze. Einige Sportler trugen gegenüber dem ULD vor, dass sie einem Meldesystem und Dopingkontrollen ausgesetzt sind, was mit ihrer Menschenwürde nur schwer in Einklang zu bringen sei. Um an internationalen Wettkämpfen teilnehmen zu dürfen, müssten sie sich den Anti-Doping-Regeln der World Anti-Doping Agency (WADA) und der Nationalen Anti Doping Agentur (NADA) unterwerfen. An dem Anti-Doping-System sind in Deutschland neben der NADA der Deutsche Olympische Sportbund (DOSB), sämtliche Landessportverbände, die Sportfachverbände und die international aktiven Sportvereine als Anti-Doping-Organisationen (ADO) beteiligt.

Ziel des Anti-Doping-Systems ist die Herstellung von fairen gleichen Bedingungen beim internationalen Spitzensport und der Gesundheitsschutz der Sportlerinnen und Sportler durch die Kontrolle der Einnahme von leistungsfördernden Mitteln – des Dopings. Da diese Einnahme nicht nur während der Wettkämpfe, sondern auch vorher und während des Trainings erfolgt und Wirkung hat, verfolgen die WADA, die NADA sowie die sonstigen ADO – zumindest nach außen hin – eine Nulltoleranzstrategie: Sportlerinnen und Sportler müssen zu jeder Tageszeit – außer in der Nacht zwischen 23 und 6 Uhr – und an jedem Tag für Dopingkontrollen, dies sind zumeist Entnahmen von Urin und eventuell von Blut, zur Verfügung stehen. Hierfür müssen sie jeweils drei Monate im Voraus ihren Aufenthaltsort und ihre Erreichbarkeit im weltweiten, in Kanada gehosteten Meldesystem ADAMS (Anti Doping Management System) eingeben. Die Dopingkontrolleure dringen bei den Tests teilweise in den intimsten Freundes- und Familienkreis ein. Um Betrug zu verhindern, kontrollieren die Tester, „wie die Probe den Körper des Athleten" verlässt. Dies gilt auch für Jugendliche unter 16 Jahren, diese dürfen aber derartige Intimbeobachtungen ablehnen. Kommt ein Sportler seinen Meldepflichten nicht nach, wird er von Kontrolleuren nicht angetroffen oder besteht ein Verdacht auf Einnahme unerlaubter Mittel, so sind Sanktionen möglich, mit denen in der Regel eine Vielzahl von Datenübermittlungen einhergehen. Bei Verstößen gegen Anti-Doping-Bestimmungen kann die Öffentlichkeit informiert werden. Die Beschwerde führenden Sportler wenden sich nicht gegen Dopingkontrollen generell, sondern gegen

die damit verbundenen unverhältnismäßigen Eingriffe in ihre Privatsphäre sowie auch gegen die teilweise äußerst unterschiedliche, willkürlich erscheinende Kontrollpraxis.

Gemeinsam mit dem Landesbeauftragten für den Datenschutz Rheinland-Pfalz erstellte das ULD eine eingehende Analyse der bestehenden Regeln und des praktizierten Verfahrens. Diese kommt zu dem Ergebnis, dass die eingeholten Einwilligungen nach deutschem Recht unwirksam sind, weil die Sportler nicht hinreichend informiert und die Einwilligungen nicht freiwillig sind, dass die Kontrollen unverhältnismäßig sind und teilweise zu stark in den Intimbereich eindringen und dass hierfür keine Rechtsgrundlagen bestehen. Gemeinsam schlugen wir den Erlass eines Gesetzes zum Anti-Doping-System vor, das rechtssicher und vorhersehbar die informationellen Eingriffe bei der Dopingbekämpfung regelt. Mittelfristig meinten wir, könne auch eine Verhaltensregel des deutschen Sportes nach § 38a BDSG sinnvoll sein. Von Sanktionen gegenüber den Verbänden und Vereinen sahen wir ab, da dies für die Beteiligten Beeinträchtigungen im internationalen Wettkampfgeschehen zur Folge hätte.

https://www.datenschutzzentrum.de/allgemein/20110726-positionspapier-dopingbekaempfung.html

Gespräche mit dem verantwortlichen Bundesinnenministerium sowie mit Bundestagsabgeordneten zeigten, dass dort keine Neigung besteht, den Forderungen nach einer datenschutzkonformen Regulierung nachzukommen. Problemverständnis zeigten bei einem Gespräch dagegen Vertreter des Landessportverbandes Schleswig-Holstein. Diese erklärten ihre Bereitschaft, die Problematik auch in die Verbände auf Bundesebene einzubringen. Parallel dazu wurde ein Hinweisblatt für Sportlerinnen und Sportler, die am Anti-Doping-System der NADA teilnehmen, erarbeitet. Folgende Aspekte sollen aus Sicht des ULD bei den erst begonnenen Gesprächen zunächst erörtert werden:

- Mehr Transparenz bezüglich Verfahren, Zuständigkeiten und Datenflüssen,
- institutionelle Absicherung einer Beschwerdestelle,
- Festlegungen, wann und wie Verstöße veröffentlicht werden,
- Sicherung der Verhältnismäßigkeit der Kontrollen,
- Einflussnahme auf Normgeber – Gesetzgeber, WADA und NADA – zur Verbesserung der Datenschutzvorkehrungen.

Im Januar 2013 fand ein erstes Gespräch statt, bei dem der Deutsche Olympische Sportbund (DOSB), die NADA und einige Landesdatenschutzbeauftragte, u. a. das ULD, verabredeten, gemeinsam nationale wie auch internationale Lösungen anzustreben, die sowohl eine effektive Dopingbekämpfung als auch einen weitgehenden Persönlichkeitsschutz zum Ziel haben.

Was ist zu tun?

Die Gespräche müssen ergebnisorientiert fortgeführt werden.

5.9 Einzelfälle

5.9.1 Teure Datensammlung ohne Überblick

Eine schleswig-holsteinische Bank hatte zwölf Jahre lang Daten von Interessenten angesammelt und unkontrolliert in die übrigen Banksysteme einfließen lassen. Es wurde ein Bußgeld verhängt.

Eine Bürgerin hatte von einer Bank, mit der sie nichts zu tun hatte, Informationen über die Änderung eines Freistellungsauftrags erhalten. Beabsichtigte Adressatin war offensichtlich eine

Namensvetterin, deren Ehepartner Kunde der Bank war. Woher kannte die Bank die Adresse und wie konnte die Verknüpfung mit der Namensvetterin zustande kommen? Die Bank räumte gegenüber dem ULD ein, dass für die Ehefrau des Bankkunden im Banksystem die falsche Adresse hinterlegt war. Als Ursache hierfür wurde ermittelt, dass zu der Nichtkundin seit 2002 ein Interessentendatensatz aus einem Kunden-werben-Kunden-Vorgang bestand. Dieser Interessentendatensatz war 2007 bei Erteilung des Freistellungsauftrags durch den Bankkunden und Erstellung eines Datensatzes hierfür wegen der Identität des Namens und des Geburtsdatums „automatisch" herangezogen worden. Die Verknüpfung zwischen Interessentendatenbank und dem übrigen Banksystem fand ohne effektive Kontrolle statt. Den Mitarbeitern des Unternehmens war die Verknüpfung weitgehend unbekannt. Aus diesem Grund waren sie für die Fehlerquelle – insbesondere bei der Erstellung von Datensätzen – nicht sensibilisiert. Es erfolgte keine persönliche Kontrolle des Datensatzes bei „automatischer Befüllung".

Der Vorgang verdeutlicht, dass transparente Verfahren innerhalb von Organisationen einen hohen Stellenwert haben. Nur durch Transparenz können Fehlerquellen identifiziert und abgeschafft werden. In der Bank waren grundlegende organisatorische Maßnahmen versäumt worden. Hinzu kam die unzulässige Datensammlung von Interessenten über Jahre hinweg. Das ULD hatte zu dieser ausufernden Interessentendatenbank weitere Beschwerden erhalten (33. TB, Tz. 5.8.4). Es wurde ein Bußgeld verhängt.

Was ist zu tun?

Datenverarbeitungssysteme in Organisationen müssen die Anforderungen der Transparenz erfüllen. Dies ist eine Grundvoraussetzung für die Kontrollierbarkeit der Datenverarbeitungsprozesse. Regelmäßige Kontrollen der vorhandenen Datenverarbeitungssysteme auf deren Rechtmäßigkeit sind eine organisatorische Grundanforderung.

5.9.2 Berechtigungen für Bankmitarbeiter und Handelsvertreter

Das ULD prüfte in einem Kreditinstitut bezüglich der Kundendaten die Vergabe von Lese- und Schreibberechtigungen. Bei der Einräumung von Zugriffsrechten für Bankmitarbeiter konnten Mängel behoben werden.

Auch Banken haben die innerbetriebliche Organisation datenschutzgerecht zu gestalten, wobei technische und organisatorische Maßnahmen zu treffen sind, die je nach der Art der zu schützenden personenbezogenen Daten und Datenkategorien geeignet sind zu gewährleisten, dass die zur Benutzung des Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Es ist sicherzustellen, dass die Kundendaten bei der Verarbeitung und Nutzung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

In der Bank waren Handelsvertreter tätig, die nur produktbezogen beraten. Ein Zugang zu Kundendaten der Bank, welche über die Regelungen des Bundesdatenschutzgesetzes hinaus dem Bankgeheimnis unterliegen, darf für Handelsvertreter nicht eingerichtet werden. Eine stichprobenartige Prüfung von deren Zugriffsberechtigungen gab keinen Anlass zur Beanstandung.

Bei der für die internen Bankmitarbeiter gewählten Berechtigungsvergabe erfolgte jedoch keine optimale Umsetzung. Zur Hauptstelle der Bank zählten auch Hauptgeschäftsstellen und weitere Geschäftsstellen. Die internen Bankmitarbeiter besaßen Zugriffsberechtigungen für die Kundendaten sämtlicher Geschäftsstellen, was die Bank mit dem Verweis auf die Mobilität der Kunden zu rechtfertigen versuchte. Es konnte jedoch nicht ausreichend begründet werden, dass gerade im Hinblick auf die Sensibilität der dem Bankgeheimnis unterfallenden Daten ein Zugriff auf Kundendaten anderer Geschäftsstellen tatsächlich erforderlich ist. Es fehlten belastbare Zahlen dazu, wie viele Kunden in jeweils anderen Geschäftsstellen den entsprechenden Service wünschen, dass Bankgeschäfte in allen Geschäftsstellen abgewickelt

werden können und somit auch geschäftsstellenfremde interne Bankmitarbeiter einen Zugriff auf die Kundendaten anderer Geschäftsstellen benötigen.

Im Rahmen der Zugriffssteuerung kann die Kundin bzw. der Kunde auf Wunsch den Zugriff auf bestimmte Bankmitarbeiter begrenzen lassen. Nach den Angaben der Bank erfolgt in diesem Fall eine Verschlüsselung, welche die Zugriffsberechtigung insgesamt beschränkt. Die Bank hat zugesichert, dass für ihre Kunden bezüglich der Möglichkeit einer Einschränkung der Zugriffsrechte auf bestimmte Mitarbeiter eine angemessene Unterrichtung erfolgt. Dem Kunden muss deutlich werden, dass er auf diese Weise ein besonderes Vertrauensverhältnis zu bestimmten Mitarbeitern begründen kann, ohne dass sämtliche Mitarbeiter auf seine personenbezogenen Daten zugreifen können.

Was ist zu tun?

Kreditinstitute dürfen den für sie tätig werdenden Handelsvertretern keinen Zugriff auf dem Bankgeheimnis unterliegende Daten gewähren. Die Vergabe von Zugriffsberechtigungen an interne Bankmitarbeiter muss zur Erfüllung der jeweiligen Geschäftszwecke zwingend erforderlich sein. Kreditinstitute müssen ihre Zugriffssteuerung auf Erforderlichkeit und Rechtmäßigkeit hin überprüfen.

5.9.3 Aufzeichnen von Gesprächen in Callcentern

In zwei Callcentern wurde die Praxis bei der Erledigung von Kundentelefonaten kontrolliert. Im Schwerpunkt war zu prüfen, ob die angerufenen Personen für die Aufzeichnung ihrer Gespräche eine Einwilligung erteilt hatten.

Zu Beweiszwecken zeichnen Callcenter bekanntlich ihre Kundengespräche auf, um auf diese Weise Vertragsabschlüsse zu dokumentieren. Dieser Umstand muss den Angerufenen allerdings deutlich gemacht werden. Eine Aufzeichnung in Unkenntnis des Angerufenen kann, wenn das nicht öffentlich gesprochene Wort ohne Einwilligung erfasst wird, den Straftatbestand des § 201 StGB erfüllen. Eine ordnungsgemäß erteilte Einwilligung am Telefon bedingt eine deutliche Aufklärung über den Zweck der Aufzeichnung und über den Umstand, dass aufgezeichnet wird. Aus der Reaktion des Angerufenen muss klar erkennbar sein, dass dieser die Unterrichtung verstanden hat und die Aufnahme des Gesprächs akzeptiert.

In den geprüften Callcentern arbeiteten die Telefonisten mit Anweisungsbögen der Geschäftsleitung, die als Arbeitshilfe verwendet werden mussten. Demnach wurde der Angerufene zunächst ordnungsgemäß auf die Aufzeichnung hingewiesen und gebeten, die folgende Aufnahme mit einem deutlichen „Ja“ zu legitimieren. Erst dann wurde die Aufzeichnung aktiviert, sodass nur der eigentliche Vertragsabschluss in den Audiodateien gespeichert wurde. Bei der Prüfung der Audiodateien ergab sich in einem Fall der Verdacht, dass entgegen der Arbeitsanweisung ein Vorgespräch aufgezeichnet wurde und der Angerufene hierzu keine Einwilligung erteilt hatte. Die Aufnahme war allerdings in einem schlechten akustischen Zustand, wodurch ein Verstoß nicht klar belegbar war.

Was ist zu tun?

Betreiber von Callcentern müssen durch Arbeitsanweisungen und gegebenenfalls durch Schulungen der Mitarbeiter sicherstellen, dass bei Aufnahmen von Telefongesprächen vorab von der Kundin bzw. vom Kunden eine wirksame Einwilligung eingeholt wird.

5.9.4 Ohne Führungszeugnis kein Sport

In einem Sportverband kam die Frage auf, inwieweit von den Mitarbeitern ein erweitertes Führungszeugnis verlangt werden darf. Ein solches Dokument gibt auch Auskunft über Angaben zu Straftaten gegen die sexuelle Selbstbestimmung, die in einfachen Führungszeugnissen nicht enthalten sind.

Der Sportverband gab an, im Sinne einer aktiven Prävention von allen haupt- und ehrenamtlichen Mitarbeitern ein erweitertes Führungszeugnis anzufordern, die bei der Erledigung von Verbandsaufgaben in Kontakt mit minderjährigen Personen kommen. Auf diese Weise wolle man Gefahren sexualisierter Gewalt im Sport vorbeugen.

Der hier tätig gewordene Kreisverband folgte der Empfehlung eines übergeordneten Sportverbandes, forderte allerdings nicht pauschal erweiterte Führungszeugnisse ein. Von der Beibringung eines erweiterten Führungszeugnisses freigestellt wurden z. B. Mitarbeiter der sogenannten Kreisgerichte, die keinen unmittelbaren Kontakt zu Minderjährigen haben. Für die Tätigkeiten als Schiedsrichter oder als Trainer führte die Beurteilung zu einem anderen Ergebnis. In diesem Tätigkeitsfeld sah man – von uns unbeanstandet – die Anforderung von entsprechenden Nachweisen als gerechtfertigt an, zumal diese Personen verstärkt bei der Ausbildung Minderjähriger mitwirken. Die Prävention bezüglich sexualisierter Gewalt im Sport ist ein legitimes Ziel.

Im Hinblick auf die Verwahrung der erweiterten Führungszeugnisse und die bestehenden Zugriffsrechte im Sportverband wurde dem ULD versichert, dass nur der Erste Kreisvorsitzende Einsicht in die übersandten Dokumente nimmt und diese dann an die entsprechenden Mitarbeiter zurückgesandt werden. Eine Verwahrung erfolge nicht.

Was ist zu tun?

Bei der Anforderung erweiterter Führungszeugnisse müssen die Sportvereine und -verbände prüfen, ob die Mitarbeiter bei der Erfüllung ihrer Aufgaben verstärkt mit Minderjährigen in Kontakt kommen und ob im Kern eine berufliche oder ehrenamtliche Beaufsichtigung, Betreuung, Erziehung oder Ausbildung Minderjähriger erfolgt.

5.9.5 Sensible Daten auf dem Kontoauszug

Auf den Kontoauszügen eines schleswig-holsteinischen Geldinstituts war zwischenzeitlich der Grad der Behinderung aufgenommen worden. Nach Intervention des ULD wurde von einem weiteren Abdruck dieser Information generell abgesehen.

Plötzlich tauchte auf den Kontoauszügen eines schleswig-holsteinischen Bürgers der Grad der Behinderung „GdB 50+“ auf. Zuvor hatte an dieser Stelle noch „Privates Girokonto“ gestanden.

Der Betroffene hatte die sensible Information über die Schwerbehinderung gegenüber dem Geldinstitut nur angegeben, weil in diesem Fall ein kostenfreies Girokonto zur Verfügung gestellt wird. Der Zweck dieser sensiblen Information auf dem Kontoauszug war dem Betroffenen nicht ersichtlich.

§ 3 Bundesdatenschutzgesetz (BDSG)

Weitere Begriffsbestimmungen

…

(9) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

…

Trotzdem wurde die persönliche Bitte, die Angabe auf den Auszügen zu entfernen, durch das Geldinstitut unter Verweis auf den damit verbundenen Programmierungsaufwand abgewiesen.

Informationen zu Behinderungen sind besondere Arten personenbezogener Daten. Sie sind besonders diskriminierungsrelevant, weshalb für diese ein besonderer Schutz gewährleistet werden muss. Daher sind die Erhebung, Verarbeitung oder Nutzung dieser sensiblen Daten grundsätzlich nur mit Einwilligung des Betroffenen zulässig. Die Vorlage des Schwerbehindertenausweises des Betroffenen bei der Bank diente allein dem Zweck des Nachweises für die Berechtigung einer vergünstigten Leistung. Der Betroffene hatte nur für diesen Zweck seine Einwilligung erteilt. Für den Zweck der Vergünstigung einer Bankleistung ist es nicht erforderlich, deren Begründung auf dem Kontoauszug abzudrucken. Das Abdrucken stellt eine Form des Speicherns bzw. Nutzens dar, die einer eigenen Rechtsgrundlage bedurfte. Eine solche lag hier nicht vor. Nach Einschaltung des ULD wurde das Abdrucken des Grades der Behinderung auf den Kontoauszügen der Bank generell eingestellt.

Was ist zu tun?

Besonders sensible Daten wie solche zur Gesundheit oder zur Behinderung einer Person bedürfen eines besonderen Schutzes. Generell ist eine Verwendung solcher Daten von der Einwilligung des Betroffenen abhängig.

5.9.6 Maßnahmen gegen volle Briefkästen

Immer wieder muss das ULD feststellen, dass die Unternehmen ihre Kundinnen und Kunden nicht über deren Recht unterrichten, gegen Werbemaßnahmen und Markt- und Meinungsforschung Widerspruch einzulegen. Die fehlende Unterrichtung ist bußgeldbewehrt.

Viele Menschen erhalten direkt an sie adressierte Werbung, ohne ansatzweise zu ahnen, woher die werbenden Unternehmen ihre personenbezogenen Daten haben. Oft werden die personenbezogenen Daten, die im Zuge eines Kaufgeschäftes erhoben wurden, zu Werbezwecken verwendet. Die gesetzlich vorgeschriebene Unterrichtung der Bürgerinnen und Bürger über deren Widerspruchsrecht wird oft unterlassen.

Die Pflicht zur Unterrichtung über ein bestehendes Widerspruchsrecht gegen die Verarbeitung oder Nutzung der Kundendaten für Werbung oder Markt- und Meinungsforschung muss bei der Ansprache mit den genannten Zwecksetzungen und bei Vertragsabschluss erfolgen. Eine Verarbeitung zu Werbezwecken erfolgt auch dann, wenn die Kundendaten an ein anderes Unternehmen übermittelt werden, damit dieses die Daten für eigene Werbezwecke nutzt. Einer solchen Übermittlung muss der Kunde widersprechen können.

In einem Fall konnte das ULD im Beratungswege umfassende Hinweise für die Verwendung von Verarbeitungsklauseln in Verträgen erteilen, welche das Unternehmen mit seinen Kundinnen und Kunden schloss. In anderen Fällen musste das ULD näher analysieren, ob es sich bei den festgestellten Verstößen um Einzelverstöße oder systematische Verletzungen des Datenschutzrechts handelte. Von den Unternehmen wird dabei oft übersehen, dass sowohl die fehlende Unterrichtung über ein Widerspruchsrecht als auch die Nichtbeachtung eines Widerspruchs bußgeldbewehrt sind.

Was ist zu tun?

Die Unternehmen müssen ihre internen Prozesse zur Belehrung über Widerspruchsrechte und die Beachtung von Widersprüchen in Bezug auf Werbung sowie Markt- und Meinungsforschung überprüfen. Die betrieblichen Datenschutzbeauftragten trifft hier eine besondere Überwachungspflicht.

5.9.7 Umfang der Auskunftspflicht gegenüber dem ULD

Die verantwortliche Stelle hat gegenüber der Aufsichtsbehörde die Pflicht, Auskunft auf gestellte Fragen zu erteilen, es sei denn, sie macht von ihrem Auskunftsverweigerungsrecht Gebrauch. Die Auskunftspflicht umfasst auch Angaben zu Schuldverhältnissen, die von der verantwortlichen Stelle als Grund für die Datenverwendung angegeben werden.

Mahnschreiben eines Inkassounternehmens waren Grund einer Beschwerde einer Bürgerin, sich an das ULD zu wenden. Das mit dem Forderungseinzug von einer anderen Stelle beauftragte Inkassounternehmen machte behauptete Forderungen aus einem Gewinnspieleintragungsservice geltend. Der zugrunde liegende Vertrag sei telefonisch geschlossen worden. Ein Telefonmitschnitt wurde dem ULD vorgelegt. Das Gespräch fand zwischen der Bürgerin und einer Mitarbeiterin eines weiteren Unternehmens statt. Ein Vertragsabschluss konnte dem Mitschnitt nicht entnommen werden. Das Gespräch wurde gegenüber der Betroffenen als Kontrollanruf bezeichnet. In dessen Verlauf wurden in schneller Abfolge Kosten, Laufzeit usw. genannt und letztendlich die Kontoverbindungsdaten der Bürgerin abgefragt. Dies geschah so schnell, dass es für die Betroffene nicht möglich war, alle Einzelheiten des Gespräches inhaltlich zu erfassen.

Das ULD zweifelte am Vorliegen einer Rechtsgrundlage für die Verwendung der personenbezogenen Daten der Bürgerin und stellte klar, dass ein Hinweis auf einen telefonischen Vertrag nicht ausreichend sei, und forderte das Inkassounternehmen auf, Auskunft darüber zu erteilen, mit welchen Angaben die Betroffene wem gegenüber wann welche vertraglichen Verpflichtungen eingegangen sei. Das gegen das Inkassounternehmen wegen nicht ordnungsgemäß erteilter Auskunft eingeleitete Bußgeldverfahren wurde im gerichtlichen Verfahren aus formellen Gründen eingestellt, ohne dass über die Frage nach dem Umfang der Aufklärungspflicht gegenüber der Aufsichtsbehörde entschieden wurde.

Die im Bundesdatenschutzgesetz enthaltenen Ermächtigungsnormen setzen in bestimmten Fällen voraus, dass die Verwendung der Daten für die Durchführung eines Vertrags erforderlich ist. Dies setzt die Wirksamkeit des Vertrags voraus. Die Aufsichtsbehörde hat daher die Befugnis, auch die einzelnen Parameter zu behaupteten Verträgen zu ermitteln. Erst wenn das Zustandekommen des Vertrags festgestellt ist, stellt sich die Frage nach der Erforderlichkeit.

5.9.8 Geldinstitute als Daten-Banken

Das ULD erhält wiederholt Beschwerden von Bürgerinnen und Bürgern zu weitreichenden Einwilligungserklärungen schleswig-holsteinischer Geldinstitute.

In Anschreiben dieser Institute wird der Anschein erweckt, es gehe in erster Linie um dringende Handlungsmöglichkeiten in Bezug auf vertragliche Fürsorge- und Beratungspflichten und nicht um weitgehende, vertraglich nicht nötige Datenfreigaben. In den fraglichen Passagen heißt es beispielsweise: „… stellen Sie sich vor: Ihre Geldanlage oder Ihr Kredit bei uns ist fällig und niemand sagt Ihnen Bescheid. Das geht nicht, oder?“ In der Einwilligungserklärung finden sich indessen Passagen wie: „Einwilligung zu Anrufen

der Bank für eigene Produkte und Produkte von aktuellen und zukünftigen Verbund- und Kooperationspartnern".

Die Verbindung eines Anschreibens, das ein konkretes Risiko bzw. Vorteile für den Verbraucher aufzeigt, mit einer Einwilligungserklärung, die offenkundig Werbezwecken dient, ist irreführend. Einwilligungen sind nur nach einer klaren Information des Verbrauchers wirksam. Bei Einwilligungen in Telefonwerbung bestehen besonders rigide Anforderungen, da solche Anrufe einen besonders belästigenden Eingriff in die Privatsphäre darstellen.

Aus vielen Beschwerden ist dem ULD bekannt, dass auch in mündlichen Ansprachen gegenüber Kundinnen und Kunden mit dem Argument eine Unterschrift verlangt wird, sonst könnte überhaupt kein telefonischer Kontakt mehr aufgenommen werden. Das ist falsch. Wenn die Speicherung und Nutzung der Telefonnummer eines Kunden für die Vertragsdurchführung erforderlich ist, ist ein Anruf auch ohne Einwilligung erlaubt. So darf beispielsweise selbstverständlich ein Kunde telefonisch informiert werden, wenn ein vereinbarter Termin kurzfristig abgesagt werden muss. Davon zu unterscheiden sind Werbeanrufe, bei denen neue Produkte beworben oder Beratungstermine für weitere Produkte vereinbart werden. Diese Anrufe sind für das eigentliche Bankverhältnis nicht erforderlich. Sie sind nur mit ausdrücklicher Einwilligung zulässig.

§ 7 Gesetz gegen den unlauteren Wettbewerb (UWG)

Unzumutbare Belästigungen

(1) Eine geschäftliche Handlung, durch die ein Marktteilnehmer in unzumutbarer Weise belästigt wird, ist unzulässig. Dies gilt insbesondere für Werbung, obwohl erkennbar ist, dass der angesprochene Marktteilnehmer diese Werbung nicht wünscht.

(2) Eine unzumutbare Belästigung ist stets anzunehmen

…

2. bei Werbung mit einem Telefonanruf gegenüber einem Verbraucher ohne dessen vorherige ausdrückliche Einwilligung oder gegenüber einem sonstigen Marktteilnehmer ohne dessen zumindest mutmaßliche Einwilligung,

…

Was ist zu tun?

Banken werden den Erwartungen ihrer Kundinnen und Kunden nur gerecht, wenn sie fair und transparent mit deren Daten umgehen. Das Erschleichen einer Einwilligung unter Vorspiegelung falscher Informationen ist eine unseriöse Geschäftspraxis und datenschutzrechtlich unzulässig.

5.9.9 Löschpflichten bei Verkauf gebrauchter Mobiltelefone

Bei der Rücknahme von Hardware im Bereich Mobilfunk muss das Unternehmen das vollständige Löschen personenbezogener Daten sicherstellen, bevor es diese Produkte erneut zum Verkauf anbietet.

Ein Elektrofachmarkt hatte nach Geräterücknahmen nicht hinreichend geprüft, ob personenbezogene Daten auf den Geräten vorhanden waren, bevor diese erneut zum Verkauf angeboten wurden. Bei einigen Mobiltelefonen waren nicht alle personenbezogenen Daten der vorhergehenden Kunden vollständig gelöscht worden. Gespeichert waren Daten aus dem Telefonbuch, private Nachrichten sowie Bildaufnahmen.

In eigenem Interesse sollte derjenige, der entsprechende Produkte zurückgibt, darauf achten, dass die von ihm gespeicherten personenbezogenen Daten gelöscht sind. Ein Unterlassen der Vorbesitzer ändert jedoch nichts an der Verantwortlichkeit des Unternehmens. Diese wird dadurch

begründet, dass es die Produkte wieder zum Verkauf anbietet. Sofern personenbezogene Daten der vorherigen Eigentümer nicht vollständig gelöscht sind, ist das Anbieten zum Verkauf ein unbefugtes Bereithalten personenbezogener Daten bzw. im Falle der Übergabe der Ware an den neuen Käufer ein unbefugtes Übermitteln personenbezogener Daten. Das ULD hat mit der verantwortlichen Stelle ein verbessertes Prüf- und Löschverfahren erarbeitet, was umgehend umgesetzt wurde.

Was ist zu tun?

Derjenige, der Hardware aus dem Bereich Mobilfunk wieder zurückgibt, sollte sorgfältig überprüfen, ob die von ihm gespeicherten personenbezogenen Daten gelöscht sind. Das diese Geräte in den Verkauf bringende Unternehmen ist verpflichtet, bei der Rückgabe das vollständige Löschen der personenbezogenen Daten zu überprüfen und sicherzustellen.

5.9.10 Videoüberwachung an Tankstellen

Videokameras in und an Tankstellen sind ein gewohnter Anblick. Für jede einzelne Kamera müssen die datenschutzrechtlichen Anforderungen geprüft werden. Hierfür muss der Tankstellenbetreiber Rede und Antwort stehen.

Das ULD erhielt Beschwerden über Videoüberwachungsmaßnahmen in Tankstellen, wobei angeblich auch eine heimliche Audioüberwachung stattfand. Bei Vor-Ort-Prüfungen stellte das ULD Kameras im Außenbereich an den Zapfsäulen und bei der Waschanlage sowie sichtbar angebrachte Kameras im Tankstellengebäude fest. Hinweise auf eine heimliche Videoüberwachung und eine Audioüberwachung haben sich nicht bestätigt. Eine Audioüberwachung hätte zudem strafrechtliche Relevanz entfaltet.

Bezüglich der Kameras im Innen- und Außenbereich der Tankstelle muss der Tankstellenbetreiber berechtigte Interessen verfolgen. Bei einer Tankstelle hatten sich in den letzten Monaten Raubüberfälle ereignet, und im Rahmen von Inventurarbeiten wurden erhebliche Warendefizite festgestellt, die mit anderen Mitteln nicht aufgeklärt werden konnten. Im Außenbereich musste für den Bereich der Waschanlage das Fehlen eines Hinweisschildes bezüglich der Videoüberwachung beanstandet werden. Da im Innenbereich auch Beschäftigte des Tankstellenbetreibers in den Erfassungswinkel der Kameras kommen, muss die Einstellung vor Ort so gewählt werden, dass eine Dauerüberwachung von Arbeitnehmern ausgeschlossen ist und nur der Bezahlbereich auf der Kassentheke erfasst wird. Eine Überwachung der Beschäftigten ist im Übrigen zumeist nicht zur Aufdeckung von Straftaten geboten und damit unverhältnismäßig. Die Unzulässigkeit einer verdeckten Videoüberwachung rechtfertigt nicht automatisch eine offene Videoüberwachung (33. TB, Tz. 5.1.4).

Was ist zu tun?

Die offene Videoüberwachung muss im Hinblick auf jede einzelne Kamera nach Art, Ausmaß und Anlass verhältnismäßig sein. Auch Tankstellenbetreiber müssen dies für jede einzelne von ihnen betriebene Kamera sicherstellen.

5.9.11 Überwachung von Kuchen und Broten

Gegen die Videoüberwachung von Kuchen und Broten zum Zweck der Prüfung einer ansprechenden Warenpräsentation ist an sich nichts einzuwenden. Dies darf jedoch nicht zu einer Leistungskontrolle von Beschäftigten führen.

Bei der Prüfung einer Bäckerei stellte das ULD mehrere Videokameras fest, die ausschließlich auf Kuchenbleche und Brotregale gerichtet waren. Der Bäcker hatte sogar ein Hinweisschild zur Videoüberwachung angebracht, obwohl sich die mit Bäckereiwaren gefüllten Vitrinen und Regale nicht in öffentlich zugänglichen Bereichen befanden und Personen nicht in den Erfassungswinkel der Kameras gerieten. Der Zweck der Maßnahme bestand im Interesse des Bäckers, die Warenpräsentation stetig zu überprüfen, um auf diese Weise seine Kundschaft mit visuellen Reizen zum Kauf zu ermuntern. Wir prüften, ob der Bäcker Rückschlüsse auf einzelne Beschäftigte ziehen konnte und ob im Zusammenhang mit der Warenprüfung eine Leistungskontrolle erfolgte. Grundsätzlich dürfen personenbezogene Daten von Beschäftigten nur für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist. Nicht jede Kontrolle ist datenschutzrechtlich zulässig. Die Videoaufnahmen waren jedoch nicht zu beanstanden, da eine Zuordnung zu Einzelpersonen nicht möglich war. Anhand der Kameraeinstellung konnte nicht ermittelt werden, welche Beschäftigtenhand beim Zugriff auf Brote und Kuchen tätig war.

Was ist zu tun?

Bei der videotechnischen Erfassung einer Warenpräsentation ist anhand der Kameraeinstellung sicherzustellen, dass Maßnahmen der Leistungskontrolle ausgeschlossen sind.

06

KERNPUNKTE

Mandantentrennung

IT-Projekte

Vorabkontrolle

6 Systemdatenschutz

6.1 Mandantenfähigkeit

Die gemeinsame Nutzung von IT-Systemen durch unterschiedliche datenverarbeitende Stellen muss sorgfältig geplant und korrekt umgesetzt werden. Häufig werden „mandantenfähige" Systeme verwendet, bei denen die umgesetzte Datentrennung nicht hinreichend bewertet wurde. Das ULD hat zusammen mit den Kolleginnen und Kollegen aus den anderen Bundesländern eine Orientierungshilfe erstellt.

Zur Zentralisierung bzw. Konsolidierung verteilter Datenverarbeitung und aus Kostengründen kommen von datenverarbeitenden Stellen zunehmend kooperative Betriebsmodelle zum Einsatz, bei denen Systeme und Programme zur automatisierten Verarbeitung personenbezogener Daten gemeinsam genutzt werden. Das gemeinsame Nutzen einer solchen Infrastruktur stellt erhöhte Anforderungen an die Trennung der personenbezogenen Daten wegen der zusätzlichen Risiken für die informationelle Gewaltenteilung, die Zweckbindung und die Vertraulichkeit. Diese Risiken müssen auf ein akzeptables Niveau reduziert werden.

In Schleswig-Holstein werden diese Fragen durch den gemeinsamen IT-Dienstleister Dataport immer aktueller. Der länderübergreifende Dienstleister praktiziert immer häufiger aus wirtschaftlichen Gründen den Betrieb desselben Fachverfahrens für unterschiedliche Auftraggeber.

Die Begriffe „Mandant" oder „Mandantenfähigkeit" werden verwendet, wenn es Organisationen ermöglicht werden soll, Daten in einer Datenbank logisch zu trennen und zu verwalten. Daten z. B. verschiedener Abteilungen einer Organisation oder verschiedener Kunden eines Rechenzentrums sollen getrennt vorgehalten werden. Das LDSG fordert, dass personenbezogene Daten, die von unterschiedlichen verantwortlichen Stellen oder von einer Stelle zu unterschiedlichen Zwecken erhoben werden, getrennt verarbeitet werden. Bei besonderen Arten personenbezogener Daten ist gesetzlich oft auch eine separate Verarbeitung gefordert. Die getrennte Verarbeitung betrifft die Speicherung und die Verarbeitungsfunktionen wie z. B. Datenbanktransaktionen oder Datensatzbuchungen.

Aus Gründen der Wirtschaftlichkeit oder der Praktikabilität kann es sinnvoll sein, dass Hard- und Software-Ressourcen, also IT-Infrastrukturen, für verschiedene, voneinander zu trennende Datenbestände gemeinsam genutzt werden. Die gemeinsame Nutzung kann so weit gehen, dass eine gemeinsame Speicherung mit mandantenbezogener Kennzeichnung der Daten erfolgt. Die Daten sind dann nur noch logisch getrennt. Voraussetzung für eine getrennte Datenverarbeitung auf einer gemeinsamen Infrastruktur ist, dass die Daten mandantenbezogen geführt und Verarbeitungsfunktionen, Zugriffsberechtigungen und Konfigurationseinstellungen je Mandant eigenständig festgelegt werden können. Technische und organisatorische Maßnahmen müssen zwingend eine getrennte Verarbeitung sicherstellen. In einer Orientierungshilfe hat das ULD zusammen mit den Kolleginnen und Kollegen aus den anderen Bundesländern die Kriterien festgelegt, anhand derer die Mandantenfähigkeit eines Verfahrens geprüft werden muss.

Im ersten Prüfschritt müssen die rechtlichen Grundlagen für die Datenverarbeitung daraufhin bewertet werden, welche datenverarbeitenden Stellen nach welcher Rechtsgrundlage und bei welcher Zweckbestimmung eine Infrastruktur gemeinsam nutzen sollen. Eventuell muss auch geprüft werden, wo die gesetzgeberische Regelungskompetenz für die jeweilige Verarbeitung liegt, ob sich Unvereinbarkeiten zwischen Landes-, Bundes- und Europarecht ergeben und ob eine Befugnis für eine gemeinsame oder eine verbundene automatisierte Verarbeitung besteht.

Im zweiten Prüfschritt ist die Datenübermittlung zwischen einzelnen Mandanten zu prüfen und zu bewerten. Bei einer gemeinsamen IT-Infrastruktur ist die Verarbeitung von Daten eines Mandanten durch einen anderen Mandanten regelmäßig als Datenübermittlung zu bewerten. Hierfür bedarf es einer rechtlichen Grundlage. Diese Grundlagen und die konkreten Anforderungen an die Zulässigkeit der Übermittlungen und an die Form ihrer Durchführung sind vorab zu klären.

Im dritten Schritt ist zu prüfen, ob ein Mandant „abgeschlossen" ist. Ein Mandant gilt als „abge-

schlossen", wenn jede Transaktion in einem Mandanten in einen neuen gültigen Datenbestand übergeht, wobei sie hierbei von Daten anderer Mandanten nicht abhängt und auf diese Daten aufgrund technischer Maßnahmen weder lesend noch schreibend zugreift. Die Datenhaltung muss stets so organisiert werden, dass für jede Instanz eines personenbezogenen Datums die Zuordnung zu genau einem Mandanten erfolgt.

Im vierten Schritt wird geprüft, ob die Konfiguration eines Mandanten unabhängig von anderen Mandanten durchgeführt werden kann. Eine ausreichende Mandantentrennung setzt voraus, dass die Zugriffsberechtigungen, die Verarbeitungsfunktionen und die Konfigurationseinstellungen je Mandant eigenständig festgelegt werden.

In einem letzten Prüfschritt wird sichergestellt, dass mandantenübergreifende Verwaltungsfunktionen auf das notwendige Maß beschränkt werden. Mandantenübergreifende Funktionen zur Verwaltung der Mandanten und der gemeinsam genutzten Infrastruktur dürfen grundsätzlich keine Verarbeitung personenbezogener Daten eines Mandanten ermöglichen.

Das Prüfvorgehen und die notwendigen Ergänzungen im behördlichen oder betrieblichen Datenschutzmanagement sind in der Orientierungshilfe „Mandantenfähigkeit" genauer beschrieben.

https://www.datenschutzzentrum.de/mandantenfaehigkeit/

Das LDSG schließt die getrennte Verarbeitung personenbezogener Daten in einer gemeinsamen Infrastruktur nicht aus. Die datenverarbeitenden Stellen müssen jedoch darauf achten, dass das Sicherheits- und Datenschutzniveau nicht darunter leidet, dass mehrere Stellen ein gemeinsames Verfahren einsetzen. Die zuständigen Datenschutzbeauftragten der datenverarbeitenden Stellen sollten frühzeitig in die Planung einbezogen werden.

6.2 Zusammenarbeit auf Landesebene

Das ULD unterstützt und berät die Landesverwaltung und die Kommunalverwaltung bei IT-Projekten. Eine frühzeitige Berücksichtigung von Datenschutz und Datensicherheit sorgt für eine erhöhte Projektsicherheit und bringt klare und nachvollziehbare Verarbeitungsprozesse hervor.

Die Zusammenarbeit auf der Ebene der Landesverwaltung ist gut strukturiert und organisiert. Neben regelmäßigen Treffen und Abstimmungsrunden auf Projektebene gibt es regelmäßige Koordinierungsrunden. In der IT-Beauftragtenkonferenz (ITBK) wirkt das ULD beratend mit und unterstützt die Ministerien bei der übergreifenden IT-Steuerung und den damit verbundenen Fragen zu Datenschutz und Datensicherheit.

Der IT-Rat Schleswig-Holstein dient der landesweiten Koordinierung des Einsatzes von Informationstechnologie und erarbeitet gleichzeitig die Positionierung des Landes für die Themen des IT-Planungsrates des Bundes. Das ULD ist hier ebenfalls beratend vertreten.

Kritisch sehen wir die mangelhafte Koordinierung der Kommunen mit dem ULD. Bei einzelnen kommunalen Projekten und mit einzelnen Kreis- oder Stadtverwaltungen findet eine direkte und erfolgreiche Abstimmung in Fragen des Datenschutzes und der Datensicherheit statt; es fehlt jedoch eine übergreifende Steuerung und Koordination in puncto Datenschutz und Datensicherheit wie bei der IT-Beauftragtenkonferenz des Landes. Das ULD wird hier im Interesse einer verbesserten Koordination auf die kommunalen Spitzenverbände zugehen.

Auf unsere Initiative hin und mit unserer Unterstützung wurde für die Landesverwaltung ein integriertes Sicherheits- und Datenschutzmanagement (ISMS) aufgebaut. Diese regelmäßig tagende Gruppe setzt sich vornehmlich aus den IT-Sicherheitsbeauftragten der Landesverwaltung zusammen. Sie soll innerhalb der Landesverwaltung die Standardisierung im Bereich IT-Sicherheit und Datenschutz vorantreiben und einheitliche Vorgehensweisen für die Bearbeitung von Sicherheits- oder Datenschutzproblemen etablieren.

Leider sind in fast allen Landesbehörden keine behördlichen Datenschutzbeauftragten bestellt. Wegen der zunehmenden Zentralisierung von Aufgaben in der Landesverwaltung ist dies ein nicht mehr haltbarer Zustand. Die Landesverwaltung braucht als entscheidungs- und tatkräftige Datenschutzbeauftragte ausgebildete Mitarbeiter, die dann für eine oder mehrere Landesbehörden offiziell zu Beauftragten bestellt und als solche tätig werden.

6.3 Zusammenarbeit auf Bundesebene

Datenschutz und Datensicherheit machen nicht vor Ländergrenzen halt. Viele Sachverhalte der automatisierten Verarbeitung personenbezogener Daten sind nicht landesspezifisch, können oder müssen gar bundeseinheitlich geregelt werden. Das ULD übernimmt arbeitsteilig mit den Kolleginnen und Kollegen der Aufsichtsbehörden der anderen Bundesländer einzelne Projekte.

Die für den Systemdatenschutz zuständigen Mitarbeiter der Aufsichtsbehörden im Norden, also von Mecklenburg-Vorpommern, Niedersachsen, Bremen und Hamburg, treffen sich regelmäßig zur Abstimmung für den Bereich der länderübergreifenden Verfahren und Infrastrukturen. Hierbei müssen zunächst die fachlich Verantwortlichen, dann aber auch die Aufsichtsbehörden ein gemeinsames, einheitliches Vorgehen anstreben.

Zur bundesweiten Abstimmung dient der Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder. Dieser erarbeitet gemeinsame Bewertungen zu Einzel- und Grundsatzfragestellungen des Datenschutzes und der Datensicherheit. Unter der Geschäftsführung durch unsere Kollegen in Mecklenburg-Vorpommern werden Orientierungshilfen, Entschließungen und Stellungnahmen vorbereitet und abgestimmt.

6.3.1 KoSIT-Beirat

Das ULD berät den IT-Planungsrat und dessen Gremien in Fragen des Datenschutzes und der Datensicherheit. Wir verfolgen das Ziel, Datenschutz und Datensicherheit auf Bundes- und Länderebene einheitlich umzusetzen. Eine frühzeitige Beteiligung bei länderübergreifenden Projekten verhindert, dass auf Bundes- oder länderübergreifender Ebene für Schleswig-Holstein datenschutzkritische Vorgaben gemacht werden.

Das ULD vertritt den Arbeitskreis Technik der Datenschutzbeauftragten der Länder und des Bundes im KoSIT-Beirat. Die KoSIT (Koordinierungsstelle für IT-Standards) ist der operative Arm des IT-Planungsrates (IT-PLR). Der IT-PLR, der sich aus Vertretern der Länder und des Bundes zusammensetzt, beschließt die Nationale E-Government-Strategie (NEGS). Die NEGS definiert den Zielrahmen für Bund, Länder und Kommunen zur Modernisierung der staatlichen Informationstechnik und E-Government-Dienste. Das Spektrum der Maßnahmen umfasst die Konzeption und den Betrieb technischer Basisinfrastrukturkomponenten sowie Dienstleistungen wie den Aufbau eines elektronischen Grundbuchs. Weitere Handlungsfelder sind die Informationssicherheit und eine Strategie für den Umgang mit elektronischen Identitäten. Der KoSIT-Beirat hat die Aufgabe, hierfür mit seinem technischen und rechtlichen Sachverstand beizutragen.

Das ULD lässt sich hier von dem Grundsatz „Privacy by Default“ leiten. Wir sorgen dafür, dass bereits in der Planungs- und Konzeptionsphase von Standardisierungsprojekten Anforderungen der Datensicherheit, der Datensparsamkeit und generell des Datenschutzes formuliert und berücksichtigt werden. Aus den Erfahrungen dieser Gremienarbeit, zusammen mit der Arbeit der Umsetzung konkreter Maßnahmen im Rahmen des XTA-Projekts (Tz. 6.3.3), entstand ein standardisiertes Datenschutzmodell. Dieses basiert auf den sechs elementaren Schutzzielen des Datenschutzes, die im seit Januar 2012 gültigen LDSG in Schleswig-Holstein und in leicht abgewandelter Form auch in anderen Landesdatenschutzgesetzen verankert sind. Das Modell benutzt die Systematik nach dem IT-Grundschutz des Bundesamtes für Sicherheit in der Informationsgesellschaft (BSI). Es bietet dadurch einen methodischen Rahmen, der die allgemeinen, wesentlichen normativen Anforderungen des Datenschutzrechts berücksichtigt und – besser kontrollierbar als bislang – eine Transformation der gesetzlichen Anforderungen in technische und organisatorische Maßnahmen gestattet. Das ULD bietet behördlichen und betrieblichen Datenschutzbeauftragten an, Fortbildungen zu diesem Datenschutzmodell durchzuführen und dieses im Rahmen von einzelnen Projekten in die Projektarbeit einzubringen.

6.3.2 Informationssicherheitsleitlinie (ISMS) für Bund, Länder und Gemeinden

Das ULD vertritt den Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder in einer vom IT-Planungsrat (IT-PLR) eingesetzten Arbeitsgruppe zur Erstellung einer Sicherheitsleitlinie.

Diese Leitlinie soll für die öffentlichen Verwaltungen in Bund, Ländern und Gemeinden gelten. Sie umfasst Regelungen

- für ein einheitliches Informationssicherheitsmanagement (ISMS),
- für die Absicherung der Netzinfrastrukturen der öffentlichen Verwaltung,
- für einheitliche Sicherheitsstandards für ebenenübergreifende IT-Verfahren,
- mit Kooperationsvereinbarungen für den Verwaltungs-CERT-Verbund sowie
- für Standards und Produktsicherheit.

Die Vertretung der Interessen der Gemeinden wurde seitens des Gesetzgebers den Ländern zugewiesen. Das hat gemäß dem Konnexitätsprinzip zur Folge, dass bei Anordnungen zur Umsetzung von Sicherheitsmaßnahmen seitens eines Landes an die Kommunen das Land auch die Kosten dafür zu tragen hat. Eine solche Konstellation wird zu einem handfesten Dilemma, wenn Gemeinden den Anforderungen der Informationssicherheitsleitlinie nicht genügen, weil die Kostenübernahme ungeklärt ist und diese Gemeinden deshalb nicht an die internen Netze der Länder und des Bundes angeschlossen werden können. Das hätte zur Folge, dass typische Verwaltungsdienstleistungen, wie sie Gemeinden beispielsweise im Meldewesen oder im Personenstandswesen erbringen, den Bürgerinnen und Bürgern solcher Gemeinden nicht zur Verfügung stünden. Das kann keine Lösung sein. Mit dem Hinweis auf „das Auslösen der Konnexität“ weigerten sich in der Arbeitsgruppe viele Länder, in einigen Teilaspekten auch Schleswig-Holstein, wesentlichen Sicherheitsanforderungen nach IT-Grundschutz zu genügen.

Aus Sicht des ULD ist das Argument der Gemeinden bezüglich des Auslösens der Konnexität nicht stichhaltig. So verlangt die Sicherheitsleitlinie in ihrer aktuellen Version nur solche Sicherheitsmaßnahmen, die nach geltendem Datenschutzrecht von den Verwaltungen in den Ländern und Gemeinden ohnehin umzusetzen sind. Es bedarf deshalb keines weiteren Auftrags durch die Länder an die Kommunen, der für die Länder das Risiko der Konnexität auslöst.

6.3.3 XTA

Das ULD arbeitet bei der Erstellung eines Konzepts für einen standardisierten Transportadapters für die öffentliche Verwaltung („XTA“) mit.

Ein XTA ist ein Programmbestandteil, das zwischen einem Fachverfahren, mit dem die Sachbearbeitung in einer öffentlichen Verwaltung durchgeführt wird, und einem Transportverfahren, mit dem die Daten eines Fachverfahrens in eine andere Verwaltungseinheit geschickt werden, angesiedelt ist. Diese Zwischenschicht einzuziehen und zu standardisieren ist notwendig geworden, weil äußerst unterschiedliche Formen des Datentransports existieren. Erfasst werden der Transport zwischen verschiedenen Datenbanken innerhalb eines Rechenzentrums ebenso wie der Transport mit dem verwaltungsinternen E-Mail-ähnlichen Kommunikationsstandard OSCI-Transport über Landesgrenzen hinweg oder moderne Transportformen wie Webservices. Die Hersteller von Fachverfahren und die Rechenzentren sollen mit XTA von der Aufgabe entlastet werden, viele komplizierte Speziallösungen für Transportaufgaben bereitstellen zu müssen. Man verspricht sich davon eine Reduktion der Kosten.

Aus der Sicht des Datenschutzes und der Datensicherheit bedeutet eine zentral betriebene Kommunikationskomponente, etwa im Rahmen einer Clearingstelle oder eines Nachrichtenbrokers, dass dort unterschiedliche Daten unterschiedlicher Sender und Empfänger vermittelt werden. An einer solchen zentralen Stelle muss eine saubere Trennung der Daten unterschiedlicher datenverarbeitender Stellen erfolgen und die Vertraulichkeit der Daten sichergestellt werden. Bei der Spezifikation des XTA-Standards muss technisch gewährleistet werden, dass der Betreiber der XTA-Schnittstelle und des Transportverfahrens nachweisbar keinen Zugriff auf die Inhaltsdaten der Fachverfahren nehmen kann und dass jederzeit vollständige Transparenz darüber hergestellt werden kann,

welche Transaktionen mit welchen beteiligten Systemen stattfanden. Eine erste technische Spezifikation von XTA liegt vor.

Der Prozess der Standardisierung mit seinen funktionalen, sicherheitstechnischen und datenschutzrechtlichen Anforderungen erfolgt durch die KoSIT (Tz. 6.3.1), die das Projekt im Auftrag des IT-Planungsrates durchführt. Das ULD wird die Standardisierungsarbeit auf Bundesebene zusammen mit den Kolleginnen und Kollegen der anderen Bundesländer im Rahmen der begrenzten personellen Ressourcen weiterhin begleiten.

Was ist zu tun?

In Schleswig-Holstein müssen bei Ausschreibungen und bei der Planung von Verfahren die standardisierten Vorgaben stärker berücksichtigt werden.

6.4 Ausgewählte Ergebnisse aus Vorabkontrollen

Lange vernachlässigt, ist sie jetzt wiederentdeckt: die Vorabkontrolle. Was als verwaltungsinterner Prozess gedacht war, um Datenschutz und Datensicherheit bei der Einführung eines Fachverfahrens sicherzustellen, entwickelt sich zur wesentlichen Erfolgsbedingung für Projekte.

Die Vorabkontrolle dient der Prüfung der Datenverarbeitung mit erhöhtem Schutzbedarf auf Rechtmäßigkeit und Ordnungsmäßigkeit vor Betriebsaufnahme. Sie soll durch die oder den behördlichen Datenschutzbeauftragten durchgeführt werden. Ist niemand für diese bei modernen Verwaltungen wichtige Funktion bestellt, so übernimmt das ULD diese Aufgabe. Im Bereich der Landesverwaltung ist die Anzahl der Vorabkontrollen stark angestiegen. Dies liegt wohl u. a. daran, dass Datenschutz und Datensicherheit verstärkt Beachtung findet. Ein Grund ist auch, dass immer mehr Verfahren zentralisiert und dann von mehreren datenverarbeitenden Stellen gemeinsam betrieben werden. Bei der Prüfung durch das ULD nimmt neben der Prüfung der Rechtsgrundlagen die kritische Bestandsaufnahme der technischen und organisatorischen Maßnahmen in Bezug auf Angemessenheit und Wirksamkeit einen großen Raum ein.

6.4.1 Vorabkontrollen sind gebührenpflichtig

Das ULD wendet die gesetzlichen Vorgaben des LDSG an und erhebt für Vorabkontrollen Gebühren. Die Gebühren sind in einer Satzung festgelegt. Der Prozess ist transparent beschrieben und für die datenverarbeitenden Stellen nachvollziehbar.

Vorabkontrollen sind aufwendige, aber klar umrissene und abschätzbare Prüfprozesse. Zu Beginn einer Vorabkontrolle werden eine Aufwandsschätzung und ein Projektplan zur Durchführung erstellt. In seiner Benutzungs- und Entgeltsatzung hat das ULD das Vorgehen zur Durchführung einer Vorabkontrolle festgelegt und die dafür zu erhebenden Gebühren dargestellt. Die Vorabkontrolle durch das ULD wird nach Personalaufwand abgerechnet. Es wird ein fester Satz von 640 Euro pro Personentag zusätzlich Reisekosten berechnet. Der Aufwand für die Durchführung der Vorabkontrolle beträgt in der Regel mindestens drei Personentage.

Der Aufwand erhöht sich, wenn uns keine ausreichenden Nachweise einer ordnungsgemäßen Datenverarbeitung vorgelegt werden. Hoher Aufwand entsteht regelmäßig bei komplexen Verfahren. Um den Aufwand einschätzen zu können, benötigt das ULD vor Beginn der Vorabkontrolle die in der Datenschutzverordnung (DSVO) festgelegten Dokumente und Nachweise einer ordnungsgemäßen Datenverarbeitung. Die vom ULD vorgenommene Aufwandsschätzung und der Projektplan zur Durchführung der Vorabkontrolle werden der anfragenden Stelle vor Auftragserteilung zur Verfügung gestellt.

6.4.2 KoPers

Die Landesverwaltung und die Kommunen führen gemeinsam mit der Hansestadt Hamburg ein neues Personalverwaltungssystem ein: KoPers. Für die Versorgungs- und Ausgleichskasse (VAK) führt das ULD die erste Vorabkontrolle in diesem Großprojekt durch.

KoPers ist ein länderübergreifendes System für die Personalverwaltung. Es wird für alle teilnehmenden Behörden durch den landesweiten und länderübergreifenden Dienstleister Dataport betrieben. Der kommunale Bereich in Schleswig-Holstein ist bei diesem Projekt Vorreiter: Die erste Vorabkontrolle von KoPers hat das ULD für die Versorgungs- und Ausgleichskasse (VAK) der Kommunen durchgeführt. Dabei wurden Mängel festgestellt, die eine vom Betreiber unabhängige Kontrolle des Verfahrens durch die datenverarbeitenden Stellen größtenteils unmöglich machten. Die Stellen waren bei einem Großteil der durch sie durchzuführenden Prüf- und Kontrolltätigkeiten auf die Mitwirkung des Dienstleisters angewiesen; das Verfahren selbst war nicht „auskunftsfähig“: Die Protokollierung der Nutzung und der Administration des Verfahrens war nicht ausreichend und konnte nicht vollständig durch die Auftraggeber geprüft werden. Diese Mängel im Verfahren wurden behoben. Bei einer Nachkontrolle stellte das ULD fest, dass nun die Auftraggeber für regelmäßige und anlassbezogene Kontrollen die erforderlichen Informationen unabhängig vom Dienstleister und direkt aus dem Fachverfahren erhalten können.

Bei der VAK prüft das ULD die für den Betrieb des Verfahrens notwendigen technischen und organisatorischen Maßnahmen. Nach Abschluss dieser Prüfung wird das ULD die kommunalen KoPers-Anwender schriftlich über die notwendigen Prüfschritte informieren, die für deren Vorabkontrolle notwendig sind. Sollten kommunale Anwender keine behördlichen Datenschutzbeauftragten bestellt haben, so ist das ULD mit der Durchführung einer kostenpflichtigen Vorabkontrolle zu beauftragen (Tz. 6.4.1).

6.4.3 BAföG21

Mit BAföG21 verwalten die Kreise sowie kreisfreien Städte und die Studentenwerke der Hochschulen die BAföG-Anträge von Studierenden.

BAföG21 besteht aus drei Modulen: dem zentral bei Dataport betriebenen Hauptverfahren BAföG21, Dialog21 als Verbindung zwischen den dezentralen Clients mit dem zentralen Server sowie Kasse21 zur Abwicklung von Zahlungsvorgängen. Die Federführung zur Entwicklung und Pflege des Programms liegt beim Land Baden-Württemberg. Das Bildungsministerium betreut den zentralen Betrieb und übernimmt die Kommunikation mit Baden-Württemberg. Die Vorabkontrolle bestand aus zwei Teilen, einer Prüfung der zentralen Komponenten bei Dataport sowie einer Prüfung der Komponenten vor Ort. Diese Kontrolle bei Dataport ergab, dass die vernetzten Systeme wie vorgesehen in den standardisierten Betriebsabläufen der Administration eingebunden sind.

Eine Kontrolle der dezentralen Verfahrenskomponenten konnte bislang nicht durchgeführt werden.

Was ist zu tun?

Die zentral koordinierte Vorabkontrolle muss zeitnah abgeschlossen werden, um den datenverarbeitenden Stellen aufwendige Prüfprozesse vor Ort zu ersparen. Das Justizministerium muss die Nachweise einer ordnungsgemäßen Datenverarbeitung vervollständigen und dem ULD zur Prüfung vorlegen.

6.4.4 forumSTAR

Im Justizbereich von Schleswig-Holstein soll mit „forumSTAR“ eine plattformunabhängige Fachanwendung für die ordentliche Gerichtsbarkeit eingesetzt werden. Das ULD prüft das Verfahren im Rahmen einer gemeinsamen Vorabkontrolle unter Koordinierung des Justizministeriums.

forumSTAR enthält neben fachspezifischen Programmteilen – für Zivilsachen, Familiensachen, Strafsachen, Immobilarvollstreckung, Mobiliarvollstreckung, Insolvenzsachen, Vormundschaftssachen, Nachlasssachen, Rechtsantragsstelle – ein programmierbares Textsystem. Gegenwärtig wird forumSTAR für Zivilsachen und Mobiliarvollstreckung eingesetzt. Die Programmentwicklung geschieht in Kooperation der Bundesländer Bayern, Sachsen, Rheinland-Pfalz und Baden-Württemberg; die Entwicklung führt die Firma Siemens Business Services durch.

Die zentralen Bestandteile, eine Datenbank und ein Fileserver, werden von Dataport betrieben. Der Pilotbetrieb für die dezentralen Verfahrensbestandteile erfolgt beim Amtsgericht Schleswig. Die Datenbank enthält die Daten von Verfahrensbeteiligten; der Fileserver stellt zentral Formulare für die verschiedenen Verfahrensbestandteile bereit. Diese zentral gespeicherten Formulare werden auf die lokalen Komponenten kopiert, wo sie dann mit den personenbezogenen Daten gefüllt werden. Dabei verbleiben die Formulare auf den lokalen Systemen; eine zentrale Speicherung ausgefüllter Formulare bei Dataport findet ebenso wenig statt wie eine Übermittlung an andere Gerichte.

Die Vorabkontrolle bei Dataport ergab, dass die vernetzten Systeme in die standardisierten Betriebsabläufe der Administration eingebunden sind. Das bedeutet, dass z. B. die Pflege der Firewall-Regeln zentral geschieht und anhand der Dokumentation sowie der Auskünfte der Administratoren die Berechtigung der Freigabe der Ports überprüfbar war. Die Aktivitäten der Administration auf der Ebene des Betriebssystems sowie der Datenbank waren mittels eines zentralen Protokollierungsservices nachvollziehbar. So waren auch die aktuellen Aktivitäten der Vorabkontrolle unmittelbar nachverfolgbar. Veränderungen an der Hardware und in den Abläufen, etwa das Einspielen von Patches und Updates, unterliegen einem geregelten, auf einem Ticketsystem aufsetzenden Changemanagement und werden vor dem Aufspielen auf das Produktionssystem getestet.

Bei der Kontrolle der Datenbank stellte sich die Frage, nach welchen teilweise unterschiedlichen Anweisungen der verschiedenen Beteiligten – den Herstellern der Datenbank, des Betriebssystems und des Anwendungsprogramms sowie des Rechenzentrumsbetreibers Dataport – die Datenbank installiert und konfiguriert wurde. Anweisungen und Abweichungen davon sind zu dokumentieren. Ausreichend dokumentiert war auch noch nicht der Fileserver, der auf WebDAV-Technologie basiert. Bei dem Ersteinsatz lagen noch keine Dataport-spezifischen Installations- und Konfigurationsvorgaben vor. Die Kontrolle zeigte, dass Default-Einstellungen entweder umbenannt oder gelöscht wurden und eine übliche anonyme Authentisierung abgeschaltet war. Die Protokollierung der Administration ist auf eine zentrale Komponente ausgelagert. Die Dokumentation der WebDAV-Installation und -Konfiguration wurde zugesichert.

Eine Durchsicht der Systeme zeigte, dass trotz Durchlaufs eines Härtungsskripts nach wie vor funktionslose Nutzer und Nutzerverzeichnisse, die seitens des Herstellers des Betriebssystems angelegt waren, sowie Compiler auf den Produktionsmaschinen vorhanden waren. Des Weiteren zeigte die Kontrolle der Nutzer mit Administrationsrechten, dass Dataport die Strategie verfolgte, in einer Standardkonfiguration eines Systems mit dem Schutzbedarf „normal“ dem gesamten verfügbaren Personal der Betriebssystemadministration Zugriff auf Systeme zu geben, wobei die Authentisierung der Administratoren zentral über LDAP geschieht. Eine solche Strategie verbessert zwar die Verfügbarkeit und Intervenierbarkeit, verschlechtert aber die aus Sicht der Datensicherheit und des Datenschutzes für Infrastrukturen in der Regel wichtigeren Schutzziele der Integrität und Vertraulichkeit. Dataport wurde aufgefordert, diese Strategie zu überdenken und eine Einschränkung des Administrationspersonals auf das erforderliche Maß auch ohne zusätzliche Kosten für den Auftraggeber standardmäßig vorzunehmen.

Die Prüfung der dezentralen Verfahrensbestandteile offenbarte, dass wesentliche Teile der Dokumentation fehlten. So waren die Rechtsgrundlagen nicht hinreichend konkret dargelegt, und es fehlte die Dokumentation der Schutzbedarfsermittlung bzw. die Rechtfertigung dafür, dass der Schutzbedarf mit „normal“ angesetzt wurde. Das ULD hält Maßnahmen zur Umsetzung des Schutzbedarfs „hoch“ bei personenbezogenen Daten in einem

Gerichtsverfahren wegen der in der Regel biografisch hohen Bedeutung für Betroffene für angemessen. Selbst unter der Annahme, dass der Schutzbedarf „normal“ angemessen sei, ist die Protokollierung der Administrationstätigkeiten der Server und der Arbeitsplätze, die in der dezentralen Justiz zum Einsatz kommen, unzulänglich. Einzig die Dokumentation zur Protokollierung der Aktivitäten im Fachverfahren war auf einem ausreichenden Niveau. Nicht hinreichend ausgebildet waren die Revisionsprozesse, um anhand der Dokumentationen und Protokollierungen sowohl auf der Administrationsebene als auch auf der Verfahrensebene Kontrollen bezüglich der technischen Funktionalität und der Aktivitäten von Mitarbeitern, Administratoren und Dienstleistern durchführen zu können. Unzureichend ist zudem das Sicherheitsniveau der Standardarbeitsplatz-PCs sowie die bauliche Sicherheit des Serverraums im Amtsgericht.

Was ist zu tun?

Es ist kurzfristig ein Plan zur Mängelbehebung sowie zum Erreichen des Schutzniveaus „hoch“ zu erstellen. Dabei darf über die Problematik der physischen und administrativen Serversicherheit die Behebung der Sicherheitsmängel der Arbeitsplätze, die über das betrachtete Fachverfahren hinaus wirken, nicht vernachlässigt werden.

6.5 Ausgewählte Ergebnisse aus Prüfungen

Das ULD überwacht nach den §§ 39 und 41 Landesdatenschutzgesetz (LDSG) die Einhaltung der datenschutzrechtlichen Vorschriften bei den öffentlichen Stellen im Land, indem es u. a. regelmäßige Prüfungen durchführt. Einzelne Ergebnisse und Auffälligkeiten werden im Folgenden dargestellt.

6.5.1 Nachkontrollen

Eine Prüfung durch das ULD ist selten mit der Erstellung des Prüfberichts beendet. Oft sind umfangreiche Nacharbeiten bei der datenverarbeitenden Stelle notwendig. Diese werden durch Nachkontrollen durch das ULD begleitet.

Es gilt der Grundsatz: Eine Prüfung ist erst dann abgeschlossen, wenn die Mängel beseitigt wurden. In den Amtsverwaltungen Schleswig-Holsteins wurde eine Reihe von Nachkontrollen durchgeführt, um vor allem festzustellen, inwieweit Mängel nach ausgesprochenen Beanstandungen behoben wurden. Die geprüften Stellen hatten unsere Beanstandungen weitestgehend akzeptiert. Deshalb hätte man erwarten können, dass in der Zwischenzeit für Abhilfe gesorgt wurde.

Leider ist dies sehr oft nicht der Fall. In vielen Verwaltungen war noch nicht einmal ansatzweise mit der Behebung begonnen worden. So wurden z. B. folgende Mängel erneut vorgefunden:

- Dienstanweisungen, die den Umgang mit der IT regeln, existieren nicht.
- Eine Verfahrensdokumentation liegt nicht vor.
- Dokumentationen von Tests und Freigaben liegen nicht vor.
- Eine Stellvertretung der Administration ist immer noch nicht bestellt.
- Datenbestände, die für die Aufgabenerfüllung nicht mehr notwendig sind, werden nicht gelöscht.
- Eine Kontrolle von externen Dienstleistern erfolgt nicht.
- Administrative Tätigkeiten werden weiterhin nicht protokolliert.
- Eine Kontrolle der Administration findet immer noch nicht statt.

Wir müssen in diesen Fällen vorgefundener Mängel erneut beanstanden. Das ULD wird in einzelnen Fällen jetzt zusammen mit den fachlichen Aufsichtsbehörden gemeinsame Kontrolltermine vor Ort durchführen und die kommunalen Spitzenverbände über die Problemfälle informieren. Nachkontrollen sind außerordentlich wichtig und müssen weiterhin durchgeführt werden – auch und gerade, um den unterstützenden Kontakt mit den Kollegen vor Ort aufrechtzuerhalten.

Was ist zu tun?

Die geprüften Stellen müssen die Mängelbehebung vorantreiben.

6.5.2 Prüfung der Verfahrensverzeichnisse

§ 7 Abs. 1 LDSG verpflichtet jede datenverarbeitende Stelle zur Erstellung eines Verfahrensverzeichnisses für Verfahren automatisierter personenbezogener Datenverarbeitung. Das ULD hat die Verfahrensverzeichnisse der schleswig-holsteinischen Behörden geprüft.

Mit der Bezeichnung „automatisiertes Verfahren" ist die Verwendung personenbezogener Daten zu einem bestimmten Zweck, mit Unterstützung von informationstechnischen Geräten (Hardware) und Computerprogrammen (Software), eingebunden in ein organisatorisches Regelwerk gemeint. Das Verfahrensverzeichnis stellt die Öffentlichkeit aller automatisierten Verfahren und die Transparenz der Datenverarbeitung der datenverarbeitenden Stelle sicher.

Ende 2012 hat das ULD eine Prüfung gestartet, die das Verfahrensverzeichnis der schleswig-holsteinischen Behörden als Prüfungsgegenstand hat. Dazu wird in bestimmten Prüfungsintervallen eine Gruppe von Behörden angeschrieben. Sie sollen Auskunft darüber geben, ob sie eine behördliche Datenschutzbeauftragte oder einen behördlichen Datenschutzbeauftragten (bDSB) förmlich nach § 10 LDSG bestellt haben. Außerdem verlangt das ULD die Bereitstellung der Verfahrensverzeichnisse zur weiteren Prüfung. Betrachtet werden nicht nur die Verfahrensverzeichnisse an sich, sondern auch die Prozesse, die mit den Verfahrensverzeichnissen zusammenhängen, z. B. die Verantwortlichkeiten oder die ordnungsgemäße Durchführung der Vorabkontrolle.

Ist ein behördlicher Datenschutzbeauftragter (bDSB) förmlich bestellt, dann führt sie oder er das Verfahrensverzeichnis und hält es in geeigneter Weise zur Veröffentlichung bereit. Denkbar ist die Bereitstellung zur Einsicht in Papierform oder die Veröffentlichung auf der Webseite. Die oder der bDSB führt weiterhin die Vorabkontrolle für gemeinsame Verfahren mehrerer datenverarbeitenden Stellen oder Abrufverfahren oder für Verfahren durch, in denen besonders sensible personenbezogene Daten verarbeitet werden, also Angaben zu rassischer oder ethnischer Herkunft, politischen Meinungen, religiösen oder weltanschaulichen Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben, sowie Daten mit einem besonderen Berufs- oder Amtsgeheimnis. Das ULD nimmt bei dem Verfahrensverzeichnis eine Plausibilitätskontrolle vor.

Ist keine oder kein bDSB förmlich bestellt, so muss die entsprechende datenverarbeitende Stelle ihrer Meldepflicht nachkommen und dem ULD ihre meldepflichtigen automatisierten Verfahren, also ihr Verfahrensverzeichnis, zur Veröffentlichung zur Verfügung stellen. Das ULD wird die Verfahrensverzeichnisse auf seiner Webseite veröffentlichen. Benötigen Verfahren eine Vorabkontrolle, dann muss die datenverarbeitende Stelle das ULD informieren und dem ULD die Gelegenheit geben, innerhalb einer angemessenen Frist die Vorabkontrolle durchzuführen (Tz. 6.4 und 6.4.1).

Im ersten Prüfungsintervall wurden die obersten Landesbehörden angeschrieben. Bei diesem noch nicht abgeschlossenen Intervall zeigen sich schon Tendenzen. So sind datenverarbeitende Stellen, die eine bzw. einen bDSB bestellt haben, in Bezug auf das Verfahrensverzeichnis generell besser aufgestellt, als wenn keine oder kein bDSB bestellt ist. Das mag daran liegen, dass das LDSG die Verantwortlichkeit der oder des bDSB zum Führen des Verfahrensverzeichnisses klar definiert; ohne eine Bestellung fühlt sich in einer datenverarbei-

tenden Stelle niemand verantwortlich; Festlegungen sind nicht erfolgt. Häufig wurde erst während der Prüfung begonnen, Verantwortlichkeiten für das Erstellen des Verfahrensverzeichnisses festzulegen bzw. das Verfahrensverzeichnis zu erstellen.

Die Prüfung wird nicht nur die obersten Landesbehörden betreffen. Sie wird sich in mehreren Prüfungsintervallen über die Landesoberbehörden und die unteren Landesbehörden bis hin auf die kommunale Ebene ausdehnen.

6.5.3 Öffnen persönlicher E-Mail-Postfächer während einer Prüfung

Aufsichtsbehörden und behördliche Datenschutzbeauftragte müssen in einzelnen Fällen auf die persönlichen E-Mail-Postfächer von Beschäftigten zugreifen. Dabei sollte ein transparentes und datensparsames Verfahren angewendet werden.

Grundsätzlich stellt die Verarbeitung – unter die auch eine Einsichtnahme durch eine Prüferin oder einen Prüfer fällt – von personenbezogenen Daten für Aufsichts- und Kontrollbefugnisse nach § 13 Abs. 5 LDSG keine Zweckänderung dar und bedarf somit keiner besonderen Prüfung der Rechtsgrundlagen.

Im Wortlaut: § 13 Abs. 5 und 6 LDSG

(5) Die Verarbeitung der Daten zur Ausübung von Aufsichts- und Kontrollbefugnissen sowie zur Rechnungsprüfung gilt nicht als Verarbeitung für andere Zwecke. Daten, die zu einem anderen Zweck erhoben oder erstmalig gespeichert wurden, sind für Ausbildungs- und Prüfungszwecke in anonymisierter oder pseudonymisierter Form zu verarbeiten. Lassen sich die in Satz 2 genannten Zwecke durch anonymisierte oder pseudonymisierte Datenverarbeitung nicht erreichen, so ist die Zweckänderung zulässig, soweit berechtigte Interessen der oder des Betroffenen an der Geheimhaltung der Daten nicht überwiegen.

(6) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherheit oder zur Sicherstellung des ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nicht für andere Zwecke verwendet werden.

Häufig ist die Nutzung von Internetdiensten und E-Mail nur zu dienstlichen Zwecken im Rahmen des Beschäftigungsverhältnisses erlaubt. So ist gemäß der „Vereinbarung nach § 59 Mitbestimmungsgesetz (MBG) betr. Richtlinie zur Nutzung von Internet und E-Mail“ für die Landesbehörden die Nutzung von E-Mail-Konten nur für dienstliche Zwecke zulässig. Es kann somit erwartet werden, dass in einem E-Mail-Postfach keine relevante Menge privater Kommunikation zu finden ist. Die Betroffenen haben jedoch häufig keine Möglichkeit, den Empfang privater E-Mails zu unterbinden. Es ist somit nicht auszuschließen, dass sich in Einzelfällen private Kommunikation im Postfach befindet.

Selbst bei rein dienstlicher Nutzung kann E-Mail im Zusammenhang mit besonders zu schützenden Funktionen stehen – z. B. Personalvertretungen, Gleichstellungsbeauftragten, Schwerbehindertenvertretungen, behördlichen Datenschutzbeauftragten – oder besonders geschützte Inhalte haben. Die Einsichtnahme in eine derartige Kommunikation mit privaten Inhalten oder erhöhtem Schutzbedarf darf selbst durch Aufsichts- oder Kontrollorgane nur im Einzelfall nach einer gesonderten Prüfung vorab und insbesondere unter Beteiligung der eventuell betroffenen Funktionsträger erfolgen.

Für die Durchführung einer derartigen Kontrolle empfiehlt das ULD das folgende Vorgehen: Vor der Öffnung des Postfaches sollte

- festgelegt werden, anhand welcher möglichst konkret festgelegter Kriterien E-Mails zur Einsichtnahme ausgewählt werden,
- ebenfalls durch möglichst vorab formulierte Ausschlusskriterien ausgeschlossen werden, dass eine Einsichtnahme in erkennbar private E-Mails erfolgt, und
- geprüft werden, ob die Daten einer funktionierenden Datensicherung unterliegen

oder ob andere Mechanismen getroffen wurden, um das Postfach bei einer unerwünschten Änderung während der Prüfung oder bei Automatismen wie z. B. Spamfiltern im Anzeigeprogramm in den Ausgangszustand vor der Prüfung versetzen zu können.

Während der Kontrolle sollten

- die Betroffenen und die Fachvorgesetzten beteiligt werden,
- eventuell betroffene Funktionsträger beteiligt oder zumindest fallweise hinzugezogen werden,
- die oder der behördliche Datenschutzbeauftragte beteiligt werden, wenn gemäß Prüfauftrag eine hohe Anzahl personenbezogener Daten oder besonders schutzbedürftige Daten von nicht direkt vom Prüfgegenstand erfassten Personen betroffen sind, und
- eine schriftliche Protokollierung der beteiligten Personen und jeder Einsichtnahme erfolgen. Hierbei muss jedes Öffnen einer E-Mail explizit nachvollzogen werden können, die Kommunikation mit besonders zu schützenden Funktionsträgern oder schutzwürdigen Inhalten, insbesondere privater Natur, enthält.

Danach sollte

- das erstellte Protokoll von allen Beteiligten unterzeichnet werden und
- das Protokoll an die Betroffenen übergeben werden.

Auch Aufsichtsbehörden müssen bei ihrer Tätigkeit datensparsam vorgehen. Das Öffnen eines E-Mail-Postfachs sollte mit einem hohen Maß an Transparenz und Nachvollziehbarkeit für die Betroffenen erfolgen.

6.6 Beratung des Rechenzentrums der CAU

Das Rechenzentrum der Christian-Albrechts-Universität (CAU) hat 2011 seinen internen Betrieb durch das ULD datenschutzrechtlich betrachten lassen. ULD und CAU vereinbarten regelmäßige Beratungen und Prüfungen.

Die Prüfungen und Bewertungen fanden direkt mit den einzelnen zuständigen Mitarbeiterinnen und Mitarbeitern statt. Dabei konnte die Aufmerksamkeit der fachlich versierten Mitarbeiter des Rechenzentrums auf Sicherheitsaspekte gelenkt werden, die im Tagesgeschäft gern aus dem Blick geraten. Durch das stark gewachsene Vertrauen in die Verlässlichkeit der einzelnen Administratoren, Studenten und Dienstleister waren organisatorische Regelungen, Abstimmungsprozesse, der laufende Wissenstransfer und die Dokumentation vernachlässigt worden. Oft wird die Bedeutung solcher Lücken erst im Schadensfall oder bei einem unerwarteten Personalwechsel wahrgenommen, da sie im laufenden Betrieb mit einem eingespielten Team kaum sichtbar werden. Ähnliches gilt, wenn Verpackungsmaterialien in Brand geraten oder bauliche Risiken zutage treten, die auf alte Gebäudesubstanz zurückzuführen sind.

Erst Dokumentationen sowie verbindliche Prozesse und Regelungen ermöglichen die Beherrschbarkeit des IT-Betriebs unabhängig von einzelnen Personen. Die Beachtung und die Umsetzung der Anforderungen der Datenschutzverordnung (DSVO) sind insofern elementar. Die IT-Verantwortlichen müssen einsehen, dass ihre Administratoren neben fachlichem Spezialwissen auch übergeordnetes Wissen bezüglich den Vorgaben und gesetzlichen Regelungen zum Datenschutz und zur IT-Sicherheit beherrschen müssen, und dafür sorgen, dass diese sich das Wissen aneignen.

Die datenschutzrechtliche Betrachtung des internen Rechenzentrumsbetriebs zeigte, dass ein Blick von außen auf einen im Grunde gut funktionierenden IT-Betrieb stets noch Optimierungspotenzial aufzeigen kann. Unsere Vorschläge und kritischen Anstöße wurden konstruktiv aufgenommen. Das Rechenzentrum der CAU ist mit der freiwilligen Bitte zur Betrachtung einen vorbildlichen Weg gegangen.

Was ist zu tun?

Andere Hochschulen des Landes sollten dem Beispiel folgen und gemeinsam mit dem ULD in einen kooperativen und vor allem regelmäßigen Prüf- und Bewertungszyklus einsteigen.

6.7 Intelligente Energieversorgung: Smart Meter

Smart Meter sind Geräte, die den Energieverbrauch eines Haushaltes zentral speichern und als Gateway zur automatisierten Verbrauchsübermittlung an das Energieversorgungsunternehmen dienen.

Aus Datenschutzsicht entsteht das Problem, dass bei häufigen Messungen über eine Analyse der Verbrauchsdaten Rückschlüsse auf Tätigkeiten von Personen im Haushalt möglich sind und hierdurch eine informationelle Beeinträchtigung der Unverletzlichkeit der Wohnung erfolgt. Die Daten können für Versicherungen interessant sein, für Finanzämter, für Sicherheitsbehörden oder für die Sozialforschung. Den Verbraucherinnen und Verbrauchern verspricht man beim Einsatz von Smart Metern mehr Transparenz und durch flexible Kostenmodelle, bei denen sich die Nachfrage am Angebot orientiert, eine rationalere Gestaltung des Verbrauchs sowie Kostenersparnisse. Über eine bessere Steuerung soll bei dem wechselhaften Energieangebot durch Wind- und Solarkraftwerke und bei der wechselhaften Energienachfrage gleichbleibender Komfort gewährleistet werden.

Um Energieunternehmen, Netzbetreibern und dem Verordnungsgeber eine Vorstellung davon zu vermitteln, wie Datenschutz beim Smart Metering gestaltet werden kann, veröffentlichten Datenschutzbeauftragte im Januar 2012 die „Orientierungshilfe für ein datenschutzgerechtes Smart Metering“. Deren Ausarbeitung erfolgte durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie den Landesbeauftragten von Mecklenburg-Vorpommern, Berlin und Schleswig-Holstein. Zur Konkretisierung von § 21g Energiewirtschaftsgesetz (EnWG), der die Datenverarbeitung beim Smart Metering regelt, soll eine Verordnung erlassen werden. Die Orientierungshilfe zum Datenschutz macht hierzu Vorgaben und ergänzt eine technische Richtlinie (TR) zur Datensicherheit, die das Bundesamt für Informationssicherheit (BSI) für das zentrale Kommunikations-Gateway des Smart Meters angefertigt hat. Bislang gibt es noch keine Smart Meter, bei denen die Spezifikationen der TR umgesetzt sind.

Die Umstellung auf die Nutzung erneuerbarer Energieversorgung, die wegen erheblicher Schwankungen schwieriger als die bisher zu regulierende ist, führt zu einem Zielkonflikt: Um einen sorgsamen Umgang mit den endlichen Energieressourcen zu erreichen, bedarf es hierbei einer gewissen Kontrolle. Auf der anderen Seite stehen Bürger- und Freiheitsrechte, eine Funktionsbedingung für moderne Gesellschaften, die durch eine Überwachung des individuellen Verhaltens eingeschränkt werden. Es geht nun darum, leistungsfähige und umweltschonende Techniken zu entwickeln, bei denen keine übermäßige Kontrolle der Menschen stattfindet. Gerade für Schleswig-Holstein haben alternative Modelle der Energieversorgung eine hohe wirtschaftliche Bedeutung. Dieser Zukunftsmarkt wird aktiv vom ULD unterstützt, das berät, wie Konzepte für ein datenschutzkonformes Messen und Steuern des Verhaltens der Verbraucherinnen und Verbraucher realisiert werden können.

07

KERNPUNKTE

Facebook

Verhaltensbasierte Internetwerbung

Rundfunkbeiträge

7 Neue Medien

7.1 Facebook

7.1.1 Die Verantwortlichkeit der Webseitenbetreiber bei Facebook Insights

Der Betrieb einer Facebook-Fanpage verstößt derzeit gegen geltendes Datenschutzrecht. Die Lösung ist alternativlos: Da Facebook bei der Bereitstellung der Hard- und Software für den Betrieb der Fanpages deutsches Datenschutzrecht missachtet, sind die Webseitenbetreiber rechtlich verpflichtet, ihre Fanpages zu deaktivieren.

Am 19. August 2011 veröffentlichte das ULD seine Analyse zur Facebook-Reichweitenanalyse „Facebook Insights“. Webseitenbetreiber, die eine sogenannte Facebook-Fanpage errichten, ermöglichen Facebook die Erhebung personenbezogener Nutzerdaten wie z. B. Internetprotokoll (IP)-Adressen und Cookie-Kennungen (IDs). Facebook verarbeitet diese Daten unter Verwendung der Cookie-IDs als Pseudonyme für Zwecke der Werbung und zur bedarfsgerechten Gestaltung von Telemedien. Registrierte Mitglieder sind zudem im Rahmen der Registrierung gegenüber Facebook verpflichtet, Familienname, Vorname und Geburtsdatum anzugeben. Facebook arbeitet im Rahmen der Profilbildung bei registrierten Nutzern mit Cookies, die die Verknüpfung eines Nutzungsdatums mit dem angemeldeten Facebook-Nutzer ermöglichen. Dieser Cookie ist für zwei Jahre aktiv, sodass auch eine namentliche Zuordnung über diesen Zeitraum hinweg möglich ist, z. B. wenn ein zunächst nicht angemeldeter Nutzer sich innerhalb des Aktivitätszeitraums des Cookies bei Facebook anmeldet. Die Nutzungsdaten verwendet Facebook zum Erstellen von Nutzerprofilen.

Facebook stellt für die Errichtung der Fanpage die technische Infrastruktur bereit und generiert aus den erhobenen Nutzungsdaten über die Art und den Umfang der Nutzung der Fanpage eine Nutzungsstatistik. Diese wird, soweit es sich um bei Facebook angemeldete Nutzer handelt, mit demografischen Angaben wie Alter, Geschlecht und Herkunft des jeweiligen Besuchers der Seite angereichert und als aggregierter und damit anonymer Nutzungsreport dem Webseitenbetreiber unter der Bezeichnung „Insights“ zur Verfügung gestellt.

Tatsächlich würde Facebook nicht die Nutzungsdaten der Fanpage erhalten, wenn diese nicht zuvor vom Webseitenbetreiber eingerichtet worden wäre. Dem Webseitenbetreiber wäre die Nutzung seiner Seite im Facebook-Netzwerk ohne die Zuarbeit des Konzerns möglich. Der Webseitenbetreiber verwendet die von Facebook automatisch zur Verfügung gestellte Nutzungsstatistik für eigene geschäftliche Zwecke. Auf Basis der erhaltenen Daten ist es z. B. einem kommerziellen Webseitenbetreiber möglich, das eigene Internetangebot an die Bedürfnisse, Wünsche und Interessen der Fanpage-Besucher anzupassen, eine stärkere Kundenbindung zu erzielen und Kundenakquise durchzuführen.

Durch das Einrichten der Fanpage leistet der Webseitenbetreiber einen aktiven und willentlichen Beitrag zur Erhebung personenbezogener Nutzungsdaten. Damit entscheidet der Webseitenbetreiber nicht nur über den Zweck der Erhebung, Verarbeitung und Nutzung der personenbezogenen Nutzungsdaten, sondern er entscheidet auch über das wesentliche Mittel der Datenverarbeitung. Ohne den Betrieb der Fanpage sind die konkreten Datenverarbeitungsprozesse nicht möglich; das Geschäftskonzept von Facebook zur Erstellung von Nutzungsprofilen wäre ohne die Kooperation mit den Webseitenbetreibern hinsichtlich der Nutzungsdaten nicht umsetzbar. Die Webseitenbetreiber sind deshalb auch für die Erhebung, Verarbeitung und Nutzung der Nutzungsdaten datenschutzrechtlich verantwortlich.

Für Zwecke der Werbung dürfen Nutzungsprofile bei Verwendung von Pseudonymen gemäß § 15 Abs. 3 Telemediengesetz (TMG) erstellt werden, sofern der Nutzer dem nicht widerspricht. Die Nutzer müssen der Bildung von Nutzungsprofilen widersprechen können und über die Möglichkeit eines Widerspruchs unterrichtet werden. Die Webseitenbetreiber unterrichten die Fanpage-Besucher nicht über ihr Widerspruchsrecht; sie stellen auch keine Widerspruchsmöglichkeit zur Verfü-

gung. Darüber hinaus besteht in der von Facebook zum Betrieb der Fanpage bereitgestellten Infrastruktur für die Webseitenbetreiber keine technische Möglichkeit zur Einrichtung eines Widerspruchsmechanismus. Diese technische Möglichkeit zum Widerspruch könnte Facebook eröffnen. Facebook hat jedoch in den mit dem ULD geführten Gesprächen bisher nicht zum Ausdruck gebracht, einen Widerspruchsmechanismus einrichten zu wollen.

Da die Webseitenbetreiber den Fanpage-Besuchern keine Widerspruchsmöglichkeit gegen die Bildung von Nutzungsprofilen eröffnen und sie darüber auch nicht unterrichten, verstoßen diese in ihrem Verantwortungsbereich gegen datenschutzrechtliche Bestimmungen des TMG. Das ULD hat Anfang Oktober 2011 sieben private und acht öffentliche Stellen angeschrieben und diese aufgefordert, die von ihnen betriebenen Fanpages abzuschalten. Eine öffentliche Stelle ist dem nachgekommen. Gegenüber sechs öffentlichen Stellen hat das ULD den Betrieb der Fanpages förmlich beanstandet. Gegen drei nicht öffentliche Stellen wurde eine Beseitigungsanordnung erlassen und ein Zwangsgeld in Höhe von 5.000 Euro für den Fall der Nichtbefolgung angedroht. Gegen die Beseitigungsanordnungen haben alle drei Stellen Widerspruch eingelegt. Das ULD hat die Widersprüche in Bescheiden zurückgewiesen, die allesamt noch im Dezember 2011 vor dem Verwaltungsgericht Schleswig angefochten wurden. Mit einer Entscheidung in den gerichtlichen Verfahren ist im Laufe des Jahres 2013 zu rechnen.

Sämtliche Dokumente, vor allem rechtliche Stellungnahmen Dritter, Pressemitteilungen sowie die Kommunikation mit Facebook, sind eingestellt unter:

https://www.datenschutzzentrum.de/facebook/

Was ist zu tun?

Webseitenbetreiber sind für die von ihnen initiierte Datenverarbeitung der Nutzer datenschutzrechtlich verantwortlich und müssen vor allem die Anforderungen des TMG beachten.

7.1.2 Facebook – Verfahren zur automatischen Erkennung von Gesichtern

Mithilfe eines Tools zur Erfassung und Auswertung biometrischer Daten entwickelte Facebook eine Gesichtserkennungsfunktion, um Personen auf Fotos unter Mitwirkung der Nutzer zu identifizieren. Das Verfahren wurde ohne Rechtsgrundlage betrieben und verstieß gegen die Persönlichkeitsrechte der auf den Fotos abgebildeten Personen.

Facebook setzt eine Gesichtserkennungssoftware ein, mit welcher die von registrierten Nutzern hochgeladenen Fotos erfasst und biometrisch ausgewertet werden. Die Ergebnisse der Vermessung von Gesichtsmerkmalen, z. B. die Erfassung des Abstandes von Nase zu Mund, verwendet Facebook zur Erstellung einer biometrischen Schablone, welche als temporäres „Template“ gespeichert wird. In einem weiteren Verfahrensschritt gleicht Facebook die temporären Templates mit dauerhaft verfügbaren Templates ab, um Übereinstimmungen zu ermitteln und im Falle einer hinreichenden Wahrscheinlichkeit dem registrierten Nutzer Markierungsvorschläge zu unterbreiten. Bei den dauerhaft verfügbaren Templates handelt es sich um Abbildungen von Personen, die mit dem registrierten Nutzer in einer „Freundschaftsbeziehung“ stehen. Die registrierten Nutzer werden mit den Markierungsvorschlägen dazu motiviert, eine Identifizierung abgebildeter Personen zu bestätigen oder zu verwerfen.

Facebook Inc. beabsichtigt mit dem Verfahren, die Namen der abgebildeten Personen zu ermitteln. Bei Einführung der Gesichtserkennungsfunktion durch Facebook wurden bei allen registrierten Nutzern die biometrische Erzeugung von Templates und die Unterbreitung von Markierungsvorschlägen ohne deren Einwilligung und ohne ausreichende Unterrichtung aktiviert. Auch bei neu registrierten Nutzern besteht eine entsprechende Voreinstellung. Die registrierten Nutzer mussten, wenn sie dies nicht wollten, in ihrem Account unter den „Privatsphäre-Einstellungen“ in einem verzweigten Klickpfad der Erstellung von Templates und der Zusendung von Markierungsvorschlägen widersprechen.

Die von Facebook erstellten biometrischen Erkennungsmuster und die hierzu verwendeten Bilddaten sind personenbezogene Daten, die als Kennzeichen aufgrund ihrer Verbindung mit einer bestimmten Person zur Identifizierung genutzt werden können. Die Besonderheit bei den biometrischen Daten besteht darin, dass sie im Gegensatz zu anderen personenbezogenen Daten lebenslang an die Person gebunden sind und sich nicht, wie z. B. Name und Anschrift, ändern lassen.

Eine wirksame Einwilligung der registrierten Nutzer als Rechtsgrundlage der Datenverarbeitung scheiterte bereits an der Bereitstellung einer leicht zugänglichen und leicht verständlichen Information über die beabsichtigte Datenerhebung, -verarbeitung und -nutzung. Die Informationen in den Nutzungsbedingungen und Datenverwendungsrichtlinien speziell zur Funktion der Gesichtserkennung mussten vom Nutzer mühsam ermittelt werden. Aus den Formulierungen ergaben sich nicht bzw. nicht klar die Funktion der Gesichtserkennung, die Zwecke der Datenverarbeitung und die Speicherdauer. Es fehlte ein Verfahren zur vorherigen Einwilligung in die Erhebung, Verarbeitung und Nutzung der biometrischen Daten. Die Funktion zur Gesichtserkennung wurde von Facebook ohne Information der Nutzer aktiviert. Mit der Voreinstellung hatten die Nutzer keine Möglichkeit, eine freie Entscheidung für oder gegen die Verarbeitung ihrer personenbezogenen Daten zu treffen. Auch jene Nutzer, die sich neu registrierten, erhielten keine entsprechende Wahlmöglichkeit und konnten erst nach der Registrierung und Aktivierung der Funktion diese wieder teilweise abschalten.

Das ULD hat im Anschluss an entsprechende Aktivitäten des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit Ende August 2012 gegen die Facebook Inc. ein verwaltungsrechtliches Kontrollverfahren eingeleitet, auf die Rechtswidrigkeit des Verfahrens hingewiesen und die Löschung der biometrischen Daten gefordert. Für den Fall der Nichtlöschung der Daten und der unveränderten Weiternutzung der Gesichtserkennungsfunktion wurde eine Beseitigungsanordnung angekündigt. Aufsichtsbehörden in weiteren Bundesländern hatten parallel verwaltungsrechtliche Verfahren gegen Facebook Inc. wegen der Gesichtserkennungsfunktion eingeleitet.

Zwischenzeitlich hat Facebook zum 15. Oktober 2012 eine Löschung der Templates bzw. der biometrischen Daten im Zusammenhang mit der Gesichtserkennungsfunktion für alle europäischen Nutzer zugesichert und die Voreinstellung für eine unterstellte Zustimmung in die Datenverarbeitung für Neuregistrierungen deaktiviert. Neu registrierte Nutzer sollen die Wahl haben, ob sie nach dem Anmeldeprozess die Gesichtserkennungsfunktion aktivieren wollen.

Was ist zu tun?

Facebook muss für sämtliche angebotenen Dienste die Anforderungen an wirksame Einwilligungen der Nutzer beachten. Hierzu zählen leicht verständliche und leicht auffindbare Informationen zu den Datenverarbeitungszwecken, eine Aufklärung vor der Abgabe einer Erklärung sowie klare Wahlmöglichkeiten des Nutzers, damit dieser frei entscheiden kann.

7.1.3 Facebook – Aufgabe der Pseudonymität oder Kontosperrung

Das ULD erreichten Eingaben von Nutzern aus Schleswig-Holstein zur Sperrung von Accounts durch Facebook, soweit die registrierten Nutzer beim Anmeldeprozess nicht ihre Klardaten, also Vorname, Nachname, Geburtsdatum, Geschlecht, eingegeben haben.

Nach der Kontosperrung verlangt Facebook von den Nutzern das Hochladen einer Kopie des Personalausweises, um auf diese Weise eine scheinbar sichere Identifizierung vorzunehmen. Anderenfalls soll keine Entsperrung erfolgen. Vom Nutzer kann nicht ohne Weiteres verlangt werden, zur Prüfung der Echtdaten eine Kopie des Personalausweises zu übersenden. Nach den Bestimmungen des Personalausweisrechts darf der Ausweis außer zum elektronischen Identitätsnachweis durch öffentliche und nicht öffentliche Stellen weder zum automatisierten Abruf personenbezogener Daten noch zur automatisierten Speicherung personen-

bezogener Daten verwendet werden. Nach der Intention des Gesetzgebers sollen hiervon alle Formen des vorbehaltlosen automatisierten Abrufs, insbesondere das Scannen, Fotokopieren und Ablichten, erfasst sein.

Mit seinen angebotenen Diensten hält Facebook eigene und fremde Telemedien zur Nutzung bereit und wird dadurch gegenüber den Nutzern als Diensteanbieter nach den Regelungen des Telemedienrechts tätig. Der Diensteanbieter hat nach § 13 Abs. 6 TMG die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren. Facebook verstößt mit dem angebotenen Registrierungsprozess unter www.facebook.de, bei welchem Familienname, Vorname und Geschlecht als Echtdaten eingegeben werden müssen, sowie mit der Forderung, eine Kontoentsperrung erst nach Eingabe der Echtdaten vorzunehmen, gegen die erwähnten gesetzlichen Vorgaben. Es ist dem Unternehmen Facebook technisch möglich und zumutbar, eine anonyme oder pseudonyme Nutzung von Telemedien sicherzustellen.

Anfang Oktober 2012 hat das ULD gegen die Facebook Inc. und gegen Facebook Ireland Ltd. jeweils ein verwaltungsrechtliches Kontrollverfahren eingeleitet und auf die Rechtswidrigkeit des Klarnamenzwangs hingewiesen. Facebook Inc. wies jedoch jede eigene Verantwortung von sich; deren Tochter, die Facebook Ireland Ltd., meint, dass sie alle maßgebenden Datenschutzbestimmungen einhält. Kurz vor Weihnachten 2012 erließ das ULD Beseitigungsanordnungen und ordnete deren sofortige Vollziehbarkeit an. Die Unternehmen legten hiergegen Widerspruch ein und beantragten beim Verwaltungsgericht (VG) Schleswig die Wiederherstellung der aufschiebenden Wirkung des Widerspruchs. Mit zwei Beschlüssen vom 14. Februar 2013 gab das VG Schleswig den Anträgen statt. Nicht deutsches, sondern irisches Recht sei anwendbar, auch wenn die gesamte Verkehrsdatenverarbeitung von Facebook mit den entsprechenden Profilbildungen in den USA erfolgt. Es soll danach keine Rolle spielen, dass das Unternehmen mit der Facebook Germany GmbH eine Niederlassung in Deutschland hat. Weiterhin sei nicht relevant, dass die wesentlichen Inhaltsdaten in Deutschland nicht nur erhoben, sondern hier auch von dem Dienstleister Akamai gespeichert und verarbeitet werden.

https://www.datenschutzzentrum.de/facebook/Facebook-Inc-vs-ULD-Beschluss.pdf

https://www.datenschutzzentrum.de/facebook/Facebook-Ireland-vs-ULD-Beschluss.pdf

Die Logik der Beschlüsse des VG Schleswig wäre, dass die One-Stop-Shop-Regelung, wie sie in einer europäischen Datenschutz-Grundverordnung – kombiniert mit einem ausgeklügelten Kooperationssystem der Aufsichtsbehörden – geplant ist, für die IT-Unternehmen gar nicht nötig wäre (Tz. 2.5). Es käme nur darauf an, die Konzernstruktur so zu gestalten, wie es Facebook tut, also eine Niederlassung in einem EU-Staat mit niedrigem Datenschutzniveau für zuständig zu erklären. Dies war nicht die Regelungsabsicht der Europäischen Union. Das ULD hat gegen die Beschlüsse des VG Schleswig vor dem Schleswig-Holsteinischen Oberverwaltungsgericht Beschwerde eingelegt.

Alle Dokumente zum aktuellen Verfahrensstand finden sich unter:

https://www.datenschutzzentrum.de/facebook/index.html

Was ist zu tun?

Facebook verstößt gegen das Recht auf informationelle Selbstbestimmung, wenn auf Bürgerinnen und Bürger zwecks Identifizierung Druck ausgeübt wird, obwohl das Unternehmen den Wunsch zur Pseudonymität respektieren muss. Es muss die Datenschutzregelungen des Telemedienrechts befolgen.

7.1.4 Facebook – Verstoß gegen die Safe Harbor Principles

Wegen des von Facebook angebotenen Dienstes „Facebook Insights", der Gesichtserkennungsfunktion und einem untauglichen Verfahren für die Nutzer zur Abstimmung über Änderungen der Facebook-Nutzungsbestimmungen hat das ULD die Federal Trade Commission (FTC) in Washington/USA als die für Facebook Inc. zuständige amerikanische Aufsichtsbehörde kontaktiert.

Im August 2012 informierte das ULD die FTC über Verstöße der Facebok Inc. gegen die Safe Harbor Principles. Das Unternehmen hatte sich im Rahmen einer Selbstzertifizierung entsprechenden Grundsätzen unterworfen und deren Einhaltung zugesichert. Zu diesen Grundsätzen zählt u. a. die Informationspflicht, wonach Privatpersonen darüber informiert werden müssen, zu welchen Zwecken ihre personenbezogenen Daten erhoben und verwendet werden. Die Wahlmöglichkeit verpflichtet Unternehmen, Privatpersonen die Chance zu unterbreiten, darüber zu entscheiden, ob ihre Daten an Dritte weitergegeben werden und eine Verarbeitung nur zu solchen Zwecken erfolgt, die mit dem ursprünglichen Erhebungszweck vereinbar sind. Die Ausübung des Wahlrechts muss durch leicht erkennbare und verständliche, leicht zugängliche und kostengünstige Verfahren ermöglicht werden.

- „Insights" – Informationspflicht: Facebook erhebt bei den Nutzern von Facebook-Webseiten, den sogenannten Fanpages, über den Cookie „datr" und die IP-Adressen Informationen zum Nutzerverhalten und verknüpft diese mit den Daten der Registrierung unter www.facebook.com (Name, Vorname, Geburtsdatum, Geschlecht). Facebook Inc. holt von den Nutzern keine Einwilligung für die Erhebung der Nutzerdaten und für die Verknüpfung mit den Registrierungsdaten ein. Die Nutzer haben keine Möglichkeit, der Nutzung der Daten für Werbezwecke zu widersprechen. Bereits im Rahmen der Registrierung werden die Nutzer nicht auf den Dienst „Insights" hingewiesen. Es erfolgt keine klare Information darüber, welche personenbezogenen Daten für welche Zwecke erhoben, verarbeitet und genutzt werden. Verwiesen wird der Nutzer lediglich auf die Datenverwendungsrichtlinien, die allgemeinen Geschäftsbedingungen und die Bestimmungen zur Cookie-Verwendung von Facebook, die ebenfalls keinen Hinweis auf den Dienst „Insights" enthalten. Zur Verknüpfung der Registrierungsdaten mit dem Cookie „datr" und den IP-Adressen erhält der Nutzer keine Hinweise. Dadurch wird das Safe Harbor Privacy Principle „Informationspflicht" verletzt.
- „Insights" – Wahlmöglichkeit: Die Verknüpfung der Registrierungsdaten mit dem Cookie „datr" und den IP-Adressen sowie die anschließende Verarbeitung zu Werbezwecken ist mit dem ursprünglichen Erhebungszweck (Registrierung) nicht vereinbar. Ursprünglich dienen die Registrierungsdaten nur dem Zweck, einen Zugang zum Facebook-Portal zu eröffnen. Einer anschließenden Verarbeitung der personenbezogenen Daten für Werbezwecke kann der Nutzer nicht widersprechen, da Facebook Inc. keine klaren und verständlichen sowie leicht zugänglichen Mechanismen bereitstellt, damit Nutzer ihr Wahlrecht ausüben können. Damit verletzt Facebook Inc. das Safe Harbor Privacy Principle „Wahlmöglichkeit".
- Gesichtserkennungsfunktion: Durch die biometrische Auswertung der Fotos und die Erstellung und Speicherung der Templates verletzte Facebook die Safe Harbor Privacy Principles „Informationspflicht" und „Wahlmöglichkeit". Die Nutzer erhielten weder im Rahmen des Registrierungsprozesses noch bei Durchsicht der Datenverwendungsrichtlinien und der allgemeinen Geschäftsbedingungen eine klare Information zum Verfahren der Gesichtserkennung. Für die Nutzer wurde nicht unmissverständlich zum Ausdruck gebracht, welche Mittel und Wege den Nutzern zur Verfügung stehen, um die Verwendung ihrer Fotos einzuschränken. Der Weg zur Deaktivierung der Funktion zur Gesichtserkennung war für den Nutzer sehr unübersichtlich, da über zahlreiche Schaltflächen im Rahmen der „Privatsphäre-Einstellungen" die gewünschte Funktion mühsam gesucht werden musste. Mit der biometrischen Auswertung der Fotos und der Erstellung und Speicherung der Templates kann Facebook auch Zwecke verfolgen, die mit dem ursprünglichen Erhebungszweck nicht vereinbar sind. Die Nutzer konnten nicht mittels eines leicht erkennbaren und verständlichen sowie leicht zugänglichen Verfahrens darüber entscheiden, ob sie der entsprechenden

Datenverarbeitung zustimmen oder widersprechen wollen.

- Abstimmungsverfahren I: Facebook behielt sich vor, seine allgemeinen Geschäftsbedingungen und damit auch die Privatsphäre-Einstellungen der Nutzer zu verändern. Erst wenn mehr als 7.000 Nutzer einen inhaltlichen Kommentar zu einer bestimmten geplanten Änderung hinterlassen, sollen registrierte Nutzer die Gelegenheit erhalten, an einer Abstimmung teilzunehmen, bei der Alternativen vorgeschlagen wurden. Das Ergebnis sollte für Facebook nur dann verbindlich sein, wenn sich mehr als 30 % der aktiven registrierten Nutzer ab dem Benachrichtigungsdatum an der Abstimmung beteiligten. Bereits der Umstand, dass der Nutzer erst dann eine Information zu geplanten Änderungen erhält, wenn er sich auf der „Facebook Site Governance"-Seite angemeldet hat, verstößt aus unserer Sicht gegen die Safe Harbor Privacy Principles „Informationspflicht" und „Wahlmöglichkeit". Das Erfordernis einer zusätzlichen Anmeldung, um überhaupt eine Information für eine beabsichtigte Änderung zu erhalten, vereitelt die Ausübung des Wahlrechts von Nutzern, da diese keine leicht erkennbaren und leicht zugänglichen Informationen bekommen. Vielen Nutzern bleibt auch die Information verborgen, dass überhaupt die Möglichkeit einer Abstimmung besteht.
- Abstimmungsverfahren II: Angesichts der von Facebook angegebenen Zahl von ca. 900 Millionen Nutzern weltweit ist eine Beteiligung von 30 % der aktiven Nutzer unrealistisch. Viele der Nutzer sind nicht aktiv, oder es handelt sich um gefälschte oder Firmenkonten. Die meisten aktiven Nutzer haben sich nicht bei separaten Anmeldeseiten angemeldet und erhalten keine Informationen über die Änderungen und die Abstimmung. Dem einzelnen Nutzer ist es unmöglich, einer Änderung seiner Privatsphäreeinstellungen und der nachträglichen Änderung der ursprünglichen Erhebungszwecke zu widersprechen.

Die FTC hat die Hinweise des ULD zur Kenntnis genommen und prüft diese nun in eigener Zuständigkeit. Im November 2012 kippte Facebook jegliche Form der Mitbestimmung nach Durchführung des genannten – gegen Safe Harbor verstoßenden – Abstimmungsverfahrens.

7.2 IPTV – die Sicht auf den Fernsehkonsum aus der Nähe

Zur Analyse seiner „Entertain"-Kundinnen und -Kunden sammelt die Telekom Nutzerdaten zum Fernsehkonsum. Diesen steht gegen eine pseudonyme Profilbildung ein gesetzliches Widerspruchsrecht zu. Dessen Umsetzung ist aus Sicht des ULD nicht gelungen.

Informationen darüber, wer wann welche Sendung konsumiert, haben hohe werbetechnische Relevanz. Daraus können Rückschlüsse auf Hobbys, berufliche und Freizeitinteressen, Lebensgewohnheiten, Familienverhältnisse, Bildungsstand, Finanzverhältnisse und politische Anschauungen gezogen werden. Fernsehsender und Unternehmen der Werbebranche haben ein großes Interesse daran, das TV-Nutzungsverhalten zu erforschen. Die Telekom beteuert, die Nutzerdaten nicht an Dritte weitergeben zu wollen. Vielmehr beabsichtige sie, die Informationen selbst ausschließlich zur bedarfsgerechten Gestaltung des eigenen Entertain-Angebots zu nutzen. Doch auch im letzteren Fall ist die Telekom an § 15 Abs. 3 TMG gebunden. Hiernach darf die Telekom als Diensteanbieter Nutzungsprofile bei Verwendung von Pseudonymen nur erstellen, wenn der Nutzer dem nicht widerspricht. Dies setzt allerdings eine klare Information über das Bestehen eines Widerspruchsrechts sowie ein leicht handhabbares Verfahren zur Ausübung desselben voraus.

Die Information über die Möglichkeit eines Widerspruchs erfolgte bei der Telekom nicht obligatorisch auf der Nutzeroberfläche des Media Receivers, sondern teilweise per Post und teilweise per E-Mail, wobei diese Mails sich von den üblichen Werbemails der Telekom nicht unterschieden. Auf dem Media Receiver musste zunächst ein nicht eindeutiger Klickpfad verfolgt werden. Zur Ausübung des Widerspruchsrechts müssen die Entertain-Kunden zunächst eine PIN eingeben. Diese PIN, die bei der Installation des Media Receivers bereitgestellt wurde, steht den TV-Nutzenden aber nicht in jedem Fall mehr zur Verfügung.

Das ULD hat dem für die Telekom zuständigen Landesbeauftragten für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen die er-

mittelten Informationen übersandt. Inzwischen stellt sich auf der Grundlage technischer Informationen durch den betrieblichen Datenschutzbeauftragten der Telekom die Frage, ob überhaupt pseudonyme Profile erstellt werden. Eine eindeutige Antwort hierzu konnte bisher nicht gefunden werden.

Die Nutzung von Internetfernsehen – kurz IPTV – wird in den kommenden Jahren in Deutschland massiv zunehmen und die bisherigen Zugänge zum Fernsehangebot über DVB-T- oder Satelliten-Antenne und über Kabel verdrängen. Sieht man in der Bereitstellung von IPTV einen Telemediendienst, so müssen die datenschutzrechtlichen Rahmenbedingungen des TMG beachtet werden, nicht nur durch die Telekom, sondern auch durch ausländische Anbieter.

Was ist zu tun?

Es ist dringend erforderlich, die allgemeinen datenschutzrechtlichen Rahmenbedingungen des Telemedienrechts für Internetfernsehen zu präzisieren, um nicht nach dem gläsernen Internetnutzer den gläsernen TV-Nutzer zu bekommen.

7.3 Verhaltensbasierte Werbung – Online Behavioural Advertising

Werbe- und Analyseunternehmen entwickeln immer ausgeklügeltere Verfahren, um Nutzerinnen und Nutzer im Netz zu verfolgen, zu typisieren und online zu identifizieren, um dann individualisiert Werbung ausliefern zu können. Dabei handelt es sich neudeutsch um „Online Behavioural Advertising“ – OBA.

Im November 2010 hatte ein Report des Ausschusses für Binnenmarkt und Verbraucherschutz des EU-Parlaments die „unfairen Praktiken der Wirtschaft“ angeprangert und die Europäische Kommission aufgefordert, eine Kennzeichnungspflicht für verhaltensbasierte Werbung einzuführen. Zuvor, im Dezember 2009, hatte die Europäische Union in Art. 5 Abs. 3 der E-Privacy-Richtlinie eine Regelung eingeführt, die beim Einsatz von sogenannten Cookies, die für die Erbringung eines Dienstes nicht erforderlich sind, eine Einwilligung der Betroffenen verlangt (sogenanntes Opt-In). Cookies werden von der Werbeindustrie zur Beobachtung und Identifizierung von Nutzerinnen und Nutzern beim Surfen im Internet im Rahmen des OBA zum sogenannten Tracking genutzt. Art. 5 Abs. 3 E-Privacy-Richtlinie wurde trotz Ablaufs der Umsetzungsfrist 2011 vom deutschen Gesetzgeber bis heute nicht umgesetzt. Dies hat dazu geführt, dass in Deutschland die Werbeindustrie ihre Praktiken nicht den verbraucherfreundlichen neuen gesetzlichen Vorgaben aus Brüssel angepasst hat.

Auch in anderen europäischen Ländern tut man sich schwer mit der Umsetzung. Seit Ende 2010 versucht sich die Europäische Kommission mit der Industrie am runden Tisch über eine praxistaugliche und zugleich rechtskonforme Lösung zu einigen – bislang ohne Erfolg. Die von der Industrie (EASA, iab-Europe) vorgeschlagenen Lösungen setzen die rechtliche Vorgabe des vorhergehenden Opt-Ins nicht um.

Die englische Datenschutzaufsichtsbehörde (ICO) hat im Jahr 2012 ein Verfahren akzeptiert, das die Anforderungen des europäischen Rahmenrechts nur unvollständig umsetzt, obwohl die Regelung gleichlautend ins englische Recht übernommen wurde. In England dürfen danach Tracking- und Analyse-Cookies gesetzt werden, bevor der Nutzer oder die Nutzerin eingewilligt hat. Im Gegensatz zu Deutschland wird aber in England seitdem zumindest auf den Umstand des Setzens von Cookies auf den Webseiten direkt hingewiesen.

Auch in den USA ist man sich der Problematik des Trackings und der verhaltensbasierten Werbung bewusst. Dort streitet die Industrie mit der zuständigen Verbraucherschutzbehörde, der Federal Trade Commission (FTC), über eine Selbstregulierung und deren Inhalte. Allerdings geht es in den USA lediglich um die Einführung eines sogenannten Opt-Outs, die Bereitstellung eines Widerspruchsverfahrens und die Frage, ob trotz eines Opt-Outs das Surfen von Nutzerinnen und Nutzern über Webseiten hinweg verfolgt und analysiert werden darf. Mit dieser Frage beschäftigt sich seit 2011 auch das World Wide Web Consortium (W3C),

ein Standardisierungsgremium der Internetindustrie – ebenfalls bislang ohne Erfolg.

Verhaltensbasierte Werbung

Dabei wird Verbrauchern auf Webseiten Werbung gezeigt, die zu ihrem Profil passt. Die Profile ermitteln die Werbeunternehmen, indem sie aufzeichnen, welche Webseiten Verbraucher besuchen und welche Links sie verfolgen.

Das ULD hat sich in die europäischen und internationalen Diskussionen eingebracht, zumal es sich hierbei um eine wichtige Fragestellung bei der europäischen Datenschutzzertifizierung handelt (33. TB, Tz. 9.3.2), und bezog in einem umfassenden Positionspapier zur Umsetzung des Art. 5 Abs. 3 E-Privacy-Richtlinie Stellung.

https://www.european-privacy-seal.eu/results/Position-Papers/20110530 e-privacy Art 5III-en.pdf

Nicht alle Arten von Cookies werden von dem neuen Einwilligungserfordernis erfasst. Keine vorherige Einwilligung ist erforderlich für Cookies, deren alleiniger Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist, und für Cookies, die unbedingt erforderlich sind, damit der Anbieter eines vom Nutzer ausdrücklich gewünschten Telemediendienstes diesen erbringen kann. Die Artikel-29-Datenschutzgruppe hat in ihrer Stellungnahme 04/2012 zu den beiden Ausnahmen von der Einwilligungspflicht Hilfestellung gegeben. Befreit vom Einwilligungserfordernis sind beispielsweise Warenkorb-Cookies und Cookies zur Authentifizierung beim Online-Banking. Keine Ausnahme greift jedoch insbesondere hinsichtlich Cookies, die zu Werbezwecken oder zu Zwecken der Webanalyse verwendet werden.

Was ist zu tun?

Der deutsche Gesetzgeber muss endlich die Regelung der E-Privacy-Richtlinie im deutschen Recht umsetzen. Bis dahin muss das europäische Recht direkt angewendet werden.

7.4 Rundfunkänderungsstaatsvertrag

Die Chance, bei der Umstellung der bisherigen Rundfunkgebühr auf einen Rundfunkbeitrag das Prinzip der Datensparsamkeit gesetzlich umzusetzen, wurde vertan.

Seit Anfang 2013 zahlen die Menschen in Deutschland keine Rundfunkgebühren mehr, sondern einen Beitrag. Während die Rundfunkgebühr davon abhängig war, dass ein Rundfunkgerät, also ein Radio und/oder ein Fernseher, zum Empfang bereitgehalten wird, wird nunmehr jeder Haushalt mit einer Abgabe belastet, unabhängig davon, ob ein solches Gerät vorhanden ist oder nicht. Der Wechsel war notwendig geworden, weil inzwischen Computer, Smartphones und andere elektronische Geräte zum Rundfunkempfang geeignet sind. Die Überprüfung, ob solche Geräte vorhanden sind, erschien nicht mehr zeitgemäß, weil diese inzwischen derart klein sind, dass sie mit den bisherigen Methoden von Gebührenbeauftragten, die im Zweifel Hausbesuche durchführten, nicht effektiv ermittelt werden können. Die bisherigen Methoden der Ermittlungen stießen zudem in der Öffentlichkeit auf viel Unmut. Die GEZ-Spitzelei wurde weitgehend als unverhältnismäßig wahrgenommen.

Der Umstieg auf die Haushaltsabgabe wäre nun die Chance gewesen, auf die bisherigen umfangreichen Datenerhebungen zur Kontrolle der Zahlungspflicht zu verzichten, worauf die Datenschutzbeauftragten des Bundes und der Länder schon früh und immer wieder hingewiesen haben. Leider wurden sie aber – wieder einmal – bei der Ausarbeitung des 15. Rundfunkänderungsstaatsvertrages (RÄStV) nicht gehört bzw. berücksichtigt. Den Länderparlamenten wurde ein Gesetzeswerk vorgelegt, dass eine noch umfassendere Bespitzelung befürchten ließ:

- Die Beitragspflichtigen werden einer umfassenden Auskunftspflicht unterworfen.

- Beitragsrelevante Daten dürfen auch ohne Kenntnis der Betroffenen erhoben werden, wobei sowohl private wie auch öffentliche Datenquellen genutzt werden dürfen. Darunter können auch Vermieter bzw. Wohnungseigentümer fallen. Die Art der Daten und deren Quellen werden nicht näher präzisiert.
- Zusätzlich sind umfassende Datenübermittlungen von den Meldebehörden vorgesehen.
- Als Grundlage für die Beitragsbefreiung wurden Originalbescheide über den Empfang sozialer Leistungen vorgesehen, die ein Mehr an sensiblen Daten enthalten als das, was nötig ist.
- Analog den bisherigen Gebührenbeauftragten wird vorgesehen, dass Funktionsübertragungen auf private Dritte erfolgen.
- Im Fall einer Abmeldung muss der begründende Lebenssachverhalt dargestellt werden.

Das ULD trug seine Kritik an diesen Regelungen vor und stieß hierbei bei den Abgeordneten des Landtags auf offene Ohren. Das Problem war jedoch, dass einzelne Bundesländer keine Änderungen am Staatsvertrag vornehmen konnten, ohne das Gesamtwerk infrage zu stellen. Deshalb beschloss der Landtag, ebenso wie andere Länderparlamente, man möge von den gesetzlichen Ermächtigungen in der Praxis nur begrenzt Gebrauch machen. Die gesellschaftliche Akzeptanz des neuen Beitragsmodells stand auf dem Spiel.

https://www.datenschutzzentrum.de/rundfunk/stellungnahme-15-rundfunkaenderungsstaatsvertrag.html

Die datenschutzrechtliche Kritik blieb diesmal nicht völlig ungehört. In „Eckpunkten für eine Konkretisierung der datenschutzrechtlichen Regelungen im Vollzug des 15. RÄStV“ von den öffentlichen Rundfunkanstalten wird nun versucht, die ausufernden Datenerhebungsregelungen in der Praxis einzuschränken:

- Der Grundsatz der Direkterhebung beim Betroffenen soll beachtet werden.
- Von der Erhebungsbefugnis bei Dritten soll nur ausnahmsweise zur Identifizierung von Beitragsschuldnern Gebrauch gemacht werden, wobei insbesondere an die Datenbeschaffung bei Meldebehörden, Handels- und Gewerberegistern sowie Grundbuchämtern gedacht sei.
- Die Anmietung von Adressdaten wird zwei Jahre ausgesetzt. Danach erfolgt eine Datenbeschaffung nur beim Adresshandel.
- Der Nachweispflicht zu Beitragsbefreiungen und -ermäßigungen soll im Rahmen des Möglichen durch datensparsame Drittbescheinigungen genügt werden.
- Die Gründe für eine Abmeldung sollen typisiert angegeben werden können, ohne dass sensible Motive erfragt werden.
- Vermieteranfragen sollen nur ausnahmsweise erfolgen, wenn weniger einschneidende Ermittlungsmaßnahmen erfolglos bleiben.

Die Rundfunkanstalten erwägen, diese „Konkretisierungen“ in einer noch zu schließenden Verwaltungsvereinbarung oder Satzung zu übernehmen.

http://www.ard.de/intern/standpunkte/-/id=2757264/property=download/nid=8236/13biet0/Eckpunkte+Datenschutz.pdf

Die Konkretisierungen bleiben hinter dem zurück, was von uns Datenschutzbeauftragten angeregt und gefordert wurde. Zunächst startet die frühere Gebühreneinzugszentrale (GEZ) mit einem einmaligen Meldedatenabgleich in allen Bundesländern. Auf Vermieter- und Eigentümeranfragen soll zunächst völlig verzichtet werden. Auf eine Nachforschung, wer alles in einer Wohnung wohnt, will man verzichten, solange ein Beitragszahler vorhanden ist. Ob diese Maßnahmen tatsächlich zu einer Einschränkung der Bespitzelung führen, muss die Praxis erweisen.

Was ist zu tun?

Beim Start der Beitragspflichtermittlung ist genau auf den Grundsatz der Datensparsamkeit zu achten. Bei der nächsten Rundfunkstaatsvertragsänderung sind die bestehenden ausufernden Regelungen auf das unbedingt Erforderliche zurückzuführen.

08

KERNPUNKTE

Vertrauenswürdige Identitäten

Online-Datenschutzauskunft

Sicherheitsforschung

8 Modellprojekte und Studien

Neben seiner Prüf- und Beratungstätigkeit beteiligt sich das ULD an drittmittelfinanzierten Projekten und Studien mit besonderen Datenschutzbezügen. Ziel ist es, über das gesetzlich geforderte Mindestmaß an Datenschutz und Datensicherheit hinauszugehen und datenschutzfördernde Technik zu entwickeln, die den Bürgerinnen und Bürgern in Schleswig-Holstein zugutekommt. Auch in den beiden vergangenen Jahren beteiligte sich das ULD an Projekten und Studien, von denen das ULD und damit auch das Land sowohl finanziell als auch durch die Aneignung von Know-how im Bereich Datenschutz profitiert (Tz. 8.1 bis Tz. 8.9).

Koordiniert werden solche Projekte durch unser Innovationszentrum Datenschutz & Datensicherheit (ULD-i), das interessierten schleswig-holsteinischen Unternehmen und Hochschulen für die Implementierung von Datenschutz und Datensicherheit in ihren Projekten und Produkten zur Verfügung steht. Immer wieder merken wir, wie wichtig es ist, Datenschutz von Anfang an einzubeziehen: Wer „Privacy by Design“ bereits bei der Konzeption von Technik, Organisation und Geschäftsmodellen berücksichtigt, erlebt später keine bösen Überraschungen. Das Ziel für alle Forschungsprogramme und Projekte sollte es sein, die Erarbeitung von Datenschutzanforderungen und die Evaluation der Systeme als projektbegleitende Aufgabe in die Planung zu integrieren.

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

8.1 PrimeLife

Im Juni 2011 ist nach etwas mehr als drei Jahren das von der Europäischen Union (EU) geförderte Projekt PrimeLife zu Ende gegangen, in dem wir gemeinsam mit anderen Projektpartnern aus Wirtschaft und Wissenschaft Konzepte und Tools für Datenschutz- und Identitätsmanagement in der digitalen Welt entwickelt haben. Die Resultate stehen allgemein zur Verfügung.

„PrimeLife – Privacy and Identity Management in Europe for Life“ und das Vorgängerprojekt „PRIME – Privacy and Identity Management for Europe“ (u. a. 33. TB, Tz. 8.1) hatten als Schwerpunkt ein nutzergesteuertes Identitätsmanagement, bei dem die Nutzenden nur jeweils die nötigsten Daten über sich preisgeben müssen und sie auch anonym oder unter Pseudonym handeln können.

Die Resultate, die auf der Abschlussveranstaltung in Luzern/Schweiz im Rahmen der renommierten Konferenz IFIP SEC vorgestellt wurden, können sich sehen lassen. Am besten verschafft man sich anhand der „PrimeLife Primer“ einen Überblick über die Ergebnisse: Die „Primer“ sind ein- oder zweiseitig bedruckte Zettel, in denen das PrimeLife-Team zu verschiedenen behandelten Themen die wichtigsten Informationen zusammengestellt hat. Dazu gehören

- das soziale Netzwerk „Clique“, bei dem Nutzende ihre verschiedenen Bekanntenkreise und das, was sie jeweils über sich preisgeben, trennen können;
- das Verschlüsselungstool „Scramble!“, das dafür sorgt, dass nur Berechtigte im sozialen Netzwerk auf den Klartext der Nachrichten und Einträge im eigenen Profil zugreifen können;
- das Webangebot „Dudle“ zur Terminabstimmung, das datensparsame Varianten der Einträge und Kommentare ermöglicht;
- PrimeLifes Arbeiten zu „Policy Languages“ (Policy-Sprachen), d. h. von Computern automatisch interpretierbaren Aussagen zum Datenschutz, mit denen vor und während einer Interaktion Anbieter über ihre Datenverarbeitung und Nutzende über ihre Anforderungen an den Schutz ihrer Daten informieren können;
- Informationen zu „Privacy on Mobile Equipment“, d. h. zu Datenschutzkonzepten für Anwendungen auf Mobiltelefonen wie Smartphones, wo bestimmte Bereiche besonders abgesichert sind und die Nutzenden durch Policy-Sprachen unterstützt werden;
- das Plugin „Privacy Dashboard“ für den Webbrowser Firefox, das darstellt, ob und wie ein Anbieter einer angesurften Website die Aktionen seiner Nutzenden nachverfolgen kann und Schutzmechanismen gegen dieses Tracking bereitstellt.

Daneben hat sich das PrimeLife-Team mit attributbasierten Credentials beschäftigt, die nun einige

der Projektpartner im Rahmen des Projektes ABC4Trust (Tz. 8.2) weiterentwickeln und im Echteinsatz testen werden.

PrimeLife hat seine Ideen zum Datenschutz- und Identitätsmanagement außerdem in die technische Standardisierung bei verschiedenen Initiativen eingebracht (Tz. 11.6). Ein Großteil der entwickelten Software steht nach Abschluss des Projektes als Open Source über die Projekt-Website zur Verfügung.

http://www.primelife.eu/results/primer

http://www.primelife.eu/results/opensource

Was ist zu tun?

Das Thema „Datenschutz- und Identitätsmanagement" bleibt nach Abschluss von PrimeLife wichtig und ist noch kein Selbstgänger. Entwicklerteams für Anwendungen und Infrastrukturen sollten sich die Resultate von PrimeLife anschauen und geeignete Bausteine in ihre eigenen Konzepte integrieren. Nutzerinnen und Nutzer können für ihren Selbstdatenschutz Tools wie das Privacy Dashboard oder Scramble! verwenden.

8.2 ABC4Trust – vertrauenswürdige digitale Identifikation im Pilotversuch

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 Identitätsdaten für bestimmte vorab definierte (Missbrauchs-)Fälle unterstützt wird.

Seit November 2010 läuft das von der EU für vier Jahre geförderte Projekt „ABC4Trust – Attribute-based Credentials for Trust". Ziel ist die praktische Erprobung von datensparsamen Berechtigungsnachweisen in der digitalen Welt.

Das gesetzlich festgeschriebene Gebot zur Datensparsamkeit ist in der Praxis oft schwer umzusetzen, wenn zugleich ein Mindestmaß an Sicherheit erforderlich ist. Beispielsweise enthalten die zur Legitimation eines Kunden verwendeten Dokumente viel mehr Daten, als für den konkreten Zweck preisgegeben werden müssten. So erfährt ein Händler bei Vorlage einer Studienbescheinigung neben der Eigenschaft „Person ist Student" oft auch Name, Adresse, Geburtsdatum und Studienfach als quasi aufgedrängte Informationen. Besteht bei einem Ausweis in Papierform noch die Möglichkeit, einzelne Felder zu schwärzen oder beim Vorzeigen abzudecken, ist dies online mit vom Aussteller digital signierten Nachweisen, sogenannten Zertifikaten, bisher nicht möglich: Bei einmal vom Aussteller erteilten Zertifikaten kann der Inhalt nicht variiert werden, denn herkömmliche digitale Signaturen verlieren ihre Gültigkeit, sobald auch nur ein Teil der signierten Informationen entfernt oder geändert wird.

Anders ist dies bei attributbasierten Nachweisen, den „privacy-enhancing attribute-based credentials" oder kurz: Privacy-ABCs. Diese ermöglichen es, aus einem umfassenden Zertifikat einzelne Attribute zu bescheinigen, z. B. Name, Studierendeneigenschaft oder Geburtsdatum. Nutzerinnen

und Nutzer können die erforderlichen Angaben auch aus mehreren Zertifikaten von unterschiedlichen Ausstellern zusammenstellen. Die Signaturen und damit die Bescheinigungen der Aussteller, dass die Angaben korrekt sind, bleiben dabei erhalten. Privacy-ABCs erlauben es so, datensparsam bestimmte Eigenschaften gegenüber Dritten nachzuweisen, ohne die eigene Identität zu offenbaren.

Das ULD bearbeitet im Projekt ABC4Trust die grundlegenden datenschutzrechtlichen Fragestellungen von Privacy-ABCs. Hierzu werden sowohl der bestehende europäische Datenschutzrechtsrahmen als auch der Vorschlag zur europäischen Datenschutz-Grundverordnung herangezogen. Zudem beteiligt sich das ULD an der Vorbereitung der zwei geplanten Pilotprojekte, mit denen die Technologie getestet und evaluiert werden soll: Der eine Pilotversuch findet an einer weiterführenden Schule in Schweden statt; hier werden Privacy-ABCs als Zugangskontrolle für ein datensparsames soziales Netzwerk eingesetzt. Der andere Pilottest wird es Studierenden der Universität Patras in Griechenland ermöglichen, Lehrveranstaltungen zu bewerten, an denen sie in ausreichender Häufigkeit teilgenommen haben. Dies können die Studierenden mit auf Smartcards gesammelten Zertifikaten nachweisen, ohne beim Bewerten ihre Identität zu offenbaren.

Das Konzept der Privacy-ABCs ermöglicht einen sehr viel größeren Grad an Datensparsamkeit als herkömmliche Ansätze: In der Tat käme man beim Einsatz von Privacy-ABCs in vielen etablierten Verfahren der privaten Wirtschaft und bei Behörden mit weniger personenbezogenen Daten aus. Der Praxistest im Projekt soll helfen, die noch offenen Fragen, beispielsweise in Bezug auf die Bedienbarkeit und das Vermeiden von zusätzlichen Risiken im Betrieb, zu beantworten. Ideal wäre eine Verbreitung geeigneter Privacy-ABCs als Bestandteil einer zukünftigen europäisch vereinheitlichten Neuauflage digitaler Personalausweise, die allerdings noch in weiter Ferne zu liegen scheint. Wir beteiligen uns an dem Diskussionsprozess auf europäischer Ebene, z. B. im Rahmen der Initiative „SSEDIC – Scoping the Single European Digital Identity Community“ oder im Projekt FutureID (Tz. 8.3), und weisen auf das Potenzial von Privacy-ABCs für mehr Datenschutz hin.

http://www.abc4trust.eu/

Was ist zu tun?

Mit innovativer datenschutzfördernder Technik wie den Privacy-ABCs kann die Privatsphäre von Nutzenden und Geschäftspartnern geschützt werden. Dafür bedarf es konkreter Anreize für Unternehmen, diese Möglichkeiten einzusetzen. Nötigenfalls sind hier gesetzgeberische Maßnahmen auf nationaler und europäischer Ebene erforderlich.

8.3 FutureID – Wie soll die Zukunft von elektronischen Identitäten aussehen?

Mit der Einführung des neuen Personalausweises (nPA) hat Deutschland einen großen Schritt für eine Verwendung von elektronischen Identitäten in der Online-Welt gemacht. Dennoch steht die Entwicklung erst am Anfang.

Viele Fragen sind noch zu klären, bevor ein interoperabler, grenzüberschreitender und vertrauenswürdiger Einsatz von elektronischen Identitäten (eIDs) möglich sein wird. Das Projekt FutureID leistet hierzu Grundlagenarbeit. Das im November 2012 gestartete EU-Projekt „FutureID – Shaping the Future of Electronic Identity“ verfolgt ein ehrgeiziges Ziel: In den drei Jahren Laufzeit sollen die insgesamt 19 Projektpartner aus elf europäischen Ländern eine Vorlage für den vertrauenswürdigen Einsatz von elektronischen Identitäten erarbeiten. Dabei spielen eIDs, wie sie in verschiedenen Ländern geplant oder sogar bereits eingeführt sind, ebenso eine Rolle wie Public-Key-Infrastrukturen. Auch Konzepte wie die Privacy-ABCs (Tz. 8.2) werden bei FutureID eingebunden.

Die erste Projektphase ist geprägt von einer umfassenden Erhebung der Anforderungen, beispielsweise aus den Bereichen Technik, Recht und Sozioökonomie, sowie spezieller zu Informationssicherheit, Privatsphärenschutz, Usability, Barriere-

freiheit und Inklusion. Überall, wo wir Berührungspunkte mit dem Datenschutz sehen, bringen wir uns ein. Dazu orientieren wir uns an den Datenschutz-Schutzzielen Transparenz, Intervenierbarkeit und Nichtverkettbarkeit (32. TB, Tz. 6.9), die mittlerweile auch Eingang in das novellierte Landesdatenschutzgesetz gefunden haben (Tz. 1.1).

Elektronische Identität

Der Sammelbegriff „elektronische Identitäten" umfasst alle möglichen Arten von Daten und Mechanismen, die zu einer Authentisierung oder Identifizierung oder zum Nachweis von bestimmten Merkmalen (z. B. Altersverifikation) einer Person in der Online-Welt geeignet sind.

Die Abkürzung „eID" wird zumeist dann verwendet, wenn die elektronischen Identitäten an ein Personaldokument, eine Chipkarte oder ein anderes Hardware-Token gebunden sind. Beim neuen Personalausweis in Deutschland bezeichnet die eID-Funktion den elektronischen Identitätsnachweis, der je nach Konfiguration zur Authentisierung, zum selektiven Transfer von bestimmen, auf dem Ausweis gespeicherten Daten oder zur Volljährigkeits- oder Wohnortverifikation in Online-Transaktionen verwendet werden kann.

An dem geeigneten Rahmen für elektronische Identitäten wird in Europa auch in anderen Initiativen gearbeitet. Ein qualitativ eher zweifelhaftes Zwischenergebnis ist der im Juni 2012 vorgestellte Entwurf für eine „Verordnung des Europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt".

In der aktuellen Fassung des Verordnungsentwurfs ist von Datenschutz kaum die Rede; datensparsame Funktionalität wie bei Privacy-ABCs kommt nicht vor. Der Entwurf nimmt keine Rücksicht auf die Datenschutzfunktionalität des deutschen nPA. Stattdessen wäre zu befürchten, dass in jedem Mitgliedstaat zum Zweck der grenzüberschreitenden Authentisierung, beispielsweise beim Online-Einkauf, eine zentrale Stelle aufgebaut würde, die Personenidentifizierungsdaten zu prüfen hätte. Es besteht das Risiko, dass schon aus Haftungsgründen bei diesen Stellen große Datensammlungen entstehen, die ein Abbild aller grenzüberschreitenden Verwendungen dieser elektronischen Identitäten enthalten. Beispielsweise wäre dann gespeichert, wer wann wo grenzüberschreitend eingekauft, eine Verwaltungsdienstleistung genutzt oder sich an einer Petition beteiligt hat.

Hier ist dringend eine Änderung geboten. FutureID wird durch seine Vorschläge für die Ausgestaltung elektronischer Identitäten und einer entsprechenden Infrastruktur Alternativen aufzeigen.

http://www.futureid.eu/

Was ist zu tun?

Die Europäische Kommission muss Datenschutzanforderungen in Bezug auf elektronische Identitäten ernst nehmen und dies in ihren Regelungen deutlich machen. Wir werden im Rahmen von FutureID Vorschläge vorlegen.

8.4 TClouds – Trustworthy Clouds

Das von der EU geförderte Projekt „TClouds – Trustworthy Clouds" forscht seit über zwei Jahren an Lösungen, um Datenschutz und Informationssicherheit für Cloud Computing zu gewährleisten.

Seit dem Start des Projektes im Oktober 2010 hat das ULD zusammen mit Projektpartnern aus Wissenschaft und Wirtschaft verschiedene Ansätze erarbeitet, um vertrauenswürdiges Cloud Computing zu ermöglichen (siehe auch Tz. 5.7). Zu den Ergebnissen gehören sowohl rechtliche Analysen und Hilfestellungen als auch technische Lösungen. Die im Projekt entwickelte Cloud-Computing-Plattform wird in drei technische Prototypen integriert:

- „Trusted Infrastructure Cloud“ – eine Cloud-Architektur basierend auf Trusted-Computing-Technik, die vor allem für den Einsatz als Private Cloud oder Community Cloud geeignet ist.
- „Trustworthy OpenStack“ – eine Erweiterung der freien Cloud-Computing-Software OpenStack um Tools, die die Sicherheit und Transparenz einer Public Cloud erhöhen können, z. B. Verschlüsselung, Remote Attestation und Logging Services.
- „Cloud-of-Clouds“ – eine föderierte Nutzung mehrerer Clouds, wodurch sich beispielsweise Verfügbarkeit und Integrität der gespeicherten Informationen erhöhen lassen.

Ein Großteil der entwickelten Software wird nach Abschluss des Projektes als Open Source zur Verfügung stehen.

Zusätzlich arbeitet das ULD im Rahmen von TClouds daran, die rechtlichen Rahmenbedingungen für Cloud Computing zu analysieren, zu evaluieren und praxisnahe Hilfestellungen für Anbieter und Kunden zu geben. Hierfür wurden relevante Cloud Assessment Schemes und Zertifizierungen untersucht und verglichen. Zudem erstellt das Projektteam eine Orientierungshilfe zur Vertragsgestaltung für grenzüberschreitende Cloud-Dienste nach geltendem Recht und entwickelt rechtspolitische Vorschläge. Die Ergebnisse der ersten zwei Projektjahre sind auf der TClouds-Website in englischer Sprache veröffentlicht:

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

Cloud Computing

Cloud Computing bedeutet die bedarfsgerechte Bereitstellung von informationstechnischen Dienstleistungen über Netze wie das Internet. Dies können Dienste in vielfältigen Formen sein, etwa Speicher- oder Rechenleistung, Entwicklungsumgebungen, Anwendungssoftware oder sogar vollständige Arbeitsumgebungen. Dies führt dazu, dass Daten der Dienstenutzenden nicht mehr lokal auf deren eigenen Systemen gespeichert und verarbeitet werden. Vielmehr wird über Netze auf diese Daten zugegriffen, wobei die Nutzenden in der Regel nicht mehr genau wissen, auf welchen Servern sich diese Daten befinden und was im Rahmen der Verarbeitungsprozesse mit diesen geschieht. Deshalb spricht man in diesem Fall von einer sogenannten Datenwolke, der Cloud.

Was ist zu tun?

Vor der Nutzung von Cloud Computing sollte der Kunde ein intensives Data Protection Risk Assessment, eine Datenschutzfolgenabschätzung, durchführen und geeignete vertragliche und technische Maßnahmen verlangen oder selbst implementieren. Wir werden im Rahmen von TClouds ein solches Risk Assessment für die genannten Prototypen durchführen.

8.5 Datenschutz-Auskunftsportal

Das Forschungsprojekt „Datenschutz-Auskunftsportal“ macht Verbesserungsvorschläge zur effektiven Umsetzung des datenschutzrechtlichen Auskunftsanspruchs.

Für Verbraucherinnen und Verbraucher ist es oft nicht einfach, von ihrem datenschutzrechtlichen Auskunftsanspruch gegenüber Unternehmen Gebrauch zu machen, obwohl Transparenz zu den Grundvoraussetzungen für Datenschutz gehört und hieran ein zunehmendes öffentliches Interesse besteht. Dies zeigen viele Anfragen und Eingaben beim ULD, die sich auf die Form und die Durchführung der Erledigung von Auskunftsanfragen sowie unterbliebene oder unvollständige Auskünfte beziehen. In diesen Fällen hat das Unternehmen meist versäumt, einen Prozess zur Erteilung von Auskunft aufzusetzen. Dadurch entstehen hinsichtlich der korrekten, vollständigen und rechtzeitigen Auskunftserteilung Defizite.

Diese Situation soll durch das Forschungsprojekt „Datenschutz-Auskunftsportal“ verbessert werden, das nach 15-monatiger Laufzeit im Oktober 2012 endete. Das Projekt zielt darauf ab, den Aufwand auf Verbraucherseite bei der Wahrnehmung des Auskunftsrechts deutlich zu verringern. Die Unterstützung für Verbraucherinnen und Verbraucher sollte vor allem darin bestehen, dass ihre Anfragen formuliert und an die Unternehmen direkt adressiert werden. Eine Internetplattform sollte zudem allgemeine Informationen zum Auskunftsrecht sowie standardisierte Schreiben an die Unternehmen anbieten. Zudem sollte Unternehmen die Abwicklung von Auskunftsanfragen mit Tools zur prozessgestützten Bearbeitung der Auskunftsersuchen erleichtert werden, auch um Aufwand und Kosten auf Unternehmensseite zu reduzieren.

Das Projekt wurde vom Kieler IT-Unternehmen Consist Software Solutions GmbH koordiniert und zusammen mit ConPolicy und dem ULD durchgeführt. Das ULD erarbeitete projektbegleitend die datenschutzrechtlichen Anforderungen an Datenschutz-Auskunftsportale. Ein zentraler Aspekt bestand in dem Entwurf eines Konzeptes, das möglichst datensparsam eine zentrale Datenhaltung über das Auskunftsverhalten der Anfragenden verhindert. Daran orientierte sich das entwickelte Labormuster, dessen Schwerpunkt auf einem Internetportal und der Interaktion mit den Verbraucherinnen und Verbrauchern liegt.

Die Ergebnisse des ULD wurden zum Projektende veröffentlicht und stehen allen Interessierten zur Verfügung. Die beiden Industriepartner prüfen, in welcher Form das Auskunftsportal seinen Echtbetrieb aufnehmen kann.

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

Was ist zu tun?

Die bestehenden und gesetzlich verankerten Verbraucherrechte im Bereich Datenschutz können durch Datenschutz-Auskunftsportale gestärkt werden. Diese müssen datensparsam vertrauenswürdige Lösungen anbieten, die zusätzliche Risiken für die Verbraucherinnen und Verbraucher vermeiden.

8.6 Anfragen zu Datenschutz in Online-Spielen nehmen zu

Im Rahmen des Projekts „DOS – Datenschutz in Online-Spielen“ veröffentlichten wir 2010 eine Studie und Leitfäden zu Datenschutzfragen rund um Online-Videospiele (33. TB, Tz. 8.5).

Zahlreiche Anfragen zu aktuellen Problemen und Fragen von Bürgern, Herstellern und Institutionen haben uns seitdem erreicht. Das Thema ist im Tagesgeschäft angekommen; die Probleme nehmen zu. Als wir 2007 mit dem Projekt DOS, gefördert vom Bundesministerium für Bildung und Forschung, begannen, gab es kaum eine Sensibilisierung für das Thema.

Die breite öffentliche Diskussion um „Origin“ von der Firma Electronic Arts (EA) Ende 2011 führte bei uns zu einer starken Zunahme besorgter Eingaben und Anfragen. Nutzende von PC-Spielen von EA, Battlefield 3 oder Fussball Manager 12 mussten zum Spielen die Software bzw. den Dienst „Origin“ installieren.

Dessen Datenschutzerklärung war so weit gefasst, dass sie die Analyse sämtlicher Dateien eines PCs im Hintergrund durch EA erlaubte, ohne dass die Spieler hierüber ausreichend informiert worden wären. EA musste aufgrund des öffentlichen Drucks – insbesondere der Spieler – seine Erklärungen präzisieren und zusichern, dass bestimmte Analysen, etwa von privaten Fotos, durch die Software nicht erfolgen. Inzwischen kam es durch den Verbraucherzentrale Bundesverband (vzbv), mit dem das ULD in engem Kontakt steht, zu ersten Abmahnungen von Spieleherstellern u. a. wegen unklarer Nutzungs- und Datenschutzbestimmungen.

Unsere aktuellen Analysen von neuen Online-Spielen und -Diensten wie Steam, Nintendo Network, Playstation Network usw. zeigen leider, dass in der Regel das gesamte Nutzungsverhalten von Spielerinnen und Spielern erfasst und ausgewertet wird, ohne dass diese das unterbinden

können und Informationen über Löschungsrechte oder eine anonyme bzw. pseudonyme Nutzung im rechtlich geforderten Maß erhalten. Selbst Auswertungen von Chats usw. behalten sich unter Verstoß gegen das Telekommunikationsgeheimnis einige Hersteller vor.

Was ist zu tun?

Nahezu alle großen Online-Spieleanbieter verstoßen gegen elementare Datenschutzvorgaben in Deutschland. Dieses „branchenübliche" Verhalten darf nicht weiter hingenommen werden. Spielende sind über ihre Rechte und Möglichkeiten aufzuklären. Zusammen mit Partnern wie dem vzbv müssen Hersteller und Betreiber von Online-Spielen nachdrücklich verpflichtet werden, sich an geltendes Recht zu halten.

8.7 SurPRISE – Sicherheit versus Privatsphäre aus Bürgersicht

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.

Das Projektakronym SurPRISE steht für „Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe". Wenn heute technische Lösungen zur Erhöhung der öffentlichen Sicherheit eingesetzt werden, stellen sich regelmäßig Fragen hinsichtlich damit einhergehender Eingriffe in die persönliche Freiheitssphäre der Bürgerinnen und Bürger durch Überwachungsmaßnahmen. Die Beeinträchtigung der Privatsphäre mag aus Sicht von Polizei und anderen Sicherheitsbehörden ein akzeptabler Preis für eine umfassendere Sicherheit, etwa vor terroristischen oder anderen schweren Straftaten im öffentlichen Raum, sein. Es liegen aber zumeist keine oder nur wenige genaue Erkenntnisse vor, ob die vermutete breite Akzeptanz von Bürgerinnen und Bürgern in Europa zum Wohle der öffentlichen Sicherheit das Meinungsbild tatsächlich widerspiegelt.

SurPRISE lenkt den Fokus auf die öffentliche Wahrnehmung des Einsatzes und der Auswirkungen von Sicherheitstechnologien. Zu diesem Zweck wird während der dreijährigen Projektlaufzeit eine repräsentative europaweite Bürgerbefragung durchgeführt. Diese soll das aktuelle Stimmungsbild von europäischen Bürgerinnen und Bürgern hinsichtlich der Folgen staatlicher Überwachung mittels moderner Sicherheitstechnologien einfangen. Des Weiteren wird erforscht, welche Anforderungen neuartige Sicherheitstechnologien erfüllen müssten, um aus Sicht der Betroffenen akzeptanzfähig zu sein. Hierbei kommen Möglichkeiten datenschutzgerechter Gestaltung von Sicherheitstechnologien ins Spiel.

Die Ergebnisse sollen in einen Anforderungskatalog für die Akzeptanzfähigkeit des Einsatzes staatlicher Sicherheitstechnologien einfließen. Dieser soll dann als Hilfestellung für die Gestaltung von Sicherheitsstrategien und entsprechenden legislativen Maßnahmen auf europäischer Ebene dienen. Die Aufgabe des ULD ist es, in Europa eingesetzte Sicherheitstechnologien und deren Auswirkungen auf die Privatsphäre von Bürgerinnen und Bürgern zu beschreiben und mögliche datenschutzfreundliche Ausgestaltungen solcher Technologien nach dem sogenannten „Privacy by Design"-Prinzip aufzuzeigen.

8.8 Multi-Biometrische 3D-Gesichtserkennung

Im Rahmen der Unterstützung der polizeilichen Ermittlungsarbeit durch technische Verfahren gewinnen visuelle Erkennungssysteme auf der Basis biometrischer Daten eine zunehmende Bedeutung. Hierbei sind die datenschutzrechtlichen Rahmenbedingungen zu beachten.

Die Gesichtsbilderkennung ist ein wichtiges Mittel zur polizeilichen Personenidentifizierung. Dabei werden tatrelevante Bilder, z. B. die Videoaufnahmen von einem Überfall, mit den Bilddaten von Personen verglichen, die in polizeilichen Dateien gespeichert sind. Derzeit erfolgt diese Identifizierung durch die zweidimensionale biometrische Gesichtserkennung. Dies ist – aus technischer Sicht – verbesserungsfähig. Im Projekt „GES-3D – Multi-Biometrische Gesichtserkennung" soll ein Verfahren entwickelt werden, das die polizeiliche Identifizierung von Straftätern aus tatrelevanten Foto-/Videodaten mittels Abgleich mit 3D-Gesichtsbilddaten ermöglicht.

An dem Verbundprojekt sind sieben Partner beteiligt – Industriepartner und Forschungseinrichtungen, das Bundeskriminalamt als Endanwender und das ULD. Die Förderung des Vorhabens erfolgt aus Mitteln des Bundesministeriums für Bildung und Forschung. Das ULD hat die Aufgabe, die datenschutzrechtlichen Rahmenbedingungen für die Gestaltung und den Einsatz des Systems projektbegleitend herauszuarbeiten und die Projektpartner in allen Bereichen zum Thema Datenschutz und Datensicherheit zu unterstützen.

Was ist zu tun?

Angesichts der immensen Eingriffe in das Recht auf informationelle Selbstbestimmung, die damit einhergehen, ist es bei der dreidimensionalen Gesichtserkennung unerlässlich, bereits in den Anfängen der Entwicklung die Weichen für eine datenschutzgerechte Ausgestaltung solcher Systeme zu stellen und eine aus datenschutzrechtlicher Sicht unzulässige Verwendung zu unterbinden.

8.9 MonIKA – Erkennung und Bekämpfung von Botnetzen und Cyber-Angriffen

Unter dem Titel „Monitoring durch Informationsfusion und Klassifikation zur Anomalieerkennung – MonIKA" fördert das Bundesministerium für Bildung und Forschung seit März 2012 für zwei Jahre ein Projekt zur Analyse und Bekämpfung von Botnetzen.

Botnetz

Ein Botnetz ist eine Menge von Computern, die mittels einer heimlich installierten Schadsoftware von Angreifern über das Internet ferngesteuert werden. Über Botnetze werden beispielsweise in großem Stil Spam-Mails verschickt, Angriffe auf Internetpräsenzen von Firmen und Organisationen durchgeführt oder sensible Daten privater Anwender, z. B. Kreditkartennummern oder Zugangsdaten zu Online-Diensten, gestohlen.

Nicht nur der massenhafte Versand unerwünschter E-Mails, sogenannter Spam-Mails, sondern auch im Internet durchgeführte Angriffe auf Computersysteme lassen sich häufig auf bestehende Botnetze zurückführen, bei denen die Computer einzelner Internetteilnehmer mit Schadsoftware infiziert und dann für entsprechende Angriffe missbraucht werden. Meistens geschieht dies ohne Kenntnis der jeweiligen Computernutzer, was die Erkennung und Bekämpfung der Botnetze erschwert.

Die Internet Service Provider (ISPs) bemerken in solchen Fällen oft ein ungewöhnliches Nutzungsverhalten (sogenannte Anomalie) bei Botnetz-infizierten Netzteilnehmern. Diese Information allein genügt jedoch nicht, um daraus umfassende und vollständige Informationen über ein eventuell aktives Botnetz zu gewinnen. Erst durch den Abgleich mit Anomaliedaten anderer ISPs kann ein Botnetz vollständig erfasst werden, sodass geeignete Gegenmaßnahmen eingeleitet werden können. Beispielsweise könnten Netzteilnehmer über Botnetz-Infektionen ihrer Systeme unterrichtet und bei der Löschung der Botnetz-Schadsoftware auf ihren Computern unterstützt werden.

Im Projekt MonIKA untersuchen wir Fragen der Zulässigkeit der Erhebung, Verarbeitung und Nutzung von Daten, um Botnetze erkennen und

bekämpfen zu können. Wir suchen nach Antworten, unter welchen Bedingungen Daten zum Zweck der Analyse von Angriffen weitergegeben und zusammengeführt werden dürfen. Wir berücksichtigen hierbei auch die auf EU-Ebene diskutierte Meldepflicht bei Cyber-Angriffen. Unser Beitrag mit dem Schwerpunkt Datenschutzrecht wird flankiert von der zivilrechtlichen Begutachtung durch das Institut für Informations-, Telekommunikations- und Medienrecht der Westfälischen Wilhelms-Universität Münster. Gemeinsam mit den technischen Projektpartnern, dem Fraunhofer-Institut FKIE und dem EADS-Unternehmen Cassidian, wollen wir geeignete Lösungen entwickeln. Eine wesentliche Rolle werden hierbei innovative Verfahren zur Anonymisierung und Pseudonymisierung spielen.

Was ist zu tun?

Bei der Bewertung der Datenerhebungen und Analyseverfahren für das Monitoring und das Bekämpfen von Botnetzen ist zu prüfen, welche Verfahren zur Anonymisierung und Pseudonymisierung geeignet sind.

09

KERNPUNKTE

Behördenaudit

Produktzertifizierung

Europäisches Gütesiegel

9 Audit und Gütesiegel

9.1 Datenschutzaudits

Das Datenschutz-Behördenaudit ist ein Erfolgsmodell. Das ULD führt kontinuierliche Auditverfahren durch. Fortschritt und Erfolg hängen hierbei immer direkt von den Ressourcen der datenverarbeitenden Stellen ab.

Auditverfahren unterliegen denselben Herausforderungen wie alle anderen IT-Projekte: Sie konkurrieren mit dem Tagesgeschäft, müssen sich geänderten Rahmenbedingungen anpassen und manchmal auch abgebrochen werden. Erfolgreiche Auditverfahren zeichnen sich dadurch aus, dass stetig und gleichmäßig am Audit gearbeitet wird. Die Auditverfahren in der Hansestadt Lübeck, der Stadt Glinde und der Unfallkasse Nord werden durch alle Beteiligten kontinuierlich bearbeitet und zielen auf einen erfolgreichen Abschluss hin.

Manchmal müssen Auditverfahren neu gestartet werden. Häufig liegt dies daran, dass sich der Auditgegenstand aufgrund neuer Anforderungen oder der technischen Weiterentwicklung stark geändert hat. Das vom Umweltministerium betriebene Auditverfahren „K3“ ist hierfür ein Beispiel. Das ULD und das Umweltministerium haben erkannt, dass der Auditgegenstand stark erweitert werden muss, um den Anforderungen an das Datenschutz-Behördenaudit zu genügen. Die bisher geleistete Arbeit in solchen Auditverfahren ist jedoch nicht vergebens. Die Ergebnisse können direkt im anschließenden neuen Auditverfahren verwendet werden und beschleunigen die Bearbeitung und Fertigstellung des Audits.

Selten müssen Auditverfahren ausgesetzt oder beendet werden, weil die ursprünglichen Annahmen zum betroffenen Verfahren oder zur Zertifizierungsfähigkeit sich bei der Durchführung als falsch erweisen. Aufgrund von engen personellen Ressourcen muss das Audit beim azv Südholstein weiterhin ruhen (33. TB, Tz. 9.1.7). Das Auditverfahren an der Christian-Albrechts-Universität musste ausgesetzt werden, weil ein neues Verwaltungsverfahren eingeführt wird. Die zuständigen Mitarbeiterinnen und Mitarbeiter müssen sich zunächst primär um die Einführung des Verfahrens kümmern. Das ULD und die Universität sind weiterhin bemüht, Datenschutz und Datensicherheit bei der Verwaltung von Studierendendaten mit einem Datenschutz-Behördenaudit zu prüfen.

9.1.1 KVSH

Seit Jahren arbeitet die Kassenärztliche Vereinigung Schleswig-Holstein (KVSH) intensiv mit dem ULD zusammen. Da war es nur folgerichtig, dass diese Zusammenarbeit irgendwann in Form einer Zertifizierung Früchte tragen würde. Bei der Einführung eines sicheren E-Mail-Dienstes für die in Schleswig-Holstein zugelassenen Ärztinnen und Ärzte hat die KVSH die Chance ergriffen. Das ULD hat das Datenschutz-Behördenaudit im November 2012 erfolgreich abgeschlossen.

Als Körperschaft öffentlichen Rechts nutzt die KVSH seit Jahren die Möglichkeit, sich vom ULD unentgeltlich in Sachen Datenschutz und Datensicherheit beraten zu lassen. Die dadurch immer datenschutzgerechter werdenden IT-Strukturen und -Verfahren der KVSH forderten die Verantwortlichen geradezu heraus, dieser Entwicklung ein öffentlichkeitswirksames Ziel zu geben. Da die KVSH plante, einen neuen sicheren E-Mail-Dienst für Arztpraxen aus Schleswig-Holstein anzubieten, wurde mit dem ULD ein Datenschutzbehördenaudit vereinbart. Wunsch der KVSH war es, die Konzeption und Umsetzung dieses neuen Dienstes nach datenschutzgerechten Gesichtspunkten offiziell überprüfen und bewerten zu lassen.

Für die KVSH ist Datenschutz von hoher Bedeutung, da die Verarbeitung von Patientendaten sehr sensibel ist. Um den Erfordernissen eines erfolgreichen Datenschutzaudits gerecht zu werden, mussten im Bereich der hauseigenen IT viele Dokumente überarbeitet werden, die nicht den Datenschutzanforderungen genügten. Die gesamte IT-Dokumentation ist nun auf dem aktuellen Stand. Die Umsetzung der Konzeption des eKVSH E-Mail-Dienstes umfasst angemessene und wirksame technische und organisatorische Sicherheits-

und Datenschutzmaßnahmen nach aktuellem Stand der Technik. Das Datenschutz- und Sicherheitsmanagement orientiert sich an internationalen Standards.

Datenschutz-Behördenaudit gemäß § 43 Abs. 2 LDSG Schleswig-Holstein: Konzeption und Umsetzung des „eKVSH E-Mail-Dienstes", Prüfnummer 28/2012, befristet bis 13. November 2015. Das Kurzgutachten mit den Ergebnissen der Auditierung ist veröffentlicht unter:

https://www.datenschutzzentrum.de/audit/register.htm

Der eKVSH E-Mail-Dienst ermöglicht es den teilnehmenden Arztpraxen, innerhalb eines geschlossenen Systems elektronische Nachrichten und Dokumente sicher zu versenden. Die Daten werden hierbei sowohl auf Inhaltsebene als auch auf Transportebene durch eine Ende-zu-Ende Verschlüsselung nach aktuellem Stand der Technik gegen den Verlust der Vertraulichkeit und der Integrität gesichert. Der Gegenstand des Audits umfasst das Konzept und die Umsetzung des Datenschutz- und Informationssicherheitsmanagementsystems. Ausdrücklich ausgenommen ist die netzwerktechnische Anbindung der Arztpraxen über das geschlossene Netzwerk „KV SafeNet". Ebenso nicht erfasst ist die korrekte Umsetzung der technischen und organisatorischen Sicherheitsmaßnahmen bei der Nutzung des Dienstes innerhalb der Arztpraxen.

Nach Übergabe der Auditurkunde im November 2012 prüfen die Verantwortlichen der KVSH, ob weitere Verfahren auditiert werden sollen. Der Datenschutz- sowie der IT-Sicherheitsbeauftragte der KVSH arbeiten mit einem Managementsystem für den Datenschutz und die Informationssicherheit, welches durch regelmäßige und anlassbezogene Kontrollen ein hohes Maß an Datenschutz sicherstellt. Definierte Prozesse zur Bearbeitung von Datenschutz- und Sicherheitsvorfällen sowie eine funktionierende Einbindung in IT-Projekte bereits in der Planungsphase sind geeignet, das hohe Niveau zu halten. Weitere Datenschutzauditierungen verursachen somit weniger Aufwand als beim ersten Mal und sind für die KVSH eine lohnende Option.

9.1.2 Kreis Plön

Der Landkreis Plön hat sein im Jahr 2007 zertifiziertes Kreisnetz wiederholt durch das ULD überprüfen lassen und verlängert so sein Datenschutzzertifikat um weitere drei Jahre. Damit setzt der Landkreis Plön seine IT-Sicherheitsstrategie konsequent fort und bleibt Vorreiter bei der Umsetzung von Datenschutz und Datensicherheit.

Dass der Kreis Plön Datenschutz und Datensicherheit auf einem hohen Niveau umsetzt, ist in Schleswig-Holstein längst bekannt. Er hat bereits 2007 das „Kommunale Kommunikationsnetz der Kreisverwaltung Plön" (Kreisnetz Plön) auditieren lassen. Es folgten im Jahr 2010 die Zertifizierung der Internetdienste E-Mail und WWW sowie eine Grundschutzzertifizierung der Basis-IT-Infrastruktur (33. TB, Tz. 9.1.1). Beim Kreisnetz Plön handelt es sich um eine netztechnische Infrastruktur auf der Plattform des Landesnetzes, über das Daten zwischen den Kommunen des Kreises Plön und der Kreisverwaltung ausgetauscht werden. Die Kreisverwaltung übernimmt für die organisatorische und technische Steuerung des Kreisnetzes die Verantwortung und tritt gegenüber den Kommunen als Netzbetreiber auf. Die Kreisverwaltung hat für ihr Netz folgende Datenschutzziele festgelegt:

- Herstellung einer für das Kreisgebiet flächendeckenden Kommunikationsinfrastruktur für die Kommunen,
- Datentransport im abgeschotteten Kreisnetz,
- Schutz der im Kreisnetz übertragenen Daten vor Angriffen aus dem Internet und aus angeschlossenen Nutzernetzen,
- einfache und revisionssichere Kontrolle der festgelegten Sicherheitsmaßnahmen durch die Nutzenden,
- Einhaltung der in der IT-Sicherheitsleitlinie festgelegten Sicherheitsziele und die damit verbundene Gewährleistung der Umsetzung des festgelegten Sicherheitsniveaus sowie
- Einrichtung einer IT-Sicherheitsorganisation durch die Festlegung von Zuständigkeiten.

Alle kreisangehörigen Kommunen sind am Kreisnetz Plön angeschlossen und nutzen die vom Kreis Plön zur Verfügung gestellten Dienste. Dazu zählt z. B. der zentrale Zugriff auf Fachprogramme und Daten der Kommunen und des Kreises. Im Rahmen der Rezertifizierung stellten wir fest, dass die Kreisverwaltung Plön die im Sicherheitskonzept fest-

gelegten Sicherheitsmaßnahmen dauerhaft umgesetzt hat. Im Jahr 2010 wurde die IT-Basisinfrastruktur der Kreisverwaltung Plön nach dem Zertifizierungsschema „ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz“ durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert. Das Zertifikat ist drei Jahre gültig, sofern jeweils nach einem bzw. zwei Jahren nach Zertifizierung ein sogenanntes Überwachungsaudit erfolgt. Dabei wird überprüft, ob das IT-Sicherheitsmanagement weiterhin wirksam ist und ob Änderungen an den IT-Systemen oder der Organisation so erfolgen, dass die IT-Sicherheit gewährleistet bleibt. Diese Überwachungsaudits im Sommer 2011 und im Sommer 2012 wurden erfolgreich abgeschlossen.

Was ist zu tun?

Der Kreis Plön muss diesen Sicherheitsstandard langfristig halten und sollte Leitbild für andere Kreisverwaltungen werden.

9.1.3 „ZIAF“ – Landwirtschaftsministerium

Das Ministerium für Energiewende, Landwirtschaft, Umwelt und ländliche Räume (MELUR) hat 2009 für die sichere Konzeption und den sicheren Betrieb seiner Agrarförderungszahlstelle (ZIAF) ein IT-Sicherheitszertifikat des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erhalten. Diese Zertifizierung auf der Basis von IT-Grundschutz nach dem Standard ISO 27001 (32. TB, Tz. 9.2.4) ist drei Jahre gültig, sofern jeweils nach einem bzw. zwei Jahren ein sogenanntes Überwachungsaudit erfolgt (Tz. 9.1.2).

Zur Erinnerung: Die Europäische Union (EU) macht sicherheitstechnische Vorgaben für Stellen, die EU-Fördermittel für die Agrarförderung auszahlen. Damit sollen Ausfällen der Informationstechnik und Manipulationen vorgebeugt werden. Die Zahlstelle des MELUR umfasst auf der Seite der Vorgangsbearbeitung Client-Systeme im Ministerium, in nachgeordneten Behörden sowie weiteren beteiligten Stellen. Der Dienstleister Dataport betreibt die zentrale Server-Infrastruktur, auf der die relevanten Daten verarbeitet und gespeichert werden. Die Umsetzung der Vorgaben wurde überprüft und zertifiziert.

Im Rahmen von Überwachungsaudits erfolgt lediglich eine kursorische Überprüfung, ob das IT-Sicherheitsmanagement weiterhin wirksam ist und ob Änderungen an den IT-Systemen oder der Organisation so erfolgen, dass die IT-Sicherheit weiterhin gewährleistet ist. Eine nach drei Jahren mögliche Rezertifizierung hingegen erfordert wieder eine Auditierung, die im Umfang der Prüfung bei der Erstzertifizierung gleicht: Die Dokumentation – die Leitlinien, Komponentenlisten, Sicherheitsanalysen, Sicherheitskonzepte enthält – wird auf Vollständigkeit und Konsistenz überprüft. An mehreren Standorten erfolgt eine stichprobenartige Überprüfung der konkreten Sicherheitsmaßnahmen, die im Sicherheitskonzept festgelegt wurden. 2011 wurde das zweite Überwachungsaudit (33. TB, Tz. 9.1.3) und 2012 die Rezertifizierung erfolgreich abgeschlossen.

9.1.4 Nordbits

Die Nordbits erhielt als Dienstleister für die Kreise Nordfriesland und Schleswig-Flensburg für die Implementierung eines übergreifenden Datenschutz- und IT-Sicherheitsmanagements ein Auditzertifikat.

Im Jahr 2008 führten die Kreise Nordfriesland und Schleswig-Flensburg ihre IT-Abteilungen in ein gemeinsames Kommunalunternehmen, die sogenannte Nordbits AöR, zusammen. Ziel dieser Umstrukturierung war es, den laufenden IT-Betrieb in beiden Kreisen zu modernisieren und zu effektivieren. Im Kooperationsvertrag haben die Kreise mit der Nordbits AöR entsprechend ihrer IT-Sicherheitsleitlinie eine Datenschutzbeauftragte und eine IT-Sicherheitsbeauftragte bestellt, um die

Einhaltung von Datenschutz und Datensicherheit zu gewährleisten. Zu deren Aufgaben gehören

- die Unterstützung des technischen Leiters der Nordbits AöR bei der Umsetzung der IT-Sicherheitskonzeption der Kreise,
- die Unterstützung und Beratung der Fachbereiche in Datenschutzrechtsfragen,
- die Überwachung der Einhaltung der internen Datenschutzvorschriften,
- die Mitwirkung im gesamten Sicherheitsprozess, insbesondere bei der Erstellung des IT-Sicherheitskonzepts und der Systemsicherheitsrichtlinien,
- die Erstellung eines Realisierungsplans für IT-Maßnahmen einschließlich der Überwachung von deren Umsetzung,
- die Entgegennahme von Meldungen über IT-Sicherheitsvorfälle und Einleitung der für die Bearbeitung und Beseitigung erforderlichen Schritte sowie
- die Erstellung von Berichten für die jeweilige Leitungsebene auf Nachfrage über den Status quo der IT-Sicherheit.

Zu den im Rahmen des Datenschutzaudits geprüften Aspekten gehörten u. a. die Wirkungsweise des IT-Sicherheitsmanagements, die wichtigsten Handlungsfelder im IT-Sicherheitsprozess und die Erreichung der festgelegten Datenschutzziele.

9.1.5 Statistikamt Nord

Das Statistikamt Nord beauftragte das ULD, sein Landesinformationssystem (LIS) auf der Basis des IT-Grundschutzstandards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu begutachten.

LIS ist ein Verfahren zur zentralen Speicherung und Auswertung von verdichteten Statistikdaten. Die Daten werden in die LIS-Kernapplikation aus Anwendungen der amtlichen Statistik übernommen. Das LIS wird auf Servern des Dienstleisters Dataport in einem abgeschotteten Netzsegment betrieben. Der Zugriff erfolgt über Clients im Statistikamt Nord an den Standorten Kiel und Hamburg. Darüber hinaus werden aggregierte Daten für die Öffentlichkeit in einer sogenannten LIS Online-Datenbank zum Abruf bereitgestellt. Der Startschuss für die Freigabe der LIS Online-Datenbank erfolgte nach Übergabe des vom ULD erstellten Gutachtens.

Das ULD überprüfte gemeinsam mit dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) das Verfahren LIS. Der HmbBfDI kontrollierte gemäß seiner Zuständigkeit für das Statistikamt Nord die rechtlichen Anforderungen, das ULD die für das LIS umzusetzenden IT-Grundschutzvorgaben. Die Begutachtung wurde in folgenden Schritten durchgeführt:

- Prüfung der Dokumentation nach den Anforderungen des IT-Grundschutzstandards,
- Vor-Ort-Prüfung über den ordnungsgemäßen Einsatz des LIS beim Statistikamt Nord,
- Überprüfung des Auftragnehmers Dataport im Rahmen der Auftragsdatenverarbeitung (hierzu zählten die Begutachtung der Dokumentation sowie die stichprobenartige Prüfung der Umsetzung von Grundschutzmaßnahmen vor Ort),
- datenschutzrechtliche Bewertung der Datenverarbeitung durch den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit.

Die stichprobenartige Überprüfung ergab, dass die Anforderungen des IT-Grundschutzstandards vom Statistikamt Nord und von dem Dienstleister Dataport vorbildlich erfüllt werden. Auch die datenschutzrechtliche Überprüfung des HmbBfDI wurde erfolgreich abgeschlossen.

Was ist zu tun?

Eine vollständige Umsetzung des IT-Grundschutzstandards setzt voraus, dass das Statistikamt Nord auch die anderen von ihr eingesetzten Fachverfahren in die Auditierung einbezieht.

9.2 Datenschutz-Gütesiegel Schleswig-Holstein

9.2.1 Abgeschlossene Gütesiegelverfahren

In den Jahren 2011 und 2012 wurde sieben Produkten erstmalig ein Datenschutz-Gütesiegel verliehen. Sechzehn weitere Produkte wurden nach Fristablauf der bestehenden Zertifizierung in einem vereinfachten Verfahren rezertifiziert.

Die Zahl von Rezertifizierungen zeigt, dass sich für die Hersteller das Gütesiegel lohnt. In einigen Branchen, etwa bei Schredderunternehmen, hat das Gütesiegel eine hohe Marktdurchsetzung. Nach Inkrafttreten der neuen Norm für Akten- und Datenträgervernichtung DIN 66399 haben sich aktuelle und zukünftige Zertifizierungsverfahren in diesem Bereich nun hieran zu orientieren. Für Produkte, die Teil eines Krankenhausinformationssystems sind, legt die unter den Datenschutzaufsichtsbehörden abgestimmte „Orientierungshilfe Krankenhausinformationssysteme“ (OH KIS) einen neuen Prüfmaßstab fest. Im Rahmen der Rezertifizierung des Produkts „Galileo 1.5“ konnten wir hiermit erste Erfahrungen sammeln.

Bei Anbietern von Targeting-Lösungen kam es zu Verzögerungen und Verschiebungen von zunächst angestrebten (Re-)Zertifizierungen. Grund hierfür ist die europäische E-Privacy-Richtlinie, die in Deutschland trotz Ablauf der Frist noch nicht vollständig umgesetzt ist und für das Setzen von Cookies durch Werbeanbieter in der Regel die ausdrückliche Einwilligung des Betroffenen verlangt (Tz. 7.3). Die dadurch notwendige Dienstanpassung wurde von den Anbietern bisher nicht ausreichend umgesetzt.

Folgende Produkte wurden u. a. neu zertifiziert:

- „ImmoSolve Central – Edition ImmoSolve Professional“, Version 3: Customer-Relationship-Management-System zur Unterstützung des Vertriebs von Immobilien (Vermietung),
- „RWAS (Archivsoftware)“, Version 1.2: Lagerverwaltungssoftware, die Prozesse der Aktenarchivierung in strukturierten Lagern unterstützt,
- „E-POSTBRIEF Kern“, Release 2.2: Plattform zur verbindlichen, vertraulichen und verlässlichen elektronischen Kommunikation für Privat- und Geschäftskunden,
- „ProCampaign“, Version 2.0: Multifunktionale, webbasierte Anwendung zur Unterstützung des Customer Relationship Managements bzw. Permission Marketings,
- „Codira PACS“, Version 9.1: Digitales Bildarchiv- und Kommunikationssystem für radiologische Bilder,
- „Verfahren zur Vernichtung von Akten“, Stand April 2012: Verfahren zur Vernichtung von Datenträgern in Papierform (inkl. Datenträger mit Informationsdarstellung in Originalgröße und Ordner) durch die REISSWOLF Deutschland GmbH,
- „DC+, DCM+, DC4, DCM4“, Stand Januar 2012: Lesegeräte zur Altersverifikation der Firma ICT Europe GmbH.

Nachdem 2011 eine relativ geringe Zahl an Anträgen für Neuzertifizierungen beim ULD einging, zogen die Nachfragen 2012 merklich an. Dennoch ist die Möglichkeit der Datenschutzzertifizierung in vielen Branchen noch unbekannt, insbesondere auch in Bereichen, in denen sensible Daten verarbeitet werden.

Weitere Informationen für Hersteller befinden sich im Internet unter:

https://www.datenschutzzentrum.de/guetesiegel/infos_hersteller.htm

Was ist zu tun?

In Branchen, in denen sensible personenbezogene Daten verarbeitet werden, muss besonders für das Gütesiegel geworben werden.

9.2.2 Sachverständige und Prüfstellen

2011 und 2012 wurden wieder zahlreiche Sachverständige für das Verfahren zur Erlangung des Datenschutz-Gütesiegels Schleswig-Holstein anerkannt.

Im Rahmen des zweistufigen Gütesiegelverfahrens erfolgt die Begutachtung der zu zertifizierenden Produkte durch beim ULD anerkannte Datenschutzsachverständige. Wer sich anerkennen lassen möchte, kann dieses für die Bereiche Recht oder Technik beantragen. Bei entsprechender Qualifikation ist auch eine Doppelzulassung möglich. Entsprechendes gilt für Prüfstellen. Voraussetzung für eine Anerkennung ist neben der Zuverlässigkeit und Unabhängigkeit der Nachweis der erforderlichen Fachkunde. Diese muss sich insbesondere auf den Datenschutzbereich und auf jahrelange praktische Erfahrungen erstrecken.

Die Attraktivität der Anerkennung als Sachverständiger bzw. sachverständige Prüfstelle hat dadurch zugenommen, dass diese auch dazu berechtigt, Gutachten zur Akkreditierung von De-Mail-Anbietern zu erstellen. De-Mail-Anbieter müssen im Rahmen ihrer Zulassung und Akkreditierung nachweisen, dass sie die datenschutzrechtlichen Anforderungen erfüllen. Als Nachweis dient ein Zertifikat des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), wofür der De-Mail-Anbieter dem BfDI ein Sachverständigengutachten vorlegen muss. Beim ULD anerkannte Sachverständige bzw. sachverständige Prüfstellen sind berechtigt, diese Gutachten zu erstellen.

Als Sachverständige/sachverständige Prüfstellen hinzugekommen sind 2011/2012:

- Mathias Reinis, Bonn (Recht/Technik),
- Karsten U. Bartels, LL.M., Berlin (Recht),
- Prof. Dr. Christoph Bauer, Hamburg (Technik),
- activeMind AG (Leitung: Klaus Foitzick), München (Recht/Technik),
- Marcus Reinberg, LL.M., Hamburg (Recht),
- Ulf Neumann, LL.M., Stuttgart (Recht),
- Kedua GmbH – Bereich Begutachtungen (Leitung: Frank Jander), Berlin (Recht),
- Dr. Peter Katko, München (Recht),
- Dr. Thomas H. Lenhard, Rotalben (Technik),
- Andreas Ebbersmeyer, Geesthacht (Recht/Technik),
- Dr. Robert Kazemi, Bonn (Recht),
- ditis Systeme, Niederlassung der JMV GmbH & Co. KG (Leitung: Andreas Zeller (Recht) und Monika Egle (Technik)), Bonn (Recht/Technik),
- Dr. Bruno Wildhaber, Schwerzenbach/Schweiz (Technik),
- PERSICON cert AG (Leitung: Prof. Dr. Rainer Rumpel (Technik) und Stefanie Brandis (Recht)), Berlin (Recht/Technik),
- Karsten Neumann, Stralsund (Recht),
- Prof. Dr. Lambert Grosskopf, LL.M. Eur., Bremen (Recht),
- Mission 100 e.V. (Leitung: Michael J. Erner (Recht) und Friedrich K. Abraham (Technik)), Bad Wörishofen (Recht/Technik),
- Dr. Frank Eickmeier, Hamburg (Recht),
- Intersoft consulting services AG (Leitung: Matthias Lindner), Hamburg (Recht/Technik),
- Dipl.-Inf. Friedrich Abraham, Hürth (Technik),
- SiCoDa GmbH (Leitung: Oliver Gönner (Recht) und Holger Filges (Technik)), Alfter (Recht/Technik).

Inzwischen sind beim ULD 56 Einzelsachverständige und 16 Prüfstellen registriert.

Im zeitlichen Zusammenhang mit der jährlich stattfindenden Sommerakademie (Tz. 13) findet jeweils ein Gutachterworkshop in Kiel statt. Von dieser Möglichkeit des Erfahrungsaustausches machen zahlreiche Sachverständige Gebrauch. Diskutiert werden aktuelle Erfahrungen mit Neu- und Rezertifizierungen, die Gestaltung von Gutachten, die Überarbeitung des Kriterienkatalogs, typische Fehler bei der Gutachtenerstellung, die aktuelle Gesetzgebung und Fragen des Marketings.

Weitere Informationen für Sachverständige befinden sich im Internet unter:

https://www.datenschutzzentrum.de/guetesiegel/akkreditierung.htm

Was ist zu tun?

Die Sachverständigen stellen einen wichtigen Faktor dar, um bei Herstellern Interesse für das Gütesiegel zu wecken. Ihr Antrieb, neue Produkte für das Gütesiegelverfahren zu gewinnen, ist zu unterstützen.

9.2.3 Überarbeitung des Gütesiegel-Anforderungskatalogs

Der Gütesiegel-Anforderungskatalog zu IT-Produkten ist Prüfgrundlage für die Sachverständigen. Gesetzesänderungen und die Einführung der Schutzziele im LDSG machten es notwendig, den Kriterienkatalog anzupassen und zu modernisieren.

Die Struktur des Anforderungskatalogs wurde beibehalten. Zu prüfen sind vier Komplexe: grundsätzliche technische Ausgestaltung des Produkts, Zulässigkeit der Datenverarbeitung, technisch-organisatorische Maßnahmen und Rechte der Betroffenen. Dies gewährleistet, dass Prüfungen nach dem alten Katalog mit neuen Untersuchungen vergleichbar sind.

Ein Prüfungsschwerpunkt liegt nunmehr bei den Schutzzielen, an denen sich IT-Produkte ausrichten müssen, wenn sie zertifiziert werden sollen: Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettbarkeit und Intervenierbarkeit. Die Herausforderung für die Sachverständigen besteht darin, die Gewichtung dieser Schutzziele vorzunehmen und so zu einem angemessenen individuellen 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 werden regelmäßig Erfahrungen im Zertifizierungsprozess u. a. mittels Beispielen den Sachverständigen zur Verfügung gestellt.

9.2.4 Zusammenarbeit mit EuroPriSe

Die Zertifizierungsverfahren des Datenschutz-Gütesiegels Schleswig-Holstein und von EuroPriSe lassen sich verbinden. Für viele Hersteller von IT-Produkten kann es sich lohnen, ein derartiges Kombiverfahren durchzuführen und damit Synergieeffekte zu nutzen.

Während das Datenschutz-Gütesiegel Schleswig-Holstein die rechtskonforme Einsatzmöglichkeit von IT-Produkten in Schleswig-Holstein nach deutschem Recht bestätigt, hat EuroPriSe vorrangig europäisches Recht – Datenschutzrichtlinien, Rechtsprechung und Auslegungen durch die Artikel-29-Datenschutzgruppe – im Blick. Will ein Hersteller national wie auch international mit seinem Produkt auftreten, kann ein Kombiverfahren sinnvoll sein. Zur Einsparung von Kosten ist es möglich, ein einzelnes Gutachten für beide Verfahren beim ULD als Zertifizierungsstelle einzureichen. Voraussetzung ist, dass die beteiligten Sachverständigen für beide Verfahrensarten anerkannt sind – was für zahlreiche Gutachter und Prüfstellen gilt. 2011 hat die Firma Consultix für ihr Produkt ProCampaign 2.0 ein solches Kombiverfahren erfolgreich durchgeführt. Weitere Anträge werden derzeit im ULD bearbeitet.

9.3 EuroPriSe – europäisches Datenschutz-Gütesiegel

Das europäische Datenschutz-Gütesiegel EuroPriSe ist aus einem von der Europäischen Kommission mit 1,3 Millionen Euro geförderten Projekt hervorgegangen. An seiner Entwicklung 2007 bis 2009 haben neben Partnern aus Forschung und Wirtschaft die französische und die Madrider Datenschutzbehörde (CNIL, APDCM) mitgewirkt (31. TB, Tz. 8.13). Seit 2008 ist das ULD als EuroPriSe-Zertifizierungsstelle tätig.

Vorrangige Arbeitssprache bei EuroPriSe ist Englisch. Seit Herbst 2012 stellt das europäische Datenschutz-Gütesiegel seine Webseite auch in deutscher Sprache zur Verfügung. Damit wird der Zugriff auf bereits vorhandene Fachinformationen in deutscher Sprache erleichtert. Eine Veröffentlichung der EuroPriSe-Kriterien in deutscher Sprache ist für das Frühjahr 2013 geplant.

https://www.european-privacy-seal.eu/criteria/kriterien

9.3.1 Zertifizierungskriterien

Das EuroPriSe-Zertifikat bescheinigt die Vereinbarkeit eines IT-Produkts oder einer IT-basierten Dienstleistung mit den Bestimmungen des EU-Datenschutzrechts. Die im Rahmen einer Zertifizierung zu prüfenden Kriterien sind aus den einschlägigen EU-Richtlinien abgeleitet und in einem Anforderungskatalog aufgelistet.

Dieser Katalog benennt Kriterien sowie die Rechtsnormen, aus denen diese jeweils abgeleitet werden. Er listet Fragen auf, die im Hinblick auf ein Kriterium regelmäßig von Relevanz sind. Der Katalog setzt sich aus vier thematischen Komplexen zusammen (31. TB, Tz. 9.4.1):

- 1. Komplex: Grundsätzliche Fragestellungen
- 2. Komplex: Rechtmäßigkeit der Datenverarbeitung
- 3. Komplex: Technische und organisatorische Maßnahmen der Datensicherheit
- 4. Komplex: Betroffenenrechte

Der englischsprachige Anforderungskatalog liegt gegenwärtig in der Version vom Mai 2011 vor und kann im Internet abgerufen werden unter:

https://www.european-privacy-seal.eu/criteria/

Eine deutsche Version des Anforderungskatalogs ist in Vorbereitung und wird ebenfalls unter der genannten Internetadresse zum Abruf bereitgestellt werden.

Die letzten inhaltlichen Änderungen der Kriterien erfolgten 2010 (33. TB, Tz. 9.3.1): Als Reaktion auf das Telekom-Reformpaket der EU wurden zwei neue Kriterien eingefügt: das Einwilligungserfordernis bei Cookies (Tz. 7.3) und die Benachrichtigungspflicht im Falle einer Kompromittierung personenbezogener Daten („Data Breach Notification“). Außerdem wurden Fragen zur Sicherheit von Webanwendungen ergänzt.

Nach Abschluss der Reform des Datenschutzrechtsrahmens auf EU-Ebene (Tz. 2.5) wird der Anforderungskatalog an die neue Rechtslage angepasst werden. Grundlegende Änderungen im Kriterienkatalog werden nicht erwartet, da viele der neuen Anforderungen, wie beispielsweise Dokumentationspflichten, bereits im Verfahren berücksichtigt sind.

9.3.2 Fachinformationen für EuroPriSe-Gutachter und Antragsteller

EuroPriSe hat weitere Fachinformationen für Gutachter, Antragsteller und Interessierte veröffentlicht. Hierzu zählen ein Informationsblatt zum Thema „Cloud Computing“, ein Positionspapier zur unmittelbaren Anwendbarkeit der neuen „Cookie-Richtlinie“ und ein Informationsblatt zu den von EuroPriSe-Gutachtern anzuwendenden Evaluationsmethoden.

Das jüngste Telekom-Reformpaket der EU führte zu einer Verschärfung der Anforderungen an eine rechtmäßige Verwendung von Cookies und ähnlichen technischen Hilfsmitteln (Tz. 7.3). Diese dürfen nach den rechtlichen Vorgaben auf EU-Ebene grundsätzlich nur noch dann verwendet werden, wenn der Nutzer seine Einwilligung hierzu erteilt hat. Der deutsche Gesetzgeber hat die

Umsetzungsfrist bis Mai 2011 untätig verstreichen lassen. Wir vertreten die Ansicht, dass die neue Cookie-Richtlinie mangels Umsetzung in nationales Recht unmittelbare Anwendung findet. Gestützt wird diese Argumentation durch die jüngste Rechtsprechung des Europäischen Gerichtshofs (Urteil vom 24. November 2011, C-468/10 und C-469/10, ASNEF/FECEMD). Das Positionspapier ist im Internet abrufbar unter:

https://www.european-privacy-seal.eu/results/Position-Papers

Im Juli 2012 veröffentlichte die Artikel-29-Datenschutzgruppe eine Stellungnahme zum Thema „Cloud Computing“ (Tz. 11.3). Das ULD nahm dies zum Anlass, die von der Gruppe getroffenen Aussagen zu Datenschutzfragen des Cloud Computing in einem Informationsblatt zusammenfassen, welches auch auf Besonderheiten des deutschen Datenschutzrechts hinweist. Das Informationsblatt ist im Internet abrufbar unter:

https://www.european-privacy-seal.eu/results/fact-sheets

Das ULD strebt als EuroPriSe-Zertifizierungsstelle an, dass die Evaluierung durch die Gutachter in verschiedenen Zertifizierungsverfahren insbesondere im Hinblick auf die technischen Gutachten eine vergleichbare Prüftiefe aufweist. So ist zu klären, ob eine Evaluation eine Vor-Ort-Prüfung (z. B. in einem Rechenzentrum) erfordert oder ob Funktionalitätschecks des IT-Produkts oder des Dienstes und die Durchsicht der Dokumentation ausreichen. Vor Beginn der Evaluierung ist das ULD über die geplanten Evaluationsmethoden zu informieren. Gegebenenfalls weist es die Gutachter darauf hin, dass die geplanten Evaluationsmethoden um weitere Prüfmaßnahmen zu ergänzen sind. In dem neuen Informationsblatt zu Evaluationsmethoden bei EuroPriSe-Zertifizierungen gibt das ULD akkreditierten Gutachtern Hilfestellung bei der Auswahl adäquater Evaluationsmethoden.

9.3.3 Zertifizierungsverfahren

Für den Aussagegehalt einer Zertifizierung ist die Transparenz des Verfahrens und der Kriterien sowie die Fachkunde und Vertrauenswürdigkeit der verleihenden Stelle maßgeblich. Allein öffentlich zugängliche Kriterien, ein transparentes Verfahren mit relevanten, ebenfalls veröffentlichten Ergebnissen, die eine Prüfbarkeit und Vergleichbarkeit sicherstellen, schaffen Vertrauen. Die finanzielle Unabhängigkeit der Zertifizierungsstelle stellt eine sachgerechte, unabhängige Prüfung und Vergabe der Siegel sicher. Aufbauend auf diesen Erkenntnissen wird das EuroPriSe-Zertifizierungsverfahren für IT-Produkte und IT-basierte Dienstleistungen durchgeführt (31. TB, Tz. 9.4.2). Fachkundige Sachverständige evaluieren den Prüfungsgegenstand, und in einem zweiten Schritt überprüft die unabhängige Zertifizierungsstelle das von den Sachverständigen eingereichte Gutachten auf Vollständigkeit, Nachvollziehbarkeit und Rechtskonformität. Sind alle Zertifizierungskriterien erfüllt, verleiht die Zertifizierungsstelle das EuroPriSe-Zertifikat. Dieses ist zwei Jahre lang gültig. Nach Ablauf dieser Zeitspanne oder bei wesentlichen Änderungen kann ein vereinfachtes Rezertifizierungsverfahren durchgeführt werden.

Alle erfolgreichen Zertifizierungen werden auf der EuroPriSe-Webseite veröffentlicht.

https://www.european-privacy-seal.eu/awarded-seals/

Neben den Angaben zum Produkt und Hersteller erstellt die Zertifizierungsstelle eine Übersicht mit den wesentlichen Angaben und Ergebnissen zum gesiegelten Produkt und Verfahren. Hier finden sich z. B. auch besondere Hinweise zur Nutzung. Über die Webseite kann das Kurzgutachten der Gutachter eingesehen werden.

IT-basierte Dienstleistungen und insbesondere webbasierte Dienste werden oft in kurzen zeitlichen Intervallen geändert, ohne dass dies für die Nutzenden transparent ist. Deshalb ist bei EuroPriSe das sogenannte Monitoring verpflichtend: Wurde ein IT-basierter Dienst zertifiziert, so muss er während der zweijährigen Gültigkeitsdauer des Siegels von den in das Verfahren involvierten Gutachtern auf seine fortwährende Vereinbarkeit mit den Zertifizierungskriterien überprüft werden. Aufgabe der Gutachter ist es zu verfolgen, ob datenschutzrelevante Änderungen an dem jeweiligen Dienst vorgenommen wurden. Die Anbieter von IT-basierten Dienstleistungen sind verpflichtet, acht Monate nach der Zertifizierung den Monitoring-Report bei der Zertifizierungsstelle einzureichen, der alle Änderungen und deren Bewertung beinhaltet. Ein weiterer Report ist nach 16 Monaten vorzulegen. Das Monitoring ersetzt nicht das erfolgreiche Durchlaufen eines Rezertifizierungsverfahrens.

Hersteller bzw. Anbieter können sich nach erfolgter Zertifizierung freiwillig dafür entscheiden, ihr Produkt bzw. ihre Dienstleistung von akkreditierten EuroPriSe-Gutachtern in regelmäßigen Abständen daraufhin prüfen zu lassen, ob es nach wie vor allen relevanten Zertifizierungskriterien genügt. Werden solche sogenannten Update Checks durchgeführt, werden damit besonders hohe Compliance-Anforderungen, wie sie z. B. bei sensiblen Finanz- oder Gesundheitsdaten bestehen, erfüllt. Beim Update Check sind im Anschluss an die Zertifizierung alle sechs Monate von den Gutachtern angefertigte Reports bei der Zertifizierungsstelle einzureichen. Bescheinigen die Gutachter dem IT-Produkt bzw. der -Dienstleistung fortdauernde Compliance mit den EuroPriSe-Zertifizierungskriterien und hat die Zertifizierungsstelle insoweit keine Einwände, so stellt sie nach Überprüfung des letzten, nach 24 Monaten einzureichenden Reports eine Rezertifizierungsurkunde aus. Die Gültigkeit des EuroPriSe-Zertifikats verlängert sich dann um weitere zwei Jahre.

9.3.4 Zulassung von Gutachtern

Als EuroPriSe-Gutachter dürfen nur Datenschutzexperten tätig werden, die das strenge EuroPriSe-Akkreditierungsverfahren erfolgreich durchlaufen und somit ihre Fachkunde nachgewiesen haben. Ende 2012 waren 141 Sachverständige aus 18 Ländern zugelassen.

Die Evaluierung der zu zertifizierenden IT-Produkte und -Dienstleistungen wird bei EuroPriSe durch akkreditierte Gutachter vorgenommen. Gutachter können bei Nachweis der nötigen Fachkunde für den Bereich Recht und den Bereich Technik akkreditiert werden.

Seit 2010 können technische und rechtliche Datenschutzexperten, die die für eine Akkreditierung als EuroPriSe-Gutachter erforderliche Berufserfahrung noch nicht in vollem Umfang aufweisen können, aber alle sonstigen Voraussetzungen für eine Zulassung als Gutachter erfüllen, als „EuroPriSe Junior Expert“ akkreditiert werden. Junior-Gutachter dürfen EuroPriSe-Evaluierungstätigkeiten durchführen, wenn ein Gutachter sie beaufsichtigt und die Verantwortung für ihre Tätigkeit übernimmt. Dadurch erhalten Datenschutzexperten die Möglichkeit, schon zu einem frühen Zeitpunkt ihrer beruflichen Karriere an EuroPriSe-Zertifizierungen mitzuwirken.

Datenschutzexperten mit Interesse an einer Akkreditierung müssen zusätzlich zum Nachweis ihrer Fachkunde und Zuverlässigkeit an einem Ausbildungsworkshop teilnehmen und ein Trainingsgutachten anfertigen, das den hohen EuroPriSe-Anforderungen entspricht. In den Jahren 2011 und 2012 wurden in Kiel vier Ausbildungsworkshops durchgeführt. Im November 2012 hat das ULD damit den zehnten Workshop seit der Einführung von EuroPriSe 2007 veranstaltet. An den internationalen Veranstaltungen haben 215 Datenschutzexperten aus 18 Ländern teilgenommen. Begrüßt werden konnten darunter auch Teilnehmer aus Asien, Nord- und Südamerika. In den Jahren 2011 und 2012 wurden 31 neue EuroPriSe-Gutachter aus neun Ländern akkreditiert.

Die Gutachter können für ihre Tätigkeit als Sachverständige mit dem EuroPriSe-Expertenlogo werben.

Eine Liste aller zugelassenen EuroPriSe-Gutachter ist abrufbar unter:

https://www.european-privacy-seal.eu/experts/register-experts/

Die Akkreditierung eines Gutachters ist drei Jahre lang gültig. Ihre Gültigkeit verlängert sich, wenn der Gutachter aktiv an einem EuroPriSe-Verfahren mitwirkt und ein Langgutachten einreicht oder wenn er an einer vom ULD angebotenen Fortbildungsveranstaltung in Gestalt von Workshops („Privacy Trainings“) oder Webinaren teilnimmt. In einem Infoblatt werden die Voraussetzungen für eine Verlängerung der Akkreditierung explizit aufgelistet. Es ist geplant, ab 2013 die Zulassungsbedingungen, insbesondere zur Verlängerung der Gutachterzulassung, weiterzuentwickeln. Es wird dann alle zwei Jahre eine Erklärung der Gutachterinnen und Gutachter verlangt, in der sie bestätigen, dass ein bestimmter Anteil ihrer Arbeit auf dem Gebiet des Datenschutzes erfolgt ist, dass Fortbildungsveranstaltungen besucht wurden und die übrigen Voraussetzungen weiterhin vorliegen.

Im Juni 2011 wurde eine Fortbildungsveranstaltung für Gutachter, ein sogenanntes Privacy Training, zu aktuellen Themen durchgeführt. Der Workshop vermittelte fundierte Kenntnisse zu den wichtigsten Stellungnahmen der Artikel-29-Datenschutzgruppe zur Auftragsdatenverarbeitung und zur datenschutzrechtlichen Verantwortlichkeit sowie zu den Anforderungen der neu eingeführten Cookie-Richtlinie und zu mobilen Apps. Es besteht

großes Interesse an Fortbildungsveranstaltungen zur standardisierten Prüfmethodik von EuroPriSe auf der Basis des europäischen Datenschutzrechts. EuroPriSe wird auch 2013 Aus- und Fortbildungsworkshops für Gutachter anbieten.

9.3.5 Zertifizierung und Rezertifizierung

Die Nachfrage nach EuroPriSe-Zertifizierungen ist in den Jahren 2011 und 2012 gestiegen. Es konnten acht Erst- und vier Rezertifizierungen erfolgreich abgeschlossen werden.

Folgende IT-Produkte und IT-basierte Dienstleistungen wurden neu zertifiziert:

- Ixquick, Startpage, Startingpage: Die Suchmaschine Ixquick wurde bereits im Juli 2008 mit dem ersten European Privacy Seal ausgezeichnet (31. TB, Tz. 9.4.4) und 2009 rezertifiziert (32. TB, Tz. 9.4.4). Nach Ablauf der Gültigkeit der Rezertifizierung wurde der Zertifizierungsgegenstand um die kosten- und registrierungsfreien Dienste Startpage und Startingpage erweitert. Anders als die Metasuchmaschine Ixquick nutzt Startpage ausschließlich Suchergebnisse von Google. Wie Ixquick verzichtet auch Startpage völlig auf die Speicherung von IP-Adressen und Suchbegriffen und gibt auch keine personenbeziehbaren Daten an Google weiter. Startingpage wird mittlerweile nicht mehr als eigenständiger Dienst angeboten. Die zertifizierten Dienste bieten eine Proxyfunktion an, die es dem Nutzer oder der Nutzerin ermöglicht, die entsprechende URL durch den Dienst abrufen und sich anzeigen zu lassen. Somit erhält der Webseitenbetreiber nur die IP-Adresse von Ixquick, nicht aber die der anfragenden Person. Bestandteile der zertifizierten Dienste sind Websuche, Bildersuche, Videosuche, Proxydienst, Ixquick-Cache sowie die Interfaces zu Anbietern von Suchmaschinen.
- RISER Service: Die RISER ID Services GmbH betreibt den RISER Service, mit dessen Hilfe Kunden bei der Einholung von einfachen Melderegisterauskünften bei Meldebehörden in bislang zehn verschiedenen Mitgliedstaaten der Europäischen Union unterstützt werden. Kunden können über das RISER-Kundenportal Aufträge zur Einholung von Melderegisterauskünften erteilen, den Status eines Auftrags einsehen und nach dessen Bearbeitung die gelieferten Ergebnisse abrufen. Der RISER-Dienst bietet Schnittstellen zu Meldebehörden, die die gewünschte Melderegisterauskunft erteilen, sofern die gesuchte Person durch die Angaben des Kunden eindeutig identifiziert werden kann und keine Auskunftssperre eingetragen ist. Die Entwicklung des RISER-Dienstes wurde von der Europäischen Kommission im Rahmen des Projektes RISERid (Registry Information Service on European Residents Initial Deployment) gefördert. Das ULD hatte als Projektpartner beratend an der Implementierung des Dienstes mitgewirkt (32. TB, Tz. 8.7). Für die EuroPriSe-Zertifizierung waren Mitarbeiter des ULD verantwortlich, die nicht im Rahmen des Projekts beratend tätig gewesen sind. Der mit dem EuroPriSe-Siegel ausgezeichnete RISER-Dienst hat im Rahmen der Zertifizierung nachgewiesen, dass er die Vorgaben des europäischen Datenschutzrechts vorbildlich umsetzt. Die Evaluierung hat ergeben, dass die RISER ID Services GmbH die erhaltenen Daten über Personen und Wohnorte nicht dauerhaft speichert. Ein sogenanntes Address Pooling findet nicht statt.
- PseudoDat: PseudoDat ist ein IT-basierter Dienst, der es An- und Verkäufern von Adressdaten ermöglicht, ihre Adressdatenbestände nicht im Klartext, sondern nur nach vorheriger Pseudonymisierung miteinander abzugleichen, um auf der Basis dieses Vergleiches Kaufentscheidungen zu treffen. Hierfür wird beim Käufer und beim Verkäufer, dem Adresshändler, eine spezielle Software installiert. Wird ein Adressabgleich initiiert, werden die Adressdatenbestände beim Käufer und Verkäufer in die Applikation eingespielt und mithilfe eines von der Software erzeugten Pseudonymisierungs-Keys pseudonymisiert. Bei den pseudonymisierten Adressdatenbeständen handelt es sich nicht um Datensätze mit Merkmalsdaten im Klartext, sondern um voll verschlüsselte Daten, bei denen der verwendete Schlüssel für jeden Abgleichsvorgang neu generiert wird. Der Abgleich der Adressdatenbestände wird auf einem vom Anbieter des Dienstes, der m-privacy GmbH, betriebenen Server durchgeführt. Nach

Beendigung des Abgleichsvorgangs können sich Käufer und Verkäufer dessen Ergebnisse (insbesondere die Anzahl der identifizierten Dubletten) in der PseudoDat-Applikation ansehen. Da der Pseudonymisierungs-Key verschlüsselt zwischen Käufer und Verkäufer ausgetauscht wird, ist sichergestellt, dass die m-privacy GmbH keine Zugriffsmöglichkeit auf die Klartextdaten erhält.

- NOVOCARD-Ampelsystem: Die Austrian Gaming Industries GmbH (AGI) betreibt Spielkasinos in Niederösterreich. Sie hat mit dem NOVOCARD-Ampelsystem ein automationsunterstütztes Zutrittskontrollsystem für Besucher der von ihr betriebenen Kasinos entwickelt, mit dessen Hilfe Häufigkeit und Dauer der Anwesenheit von Besuchern in den Kasinos erfasst werden. Dies dient dazu, spezialgesetzlichen Vorschriften zur Spielsuchtprävention zu genügen. Die AGI verarbeitet nur solche personenbezogenen Daten, die zur Identifizierung der Kasinobesucher, für die Erfassung und Auswertung von Anwesenheitszeiten und für die Verhängung einer (möglichen) Zutrittssperre erforderlich sind. Hervorzuheben ist hierbei, dass nur summarische Werte zu Anwesenheitstagen und -stunden, nicht aber das genaue Datum, die Uhrzeit und der Standort des entsprechenden Kasinos gespeichert und ausgewertet werden. Bei der NOVOCARD handelt es sich um eine kontaktlos auslesbare Karte. Die AGI rät den Besuchern ihrer Kasinos, die Karte durch eine Schutzhülle vor unberechtigtem Auslesen zu schützen. Besucher können solche Schutzhüllen zum Einkaufspreis von der AGI erwerben.
- V3 Self-Certification, Version 1.0 (Vermarktung als VALid-4F Self-Certification): VALid-4F ist ein Softwaretool, mit dem sich Personen gegenüber einer das Tool einsetzenden Stelle authentisieren und nachweisen können, dass sie sich in einem bestimmten Staat aufhalten. Betroffenen wird durch das Tool auf freiwilliger Basis ermöglicht, mithilfe eines Mobiltelefons eine sogenannte Selbstzertifizierung (Authentisierung und Nachweis, dass sie sich im Inland aufhalten) vorzunehmen. Auf diesem Weg können beispielsweise Empfänger von Sozialleistungen ihrer Verpflichtung nachkommen, in festgesetzten Abständen bei der zuständigen Behörde nachzuweisen, dass sie sich im Inland aufhalten. Der Nutzen für die Betroffenen besteht darin, dass sie nicht bei der jeweiligen Stelle vor Ort erscheinen müssen. Die Authentisierung erfolgt mittels Besitz (Mobiltelefon), Wissen (Antworten auf vereinbarte Fragen) und Biometrie (Spracherkennung). Eine bestimmte Spracherkennungssoftware war jedoch nicht Gegenstand der Zertifizierung. Ob sich der Betroffene im Inland aufhält, wird mithilfe eines Partnerunternehmens aus dem Telekommunikationsbereich festgestellt.
- ProCampaign, Version 2.0: Bei ProCampaign handelt es sich um einen IT-basierten Dienst zur Unterstützung des Customer Relationship Managements (CRM) eines Unternehmens. Mithilfe von ProCampaign können Unternehmen personenbezogene Daten ihrer Kunden (Verbraucher) zu Zwecken der Marktanalyse, der Kundenbindung oder der Werbung verarbeiten. Die Daten können auf zwei Arten in die Datenbank von ProCampaign gelangen: Zum einen kann das den Dienst einsetzende Unternehmen bereits vorhandene Kundendaten auf die ProCampaign-Datenbank überspielen, zum anderen können von Verbraucherinnen und Verbrauchern – z. B. in einem Webformular – angegebene Daten (direkt) in die Datenbank von ProCampaign übertragen werden. ProCampaign unterstützt die Einholung, Speicherung und Verwaltung von Einwilligungserklärungen der Verbraucherinnen und Verbraucher in die jeweiligen Datenverarbeitungen (z. B. die Zusendung von Werbung über unterschiedliche Kanäle wie E-Mail, (Mobil-)Telefon oder Post). ProCampaign nutzende Unternehmen werden in einem Informationsblatt in umfassender und gut verständlicher Art und Weise über datenschutzrelevante Fragestellungen, die bei der Nutzung des Dienstes zu beachten sind, informiert.
- SAP Test Data Migration Server (TDMS), Version 4.0: TDMS bietet eine Erweiterungssoftware für SAP-Systeme, mit deren Hilfe Daten für Entwicklungs-, Test-, Qualitätssicherungs- und Schulungszwecke bereitgestellt werden können. Bei der Nutzung von – aus Produktivsystemen übernommenen – Daten müssen besondere datenschutzrechtliche Anforderungen beachtet werden. So ist eine Verwendung unveränderter Echtdaten nur unter ganz bestimmten Voraussetzungen und in sehr engen Grenzen zulässig. Mit dem Einsatz von TDMS haben Nutzerinnen und Nutzer die Möglichkeit, die verwendeten Daten auf ein Minimum zu reduzieren und diese zu verfremden, ohne dass die Konsistenz der Daten verloren geht. Die Software ermög-

licht es, personenbezogene Daten so zu löschen oder zu modifizieren, dass die Identifizierbarkeit der Betroffenen entweder vollständig verhindert (Anonymisierung) oder zumindest erschwert wird (Pseudonymisierung). Hierfür bietet TDMS eine Reihe von vordefinierten Regeln, die um eigene Regeln ergänzt werden können. Ob die Verwendung bestimmter Regeln zu einer Anonymisierung bzw. Pseudonymisierung im Sinne des Datenschutzrechts führt, ist von den Nutzerinnen und Nutzern in jedem Einzelfall genau zu prüfen. Vorbildlich ausgestaltete Produkt- und Nutzerinformationen geben Hilfestellungen für den rechtskonformen Einsatz von TDMS (insbesondere für die einzusetzenden Verfremdungsregeln).

- VALid-SSD (Sim Swap Detection), Version 3.5: Die Software VALid-SSD dient der Erkennung von SIM-Kartenwechseln und unterstützt Organisationen dabei, die Integrität einer Kommunikation mit Handynutzerinnen und -nutzern sicherzustellen. Besondere Bedeutung hat dies bei sogenannten „Out Of Band"-Authentifikationen, wie sie z. B. beim Online-Banking (mobileTAN) zum Einsatz kommen. VALid-SSD betrachtet dabei das folgende Angriffsszenario: Gelingt es einem in betrügerischer Absicht handelnden Angreifer, sich gegenüber einem Mobilfunkanbieter als dessen Kunde auszugeben und diesen dazu zu veranlassen, der Mobilfunknummer des tatsächlichen Kunden eine neue SIM-Kartennummer zuzuordnen, so erhält im Rahmen einer Banktransaktion der Betrüger und nicht der eigentliche Bankkunde die von der Bank versendete TAN. Durch den Einsatz von VALid-SSD kann ein solches Szenario verhindert werden, denn mithilfe der Software können kürzlich erfolgte (und potenziell verdächtige) SIM-Kartenwechsel festgestellt werden. Datenschutzrechtlich vorbildlich sind bei VALid-SSD die Begrenzung der verarbeiteten Daten auf das absolute Minimum sowie die strikten, dem Datenschutz verpflichteten Nutzungsbedingungen.

Erfolgreich rezertifiziert wurden die folgenden IT-Produkte und IT-basierten Dienstleistungen:

- e-pacs Speicherdienst, Version 3.0 (Erstzertifizierung 2008): e-pacs bietet eine elektronische Archivierung von Röntgenbildern und anderen medizinischen Daten durch einen externen Dienstleister. Der Dienst besteht im Wesentlichen aus dem lokal beim Kunden einzurichtenden Department-Server und dem externen Deep Storage Server im Verantwortungsbereich des Dienstleisters und hat sich seit der Erstzertifizierung (31. TB, Tz. 9.4.4) in datenschutzrelevanten Bereichen nicht verändert.
- KiwiVision Privacy Protector, Version 1.0 (Erstzertifizierung 2009): Das Softwaremodul „Privacy Protector" ermöglicht die Verschleierung von Videoklardaten in Echtzeit. Bewegte Personen oder personenbeziehbare Objekte (z. B. Kfz-Kennzeichen) können in digitalen Videobildern unkenntlich gemacht werden. Das restliche Videobild bleibt unverändert. Mit dem Modul können Videoüberwachungsanlagen so eingesetzt werden, dass sie weniger intensiv in das Recht auf informationelle Selbstbestimmung eingreifen. Seit der Erstzertifizierung (32. TB, Tz. 9.4.4) sind keine datenschutzrelevanten Änderungen am Privacy Protector vorgenommen worden.
- Predictive Targeting Networking, Version 2.1 (Erstzertifizierung 2009): PTN ist ein Verfahren zur gezielten Ansprache von Internetnutzerinnen und Nutzern im Bereich der Online-Werbung („Online Behavioural Advertising"). Zu beachten war eine Änderung der gesetzlichen Rahmenbedingungen auf europäischer Ebene, die die Einholung einer Einwilligung vor dem Setzen eines Cookies auf einem Endgerät erforderlich macht (33. TB, Tz. 9.3.1). Dazu wurde eine Anpassung der für diesen Bereich geltenden Zertifizierungskriterien und damit auch eine Änderung des Dienstes notwendig. PTN wurde nach den EuroPriSe-Übergangsregelungen für OBA-Verfahren zertifiziert. Wie bei der Erstzertifizierung auch erfolgt die Ansprache der Nutzerinnen und Nutzer auf der Grundlage ihres Surfverhaltens, welches mit Umfragedaten einer kleinen Zahl zufällig ausgewählter Nutzer kombiniert und mithilfe mathematischer Algorithmen ausgewertet wird. Hierbei werden weder anbieterübergreifende Profile von Nutzerinnen und Nutzern erstellt noch sensitive Daten im Sinne des Datenschutzrechts verwendet. Nutzerinnen und Nutzer können den Einsatz des PTN-2.1-Verfahrens durch Verwendung eines sogenannten Block-Cookies („Opt-Out") unterbinden. Darüber hinaus haben sie in der rezertifizierten Version von PTN die Möglichkeit, explizit in die Verwendung ihrer Daten einzuwilligen und mithilfe eines

sogenannten Themenmonitors auf einfache Weise zu erfahren, in welche Kategorien (z. B. Sport oder Fashion) sie durch den Dienst eingeordnet wurden. Ebenfalls neu ist, dass unmittelbar angrenzend an jede mittels PTN eingeblendete Werbeinformation ein Icon angezeigt wird. Dieses Icon ist mit einer Seite verlinkt, die sowohl allgemeine Informationen zum Thema „verhaltensbasierte Online-Werbung" als auch spezielle Informationen zu PTN bereithält. Wie auch schon bisher können Nutzerinnen und Nutzer auf der Webseite des Anbieters des Dienstes, der nugg.ad AG, eine verständlich formulierte Datenschutzerklärung mit Informationen zu allen relevanten Aspekten von PTN 2.1 einsehen.

- VALid-POS® Standard Edition, Version 2 (Erstzertifizierung 2010): VALid-POS ist eine datensparsame Lösung zur Betrugsbekämpfung beim Vor-Ort-Einsatz von EC-und Kreditkarten an Geldautomaten und Kassenterminals. Mithilfe des Softwaretools kann festgestellt werden, ob sich ein zuvor registriertes Mobiltelefon des Karteninhabers in der Nähe des Geldautomaten oder Kartenterminals befindet, an dem die Karte eingesetzt wird. Seit der Erstzertifizierung (33. TB, Tz. 9.3.5) sind keine datenschutzrelevanten Änderungen an VALid-POS vorgenommen worden.

Die öffentlichen Kurzgutachten zu allen verliehenen EuroPriSe-Gütesiegeln sind im Internet abrufbar unter:

https://www.european-privacy-seal.eu/awarded-seals/

Ende 2012 liefen bei EuroPriSe mehr als 25 Erst- und Rezertifizierungsverfahren. Bei den Zertifizierungsgegenständen handelt es sich überwiegend um IT-basierte Dienste, aber auch um IT-Produkte, insbesondere Software. Sie sind für unterschiedliche Einsatzbereiche bestimmt, etwa für den Gesundheits-, den Finanz- oder den Werbesektor.

9.3.6 Zusammenarbeit mit anderen Datenschutzbehörden

Im Rahmen von EuroPriSe fand ein Informationsaustausch mit Datenschutzbehörden im In- und Ausland zu fallbezogenen wie auch allgemeinen Datenschutzfragen statt, z. B. zum Cloud Computing, zur Umsetzung der Cookie-Richtlinie, zu Tracking und verhaltensbasierter Werbung.

Der Entwurf der EU-Kommission zu einer Datenschutz-Grundverordnung (Tz. 2.5) sieht in Art. 39 eine Regelung vor, die es zukünftig den Datenschutzbehörden in Europa ermöglichen kann, Zertifizierungsstelle für EuroPriSe zu werden. Das ULD unterstützt diese Regelung und hat zu deren Konkretisierung Vorschläge bei der Europäischen Kommission und dem Europäischen Parlament vorgelegt.

Im Rahmen des von der Europäischen Kommission geförderten TAIEX-Programms hat das ULD eine Informationsveranstaltung zur Zertifizierung nach EuroPriSe für die Datenschutzkommission Mazedonien ausgerichtet.

10

KERNPUNKTE

BYOD

Browser

Schnittstellen

10 Aus dem IT-Labor

10.1 Bring Your Own Device

Die Bereitschaft zum Einsatz privater IT-Geräte im beruflichen Arbeitsumfeld steigt, wobei auf Arbeitgeber- und auf Arbeitnehmerseite unterschiedliche Interessen bestehen.

In der Verwaltung von Kommunen wie auch von Landesbehörden existieren Pilotprojekte, die es Beschäftigten ermöglichen sollen, dienstliche Datenverarbeitung auf privaten Geräten durchzuführen. Unter „Bring Your Own Device“ (BYOD) werden verschiedene Szenarien mit unterschiedlichen Motivationen zusammengefasst. Für Beschäftigte besteht die Chance, die Vielzahl der zu bedienenden Geräte einzuschränken und dabei sogar den persönlichen Markenpräferenzen zu folgen. Für Arbeitgeber besteht die Aussicht auf verbesserte, ja permanente Erreichbarkeit der Bediensteten, sinkende IT-Investitionskosten und schnelle Reaktionsmöglichkeiten auf Hard- und Softwareanforderungen.

Arbeitgeber müssen stets im Auge behalten, dass sie datenschutzrechtlich die volle Verantwortung für dienstliche Datenverarbeitung tragen. Diese Verantwortung in Bezug auf die Integrität, die Verfügbarkeit und die Vertraulichkeit ihrer Daten nimmt zu, wenn nicht mehr nur auf den IT-Geräten und in den Räumlichkeiten des Arbeitgebers Datenverarbeitung erfolgt, sondern auch auf privaten IT-Geräten und im privaten Umfeld der Arbeitnehmerinnen und Arbeitnehmer. Ein angemessener Schutz der Daten kann nicht allein durch organisatorische Maßnahmen wie Dienstanweisungen oder vertragliche Vereinbarungen zum ordnungsgemäßen Umgang mit den Daten und Geräten erreicht werden. Eine BYOD-Strategie mit einem Konzept und technischer Hinterlegung ist erforderlich, wobei – vor dem ersten BYOD-Einsatz – die Zugriffsrechte, -wege und -bedingungen verbindlich und kontrollierbar festgelegt werden.

Die zentrale Frage ist: Wie sollen die Arbeitnehmer auf unsere Daten zugreifen? Der Arbeitsaufwand, der Investitionsbedarf und der Regelungsaufwand erhöhen bzw. verringern sich abhängig danach, ob die privaten Geräte direkt ins Behörden- bzw. Unternehmensnetzwerk eingebunden werden sollen, ob Verbindungen über das Internet zustande kommen sollen, die Daten auf den Geräten gespeichert oder über Terminallösungen lediglich angezeigt werden sollen. Den Einsparungen bei IT-Investitionen kann zum Teil ein erheblich erhöhter Betreuungsaufwand sowie Investitionen in die Infrastruktur gegenüberstehen. Hierfür ist von Bedeutung, wie breit das unterstützte Produktspektrum gefasst wird und welche Serviceleistungen der IT-Bereich für die Nutzenden bieten soll. Zu berücksichtigen sind grundsätzlich das Management der Softwarelizenzen, individuelle Hilfestellungen bei Installation und Konfiguration der Geräte und Kompatibilitätsprüfungen.

Wie sollen welche Arbeitnehmer auf welche Daten zugreifen? Es gilt den Schutzbedarf der Daten zu bestimmen. Sind sie eventuell aufgrund von Amts-, Berufs- oder Geschäftsgeheimnissen besonders zu schützen oder handelt es sich um datenschutzrechtlich sensible Daten, dann sind besondere Sicherheitsmaßnahmen geboten. Möglicherweise eignen sich die Daten nicht für eine wirtschaftlich abbildbare Speicherung und Verarbeitung auf privaten Geräten. Meist geht die Idee von BYOD Hand in Hand mit mobiler Arbeit bzw. Heimarbeitsplätzen. Hierfür bestehen im Allgemeinen bereits Konzepte und Regelungen, auf denen aufgebaut werden kann.

Die sicherste Umsetzung von BYOD ist, wenn hierauf nicht gänzlich verzichtet werden soll, die Realisierung einer Terminallösung, bei der die Daten über eine sichere Verbindung lediglich auf dem privaten Gerät angezeigt werden. Hierbei behält der Arbeitgeber alle Möglichkeiten der Kontrolle: Die Daten werden weiterhin nur intern gespeichert und verarbeitet. Die Zugriffsberechtigungen können jederzeit gelöscht und die Verbindungsversuche von fremden oder tatsächlich bzw. potenziell infizierten privaten Geräten können technisch unterbunden werden.

Werden betriebliche bzw. dienstliche Daten direkt auf den privaten Geräten gespeichert, sind ein strenges Löschkonzept und klare Regelungen bezüglich der Zugriffsrechte des Arbeitgebers unumgänglich. Ähnlich wie vom Arbeitgeber zugelassene private E-Mails am Arbeitsplatz sind die privaten Daten und E-Mails auf den privaten Geräten für den Arbeitgeber tabu. Sie dürfen durch ihn

weder gelesen noch gelöscht werden. Neben den zu beachtenden herkömmlichen Löschfristen sind insbesondere für die Fälle des Gerätewechsels, des Geräteverlustes und des Personalabgangs geeignete organisatorische Regelungen sowie technische Maßnahmen nötig. Hierbei kann nicht immer auf die Kooperation der Arbeitnehmer gesetzt werden. Ein Fernlöschen des gesamten Datenbestands auf dem privaten Gerät durch den Arbeitgeber wäre zumeist eine massive Grenzüberschreitung.

Das ULD berät bei einigen Projekten auf Ebene der Landes- und Kommunalverwaltung. Hierbei zeigt sich, dass auf technischer und auf organisatorischer Ebene eine Vielzahl an Maßnahmen zu treffen sind, die unerfahrene Stellen überfordern können. Das ULD bietet hier seine Mitarbeit bereits frühzeitig in der Planungsphase an, um Fehlinvestitionen zu vermeiden und ein angemessenes Datenschutz- und Sicherheitsniveau sicherzustellen.

10.2 Browsersicherheit – aktuelle Empfehlungen

Webbrowser lösen an vielen Stellen spezielle Programme oder Fachverfahren ab. Viele Systeme werden heutzutage nur noch über eine Weboberfläche bedient. Webbrowser sind mittlerweile unverzichtbar. Zugleich sind sie häufig durch Sicherheitslücken ein Datenschutzrisiko.

Der Browsermarkt ist vielfältig wie noch nie. Als Konkurrenz zum weitverbreiteten Internet Explorer hat sich neben Firefox Google Chrome etabliert. Für die Anwenderinnen und Anwender bedeutet dies, dass eine reale Wahlmöglichkeit besteht. Hinsichtlich Funktionalität und Geschwindigkeit haben Firefox und Chrome den Internet Explorer momentan hinter sich gelassen. Aus Datenschutzsicht ist insbesondere die Möglichkeit interessant, diese Browser mit Erweiterungen auszustatten. Datenschutzfördernde Erweiterungen können z. B. Schutz vor Nutzerverfolgung im Netz, dem sogenannten Tracking, bieten oder das Identitätsmanagement erleichtern.

Sicherheitslücken in der Browsersoftware sind hochkritisch, da sich diese Programme in ständigem Austausch mit fremden, nicht vertrauenswürdigen Servern befinden können. Derartige Lücken sind so schnell wie möglich zu schließen. Dazu ist der Anwender auf den Browserhersteller angewiesen. Microsoft hat sich zu einem monatlichen „Patch Day“ entschlossen. Fehlerbehebungen werden einmal monatlich ausgeliefert. Zwar können besonders kritische Fehler auch kurzfristig außerhalb dieses Termins behoben werden; die Regel ist jedoch der monatliche Patch Day. Mozilla und Google liefern ihre Browser-Updates ohne festen Zeitrahmen aus. Das ermöglicht einerseits eine verzögerungsfreie Reaktion auf Bedrohungen, stellt andererseits jedoch die IT-Administration in Unternehmen und Behörden vor größere Herausforderungen bei Test und Freigabe neuer Programmversionen. Alle Browser weisen spezifische Sicherheitslücken auf. Daher ist es wichtig, bei der Wahl des Browsers auf eine schnelle Reaktionszeit des Herstellers zu achten und im Falle einer bekannten, aber noch nicht behobenen Sicherheitslücke vorübergehend einen anderen Browser zu verwenden.

Weitere Sicherheitsprobleme rühren nicht vom Browser direkt, sondern von Erweiterungen oder Plugins her. Erweiterungen sind insofern unproblematisch, als sie sich schlicht deaktivieren lassen, ohne die Browsernutzung grundlegend zu beeinflussen. Plugins hingegen sind oft systemweit installiert, sodass eine Installation für alle verwendeten Browser zum Einsatz kommt. Die bekanntesten Vertreter sind hier Flash- und Java-Plugins, die regelmäßig durch zum Teil gravierende Mängel auffallen. Hier hilft ein Wechsel des Browsers wenig, stattdessen muss Java in jedem verwendeten Browser deaktiviert werden. Um die Angriffsfläche durch Sicherheitslücken so gering wie möglich zu halten, empfiehlt es sich, die Zahl von Plugins in System und Browser möglichst zu reduzieren bzw. standardmäßig alle vorhandenen, aber nicht benötigten Plugins zu deaktivieren. Patches und Aktualisierungen sind umgehend einzuspielen. Für den Fall einer bekannten, aber aktuell nicht behobenen Sicherheitslücke sollte ein Alternativbrowser auf dem System vorgehalten werden, dessen Benutzung bei Bedarf vorübergehend verpflichtend ist.

Was ist zu tun?

IT-Sicherheits- und Datenschutzbeauftragte müssen darauf achten, dass das Patch- und Update-Management der datenverarbeitenden Stelle die verwendeten Browser und die installierten Plugins umfasst. Aus Sicht des ULD ist ein automatisiertes Patch- und Update-Management auch für Browsererweiterungen zwingend erforderlich.

10.3 Schnittstellensicherheit

Jeder Arbeitsplatzrechner verfügt über eine Vielzahl an Schnittstellen. Über USB-Schnittstellen können mobile Geräte wie Handys oder Datenspeicher wie USB-Sticks oder Festplatten angeschlossen werden. Hierüber kann es zum nicht erlaubten Abfluss von personenbezogenen Daten kommen. Häufig kann man diese Schnittstellen bereits mit Bordmitteln absichern.

Über offene Schnittstellen (USB, CD/DVD-Laufwerke o. Ä.) können in Server-Client-Umgebungen sensible Daten mithilfe von mobilen Datenträgern (USB-Sticks, externe Festplatten, CDs/DVDs usw.) aus dem geschützten internen Netz in andere ungeschützte Netze oder auf einen ungeschützten PC übertragen werden. Nicht nur der Abfluss sensibler personenbezogener Daten, also der Verlust von Vertraulichkeit, Integrität und Verfügbarkeit, sondern auch der Zufluss von unerwünschten Daten und Dateien kann ein Sicherheitsrisiko darstellen.

Bisher hat das ULD für die Schnittstellensicherheit – vor allem für die Server-Client-Umgebungen Windows 2000 Server/Windows 2000 Professional und Windows Server 2003/Windows XP – eine Empfehlung für externe Softwarelösungen ausgesprochen, da diese Betriebssystemversionen noch über keine komfortable Möglichkeit der Schnittstellenkontrolle mit Bordmitteln verfügten. Im Gegensatz dazu bieten externe Softwarelösungen eine zentralisierte Administration aller Schnittstellen aller Server und Clients in einem Netzwerk. So kann z. B. eine USB-Schnittstelle von einem bestimmten Client im Netzwerk für einen bestimmten Scanner freigeschaltet werden, während die anderen Clients diesen Scanner nicht nutzen können. Oder es werden dienstliche USB-Sticks zur Benutzung freigeschaltet, die dann zum Datentransfer verwendet werden dürfen, während fremde USB-Sticks an dieser USB-Schnittstelle nicht akzeptiert werden.

Mit der Server-Client-Umgebung Windows Server 2012 und Windows 7 bzw. Windows 8 können die Schnittstellen auch mit Bordmitteln verwaltet werden. Die hierfür notwendigen Einstellungen lassen sich jedoch nur dann umfassend in einer Server-Client-Umgebung einsetzen, wenn auch auf allen Servern und allen Clients diese Betriebssystemversionen installiert sind. Sobald es sich um eine gemischte Umgebung handelt, dann werden nicht auf allen Maschinen die gleichen Richtlinien angewendet; das bedeutet unter Umständen, dass einige Maschinen keiner Schnittstellenkontrolle unterliegen. Aus diesem Grund empfiehlt das ULD zur Schnittstellensicherheit folgendes Vorgehen:

- Die datenverarbeitende Stelle sichert die Schnittstellen ihrer Server und Clients in ihrer Netzwerkumgebung aktiv ab (aktive Schnittstellenkontrolle). Damit wird ein unkontrolliertes Abfließen von vertrauenswürdigen Daten bzw. ein unkontrolliertes Einfließen von externen Daten verhindert.
- Die aktive Schnittstellenkontrolle kann durch verschiedene Maßnahmen realisiert werden. So kann bei einer aktuellen Windows Client-Server-Umgebung z. B. mit Bordmitteln oder in gemischten Umgebungen mit externen Softwarelösungen gearbeitet werden. Eine spezielle Softwareempfehlung wird das ULD nicht aussprechen.
- Die aktive Schnittstellenkontrolle muss gewährleisten, dass alle offenen Schnittstellen gesperrt werden. Schnittstellen, die für die Aufgabenstellung benötigt werden, müssen explizit durch die entsprechend verantwortliche Person freigegeben werden. Diese Freigabe muss technisch im System abgebildet und dokumentiert werden.

Das ULD weist darauf hin, dass die aktive Schnittstellenkontrolle, wie sie hier beschrieben wird, nur die Hardware-Schnittstellen und -Laufwerke absichert. Das Risiko des Abflusses von personenbezogenen Daten per E-Mail, durch Heraufladen in das Internet, Erstellen von Screenshots o. Ä. muss gesondert betrachtet und insbesondere durch organisatorische Maßnahmen geregelt werden. Das ULD stellt für diesen Themenkomplex im Internet eine Handreichung zur Verfügung.

https://www.datenschutzzentrum.de/schnittstellenkontrolle/

10.4 Windows Server 2012 und Windows 8

Die aktuellen Client- und Server-Betriebssysteme des Herstellers Microsoft ermöglichen ein deutlich höheres Sicherheitsniveau. Vor allem die verbesserten Möglichkeiten zur zentralen Konfiguration und Überwachung der Endgeräte sollten durch datenverarbeitende Stellen genutzt werden. Veraltete Betriebssysteme stellen ein zunehmendes Sicherheitsrisiko dar.

In einigen Verwaltungen und Betrieben in Schleswig-Holstein werden immer noch mittlerweile stark veraltete Betriebssysteme eingesetzt. Dies kann im Jahr 2013 zu konkreten Sicherheitsproblemen führen. Zugleich bleibt diesen Stellen eine Vielzahl an Funktionen vorenthalten, die die tägliche Arbeit deutlich erleichtern. Im Rahmen einzelner Kontrollen hat das ULD noch Serversysteme auf der Basis von Windows NT 4 angetroffen. Diese Systeme werden seit 2004 nicht mehr von Microsoft unterstützt und stellen ein erhebliches Sicherheitsrisiko dar. Auch Systeme auf der Basis von Windows 2000 Server werden seit 2005 nicht mehr von Microsoft unterstützt. Systeme auf der Basis dieser stark veralteten Betriebssystemversionen müssen schnellstmöglich abgelöst werden. Das ULD beanstandet den Betrieb derartig veralteter Infrastrukturen.

Microsoft hat für Windows Server 2003 und Windows XP bereits in den Jahren 2009 und 2010 das Bereitstellen von Sicherheitsupdates und Fehlerbehebungen eingeschränkt und wird derartige Aktualisierungen nur noch bis zum Jahr 2014 und 2015 anbieten, soweit erweiterte Wartungsverträge abgeschlossen wurden. Datenverarbeitende Stellen sollten für diese mittlerweile veralteten Systeme im Jahr 2013 ein Projekt zur Migration auf aktuellere Plattformen einplanen.

Neben den Sicherheits- und Datenschutzaspekten ergeben sich durch die Migration auf aktuelle Betriebssystemversionen auch deutliche Vorteile für den Betrieb der Systeme. Aktuelle Betriebssystemversionen bieten

- Funktionen zur automatisierten Installation und Konfiguration,
- Funktionen zur zentralen, richtlinienbasierten Konfiguration,
- Möglichkeiten zur zentral administrierten, vollständigen Festplattenverschlüsselung,
- Möglichkeiten, externe Schnittstellen zu kontrollieren,
- Funktionen, um eine zentrale Protokollierung und ein zentrales Berichtswesen aufzusetzen, um die Anforderungen beispielsweise der Datenschutzverordnung (DSVO) automatisiert umzusetzen.

Das ULD hat die aktuellen Sicherheitsfunktionen von Windows Server 2012 und Windows 8 getestet und bereits in mehreren Schulungen für Administratorinnen und Administratoren vermittelt. Es zeigt sich: Mit Kenntnis der neuen Funktionen und einer vorausgehenden, umfangreichen Planung kann neben einem angemessenen Sicherheits- und Datenschutzniveau auch eine wirtschaftlichere Datenverarbeitung erreicht werden.

Das ULD bietet allen Stellen in Schleswig-Holstein seine Unterstützung bei der Planung von Migrationsprojekten an, um Aspekte eines wirtschaftlichen, sicheren und datenschutzkonformen IT-Betriebs zu berücksichtigen. Administratorinnen und Administratoren sollten sich über Schulungen rechtzeitig fortbilden. Neben den einschlägigen Schulungsangeboten der Hersteller und den in Schleswig-Holstein vertretenen Schulungsanbietern bietet das ULD spezielle Datenschutz- und Sicherheitskurse in der DATENSCHUTZAKADEMIE an.

11

KERNPUNKTE

Europäischer Rechtsrahmen

Vereinigte Staaten von Amerika

Standardisierung

11 Europa und Internationales

Datenschutz erhält sowohl hinsichtlich der Praxis als auch der Regelungsfragen immer mehr eine internationale Dimension. Zentral sind hierbei die Regulierungsbestrebungen der Europäischen Union (Tz. 2.5, 11.1). Die praktische Bedeutung der Artikel-29-Datenschutzgruppe der EU für die europaweite Koordinierung der Aufsichtstätigkeit sowie für die einheitliche Auslegung der europäischen Datenschutzrichtlinie aus dem Jahr 1995 nimmt weiter zu (Tz. 11.2, 11.3). Dies betrifft auch den Umgang mit der Datenverarbeitung von europaweit präsenten US-Unternehmen sowie mit der äußerst aktiven Datenbeschaffung durch US-Sicherheitsbehörden (Tz. 11.4, 11.5).

11.1 Europäische Regulierung

Nach umfangreichen vorbereitenden Diskussionen legte die EU-Kommission am 25. Januar 2012 ein Gesamtkonzept zur Reform bzw. Fortentwicklung des europäischen Datenschutzrechts vor.

Dieses Reformpaket enthält zunächst einen Vorschlag für eine Richtlinie zum Datenschutz „durch die zuständigen Behörden zum Zweck der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafverfolgung“ sowie zum freien Datenverkehr (KOM(2012) 10 endgültig), mit der für die Bereiche Polizei, Staatsanwaltschaft, Justiz- und Ordnungsverwaltung Vorgaben an die nationalen Gesetzgeber gemacht werden sollen und die den bisher gültigen Rahmenbeschluss 2008/977/JI ersetzen soll. Der Kommissionsvorschlag bleibt in mancher Hinsicht hinter der ausdifferenzierten deutschen Datenschutzgesetzgebung im Sicherheitsbereich, die stark durch Entscheidungen des Bundesverfassungsgerichts bestimmt wird, zurück. Das ULD und die Datenschutzbeauftragten des Bundes und der Länder drängen daher darauf klarzustellen, dass mit einer derartigen Richtlinie allenfalls Mindeststandards festgelegt werden können und dürfen. Die Verabschiedung einer entsprechenden Richtlinie wird Auswirkungen auf das Landespolizeirecht haben; der Landtag muss danach prüfen, wie sie für Schleswig-Holstein im geltenden Landesverwaltungsgesetz umzusetzen ist.

Erheblich größere öffentliche Aufmerksamkeit und Resonanz gefunden hat der Vorschlag einer Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, kurz „Datenschutz-Grundverordnung“ genannt, mit Änderungen für die Wirtschaft und die Verwaltung (KOM(2012) 11 endgültig). Dieser Verordnungsentwurf macht Vorgaben, die den datenschutzrechtlichen Anforderungen des Internetzeitalters genügen sollen.

Der Landtag Schleswig-Holstein hat begonnen, sich mit dem europäischen Reformpaket zu befassen. Zunächst ging es um die Frage, ob die EU überhaupt Regelungen erlassen darf, welche auch der nationalen Gesetzgebung überlassen werden können. Diese Frage wurde vom deutschen Bundesrat verneint (BR-Drs. 52/12 – Beschluss). Diese Subsidiaritätsrüge wurde von der EU zurückgewiesen. Dessen ungeachtet bleibt die Frage offen, inwieweit durch nationale Regelungsvorbehalte sowohl ein Höchstmaß an Einheitlichkeit und europaweiter Verbindlichkeit erreicht als auch regional bzw. national bewährte Regelungs- und Vollzugsstrukturen bewahrt werden können.

Im Dezember 2012 legte der Berichterstatter des zuständigen Ausschusses des Europaparlaments einen umfangreichen Katalog von Änderungsvorschlägen vor, die in vieler Hinsicht die Kritik an dem Regelungspaket der EU-Kommission aufgreift (Tz. 2.5).

Was ist zu tun?

Die Erörterungen des Reformpakets sollten zügig und ergebnisorientiert fortgesetzt werden, damit im Jahr 2014 ein beschlussfähiger Vorschlag zur Abstimmung gestellt werden kann.

11.2 Artikel-29-Datenschutzgruppe

Die Artikel-29-Datenschutzgruppe ist das unabhängige Beratungsgremium der Europäischen Union in Datenschutzfragen. Die Gruppe macht von der ihr eingeräumten Möglichkeit, Stellungnahmen und Empfehlungen zu Fragen des Datenschutzes abzugeben, regen Gebrauch: Seit 1997 hat sie mehr als 200 Dokumente zu einer Vielzahl von Themen veröffentlicht.

Die Artikel-29-Datenschutzgruppe trägt ihren Namen, weil sie gemäß Artikel 29 der Datenschutzrichtlinie 95/46/EG eingesetzt ist. Sie besteht aus Vertretern der nationalen Aufsichtsbehörden für den Datenschutz, des Europäischen Datenschutzbeauftragten sowie der EU-Kommission. Anders als gerichtliche Entscheidungen sind die Stellungnahmen und Empfehlungen der Gruppe rechtlich nicht bindend. Ihnen kommt aber eine hohe Bedeutung zu, weil sie die gemeinsamen Ansichten der nationalen Aufsichtsbehörden zu den bearbeiteten Themen widerspiegeln.

Das ULD engagiert sich in mehreren Arbeitsgruppen der Datenschutzgruppe, bei deren Sitzungen aktuelle Themen diskutiert und gegebenenfalls Stellungnahmen oder Empfehlungen erarbeitet werden. 2011 und 2012 hat die Datenschutzgruppe u. a. Papiere zum Datenschutz bei Smart Metern, Geolokalisierungsdiensten von mobilen Endgeräten, verhaltensbasierter Online-Werbung, Biometrie und Gesichtserkennung bei Online- und Mobilfunkdiensten veröffentlicht. Nach Beschlussfassung werden die Papiere auch in deutscher Übersetzung bereitgestellt. Die Stellungnahmen und Empfehlungen der Gruppe können im Internet abgerufen werden unter:

http://ec.europa.eu/justice/data-protection/article-29/documentation

Aufgrund ihrer praktischen Relevanz besonders hervorzuheben sind die Stellungnahmen der Artikel-29-Datenschutzgruppe zur Definition von Einwilligung (WP187) und zum Cloud Computing (WP196 – Tz. 11.3, 7.3). Im WP187 analysiert die Gruppe das derzeit im Datenschutzrecht verwendete Konzept der Einwilligung und führt zahlreiche Beispiele für gültige und ungültige Einwilligungen auf. Sie weist darauf hin, dass in der Praxis in einigen Fällen Methoden angewendet werden, die für die Erteilung einer echten, eindeutigen Einwilligung nicht geeignet sind. Im Anschluss an die Bewertung des derzeitigen Rechtsrahmens gibt die Gruppe Empfehlungen für Änderungen der rechtlichen Rahmenbedingungen durch den EU-Gesetzgeber.

11.3 Artikel-29-Datenschutzgruppe zu Cloud Computing

Die Artikel-29-Datenschutzgruppe hat im Juli 2012 eine Stellungnahme zum Cloud Computing abgegeben. Diese bezieht Stellung zu relevanten rechtlichen Fragestellungen sowie zu geeigneten technischen und organisatorischen Maßnahmen.

In ihrer Stellungnahme, an der das ULD maßgeblich mitgewirkt hat, äußert sich die Artikel-29-Datenschutzgruppe zu zentralen, datenschutzspezifischen Fragen des Cloud Computing (Tz. 5.7). Als spezifische Risiken des Cloud Computing identifiziert die Gruppe Kontrollverlust und mangelnde Transparenz. Diese Risiken sind besonders groß, wenn personenbezogene Daten in verschiedenen Rechenzentren rund um den Globus und durch eine Vielzahl von (Unter-)Auftragnehmern verarbeitet werden. Die Stellungnahme konzentriert sich auf den Normalfall eines Cloud-Angebotes, in dem der Anwender als verantwortliche Stelle und der Cloud-Anbieter als Auftragsverarbeiter zu qualifizieren ist, und trifft Aussagen dazu, wie die Vorgaben des geltenden EU-Datenschutzrechts eingehalten werden können. Schwerpunkte liegen auf den vertraglichen Sicherungen im Verhältnis zwischen Cloud-Anbieter und Anwender sowie der Problematik der Übermittlung personenbezogener Daten in Drittstaaten außerhalb des Europäischen Wirtschaftsraums (EWR).

Die Artikel-29-Datenschutzgruppe stellt klar, dass technisch-organisatorische Maßnahmen nicht nur an den klassischen Schutzzielen der Verfügbarkeit, Vertraulichkeit und Integrität, sondern auch an den Datenschutz-Schutzzielen der Transparenz, Intervenierbarkeit und Nichtverkettbarkeit auszurichten sind. Eine Checkliste soll Cloud-Anbietern und Anwendern dabei helfen, eine datenschutzkonforme Verarbeitung von Daten in der Cloud sicherzustellen.

Was ist zu tun?

Das ULD wird die datenschutzfreundliche Technikgestaltung im Bereich Cloud Computing durch Umsetzung der Anforderungen der Artikel-29-Datenschutzgruppe konstruktiv unterstützen und weiterhin in dieser Gruppe zu diesem Thema mitarbeiten.

11.4 Datenschutz in den USA

Die USA sind die Wiege des modernen Datenschutzrechts. Die Präsenz von US-Unternehmen ohne hinreichenden Datenschutz ist inzwischen eine beachtliche Gefahr für die informationelle Selbstbestimmung in Europa.

Im Jahr 1890 veröffentlichten die US-Juristen Samuel D. Warren und Louis D. Brandeis im *Harvard Law Review* den Aufsatz „The Right to Privacy" – das Recht auf Privatheit – und begründeten damit den modernen Datenschutz.

https://www.datenschutzzentrum.de/allgemein/20111219-Warren-Brandeis-Recht-auf-Privatheit.html

Noch in den 60er-Jahren des 20. Jahrhunderts wurde die Diskussion über den Privatheitsschutz in den USA zumindest so intensiv geführt wie in Europa. Die Beiträge von Alan F. Westin aus dieser Zeit sind noch heute in mancher Hinsicht richtungsweisend. Während aber danach in Europa eine kontinuierliche Weiterentwicklung des Persönlichkeitsschutzes unter Berücksichtigung der technischen Entwicklung erfolgte, entstanden in den USA zwar eine Vielzahl von Datenschutzregeln; diese sind aber zumeist regional und immer sachlich beschränkt. Mit Artikel 8 der Europäischen Grundrechtecharta wurde europaweit explizit ein Grundrecht auf Datenschutz etabliert. Währenddessen blieb der Datenschutz in den USA ein unübersichtlicher, inkonsistenter Flickenteppich mit zwei großen Lücken: US-Sicherheitsbehörden haben äußerst weite Kompetenzen zu Eingriffen ins Persönlichkeitsrecht. Und der Bereich des Internetdatenschutzes für Erwachsene blieb bis heute vollständig den Selbstverpflichtungen der Wirtschaft überlassen.

Diese beiden Rahmenbedingungen haben massive Konsequenzen für den Datenschutz in Europa und konkrete praktische Effekte für die Menschen – auch in Schleswig-Holstein. Die informationellen Beziehungen zwischen Europa und den USA führen zu einer Weitergabe personenbezogener Daten von Europa in die USA, ohne dass die europäischen Datenschutzstandards gewahrt werden. Dies hat Konsequenzen z. B. für Auskunfts- und Löschansprüche nach der Weitergabe von Bankdaten (32. TB, Tz. 11.3), Fluggastdaten (30. TB, Tz. 11.1) oder bei sonstigen für Sicherheitszwecke übermittelten Informationen, da die Empfänger den Betroffenen keine informationelle Selbstbestimmung gewähren.

Zumindest quantitativ noch schwerwiegender ist, dass auf dem europäischen Markt agierende US-Internetunternehmen nach Heimatrecht nur beschränkten Restriktionen unterliegen und sich zugleich einer effektiven europäischen Datenschutzaufsicht zu entziehen versuchen. Insofern stand das Unternehmen Google in den vergangenen Jahren immer wieder im Fokus des ULD (33. TB, Tz. 7.2; 32. TB, Tz. 7.1, 7.2; 31. TB, Tz. 7.1-7.3, 10.5, 10.6; 30. TB, Tz. 7.4, 10.6; 29. TB, Tz. 10.6-10.9). Im Berichtszeitraum geriet Facebook mit seinem Internetangebot in das Blickfeld der Aufsichtsbehörden (Tz. 1.5, 7.1). Diese beiden Unternehmen sind aber nur die Spitze eines viel größeren Eisberges: Es vergeht kaum ein Tag, an dem das ULD nicht Anfragen zu weiteren global agierenden Internetunternehmen erhält, die in der Regel ihren Stammsitz in den USA haben. Die zentrale Fragestellung ist, wie der Datenschutz in Bezug auf die kommerzielle Nutzung von Internetdaten zu Werbezwecken realisiert werden kann (Tz. 7.3).

Das Safe-Harbor-Abkommen zwischen der EU und den USA verfolgt das Ziel, beim transatlantischen Datenaustausch mit den USA dort ein ansatzweise angemessenes Datenschutzniveau zu realisieren. Die hierzu bestehenden Vorbehalte bestätigen sich weiterhin (33. TB, Tz. 11.1; 32. TB, Tz. 11.4). Es mag viele US-Unternehmen geben, die mit großer Ernsthaftigkeit versuchen, die in dem Abkommen festgelegten Voraussetzungen für die Selbstzertifizierung zu erfüllen. Das Beispiel Facebook zeigt aber zugleich, dass die schwerfälligen Mechanismen des Abkommens es Unternehmen leicht

machen, datenschutzwidrige Geschäftsmodelle zu betreiben. Insofern ist von großem Interesse, welche Resonanz die Beschwerde des ULD gegenüber der US-Verbraucherschutzbehörde FTC in Bezug auf Facebook findet, die nur zwei der Safe-Harbor-Prinzipien in Bezug auf wenige Funktionalitäten thematisiert (Tz. 7.1.4).

Die Diskussion einer Datenschutz-Grundverordnung in Europa (Tz. 2.5) hat in den USA heftige Diskussionen ausgelöst, ob das dort bestehende Datenschutzrecht noch zeitgemäß ist. Als direkte Antwort der US-Regierung auf den Vorschlag der EU-Kommission vom Januar 2012 darf der Vorschlag eines „Consumer Privacy Bill of Rights" einen Monat später verstanden werden. Dieser Vorschlag ist jedoch aus europäischer Grundrechtssicht nicht adäquat: Es werden keine subjektiven Datenschutzrechte garantiert, sondern es wird auf eine nur begrenzt verbindliche Selbstregulierung der Wirtschaft gesetzt.

https://www.datenschutzzentrum.de/gesetze/Consumer-Privacy-Bill-of-Rights.html

Was ist zu tun?

Mit einer Neuregelung des Datenschutzes in Europa muss eine Überarbeitung des Safe-Harbor-Abkommens einhergehen.

11.5 Der Zugriff der USA auf europäische Daten

Ein spezielle Frage, bei der sich ungenügender Datenschutz in den USA im Sicherheitsbereich und transatlantische private Datenverarbeitung überschneiden, hat sich mit den zunehmenden Angeboten des Cloud Computing ergeben (Tz. 5.7, 11.3). Immer wieder erhält das ULD Anfragen, inwieweit eine Auftragsdatenverarbeitung bei Unternehmen durchgeführt werden darf und kann, die in den USA Tochterunternehmen betreiben. Über besondere Gesetze, u. a. den Patriot Act, und nach der Rechtsprechung in den USA ist es dortigen Sicherheitsbehörden möglich, in den USA verarbeitete Daten für Zwecke der Gefahrenabwehr, der Strafverfolgung oder der Geheimdienste zu beschlagnahmen. Das Recht erlaubt es darüber hinaus, über US-Tochterunternehmen Partnerfirmen in anderen Staaten zu zwingen, dort verarbeitete Daten herauszugeben. Dies betrifft auch die Datenverarbeitung in Europa.

Eine Analyse der Rechtssituation in den USA durch das ULD bestätigte das Problem. Anfragen bei Unternehmen ergaben, dass derartige territoriale Übergriffe auf die europäische Datenhoheit stattfinden, wenngleich sie nicht an der Tagesordnung sein sollen. Unsere Erkenntnisse werden durch eine Anfang 2013 bekannt gemachte, im Auftrag des Europäischen Parlaments erstellte Studie bestätigt, die hervorhebt, dass die Datenzugriffe geheim erfolgen, sodass eine quantitative oder qualitative Bewertung kaum möglich ist.

Als Konsequenz können wir nur empfehlen, auf Auftragsdatenverarbeitungen in den USA zu verzichten. Hinsichtlich der Inanspruchnahme von Unternehmen mit Sitz in Europa und Töchtern in den USA haben wir die Empfehlung ausgesprochen, ein explizites Verbot der Herausgabe von Daten an US-Behörden vertraglich zu vereinbaren und für den Fall einer absprachewidrigen Datenweitergabe eine erhebliche Vertragsstrafe vorzusehen. Letztlich liegt es in der Verantwortung der politisch Verantwortlichen in der deutschen Regierung sowie in der EU, mit den USA Regelungen auszuhandeln, die einen Schutz personenbezogener Daten bei Auftragsdatenverarbeitungsverhältnissen vor Zugriffen durch US-Behörden sicherstellen.

https://www.datenschutzzentrum.de/internationales/20111115-patriot-act.html

11.6 Internationale Standardisierung

Technische Datenschutzstandards sollen und können zur internationalen Vereinheitlichung im Umgang mit personenbezogenen Daten beitragen. Dabei darf es aber nicht zu einer Absenkung des Datenschutzniveaus kommen.

Das ULD ist im Rahmen seiner drittmittelfinanzierten Projektarbeit seit vielen Jahren in verschiedenen Gremien der nationalen und internationalen Datenschutzstandardisierung aktiv. Schwerpunkt der Arbeit war bislang die Mitwirkung in den Gremien der Internationalen Standardisierungsorganisation (ISO). Daneben brachte sich das ULD aktiv in die jüngste Arbeit des World Wide Web Consortiums (W3C) ein.

Innerhalb der ISO hat die Konkretisierung des Rahmenstandards ISO/IEC 29100 an Fahrt aufgenommen. Aufbauend auf den in diesem Dokument beschriebenen Prinzipien wurden mehrere Projekte mit großer Praxisorientierung initiiert. Das zuständige Komitee hat entschieden, bestehende Informationssicherheitsstandards um spezifische Anforderungskataloge für personenbezogene Daten zu erweitern; hierzu sind sowohl ein genereller Standard als auch ein Standard mit Ausrichtung auf Datenschutz im Cloud Computing in Vorbereitung. Außerdem entwickelt die Arbeitsgruppe zu Datenschutztechnologie und Identitätsmanagement einen Standard zum Privacy Impact Assessment. Hierdurch soll vereinheitlicht werden, wie vor der Einführung eines Verfahrens die mit ihm verbundenen Risiken abgeschätzt werden. Diese Entwicklung geht Hand in Hand mit aktuellen Diskussionen zur Novellierung des europäischen Datenschutzrechts in der neuen Datenschutz-Grundverordnung (Tz. 2.5), die in bestimmten Fällen die Durchführung einer solchen Risikoabschätzung vorschreibt.

Das W3C ist eine Standardisierungsorganisation, die sich insbesondere um die Entwicklung von technischen Protokollen und Standards für das Internet kümmert. Hier wird der Standard für die Beschreibung von Webseiten (HTML) entwickelt. Das W3C hat sich im vergangenen Jahr der Aufgabe angenommen, Transparenz und Wahlmöglichkeit im Bereich von Nutzer-Tracking und Profilbildung beim Surfen im Internet zu erhöhen. Beim Surfen hinterlässt jeder Nutzer Spuren, die insbesondere von Diensteanbietern und Werbetreibenden ausgewertet werden, um gezielt ihre Produkte zu bewerben. Durch die eingesetzten Verfahren ist es etwa möglich, dass man Werbung für Luxusartikel erhält, wenn früheres Surfverhalten darauf hinweist, dass man ein hohes Einkommen und die entsprechende Konsumbereitschaft hat. Durch den vom W3C entwickelten Standard unter dem Titel „Do Not Track“ – also sinngemäß „Verfolge mich nicht“ – soll den Nutzenden die Möglichkeit gegeben werden, den Anbietern von Diensten und Inhalten im Internet ihren Wunsch zu übermitteln, dass ihr Verhalten hierfür nicht oder in geringerem Umfang ausgewertet wird (Tz. 7.3).

Ein solcher Standard wäre für den Umgang mit Nutzungsdaten von europäischen Nutzenden durch nicht europäische Diensteanbieter im Internet von Bedeutung. Ein globaler industrieller Standard kann, wenn die Durchsetzung europäischen Datenschutzrechts aus praktischen Gründen bisher nicht gewährleistet wird, die Position der europäischen Nutzerinnen und Nutzer verbessern. Die Entwicklung dieses Standards wird von der betroffenen Industrie begleitet und sehr kontrovers diskutiert. Es bleibt abzuwarten, ob es gelingt, gegen Widerstände von Teilen der US-Industrie einen Standard zu setzen, der eine tatsächliche Verbesserung der Informations- und Wahlmöglichkeiten der Nutzenden mit sich bringt, die Durchsetzung europäischer Vorgaben erleichtert und dadurch zu mehr Akzeptanz beiträgt.

12

KERNPUNKTE

Informationszugangsgesetz

Open Data

12 Informationsfreiheit

Das Informationsfreiheitsrecht in Deutschland ist in Bewegung. Schleswig-Holstein ist das erste Bundesland, das den Zugang zu Umweltinformationen und zu allgemeinen Verwaltungsinformationen in einem einheitlichen Informationszugangsgesetz (IZG-SH) geregelt hat (Tz. 1.2). Selbst in Süddeutschland bestehen teilweise hoffnungsvolle Initiativen zur erstmaligen gesetzlichen Etablierung von Informationszugangsrechten. Nach ersten Bestrebungen systematischer Informationsangebote der öffentlichen Verwaltung in Bremen und in Berlin hat Hamburg ein Transparenzgesetz in Kraft gesetzt, welches das Prinzip von Open Data in der Verwaltung konsequent regelt und so als Vorbild für andere Bundesländer dient (Tz. 1.3).

12.1 Eckpunktepapier zu Open Data

Im Rahmen des IT-Planungsrates auf Bundesebene gibt es eine Arbeitsgruppe zu einer nationalen E-Government-Strategie und hierzu eine Arbeitsgruppe „Open Government" zur Förderung von Transparenz, Teilhabe und Zusammenarbeit.

Im Rahmen der nationalen E-Government-Strategie ist im September 2011 ein Eckpunktepapier des Bundesinnenministeriums über offenes Regierungs- und Verwaltungshandeln, also zum „Open Government", veröffentlicht worden und lud zur öffentlichen Konsultation ein. Die Beauftragten für Informationsfreiheit des Bundes und der Länder haben zu dem Eckpunktepapier im Januar 2012 Stellung genommen. Sie begrüßen die Vorlage des Eckpunktepapiers „Open Government" und sehen im Einsatz der Informationstechnik die große Chance, Transparenz und Informationsfreiheit auf der Ebene des Bundes, der Länder und der Kommunen einen großen Schritt voranzubringen.

Dessen Leitgedanke, das überkommene Amtsgeheimnis zu überwinden, ist als wesentlicher Beitrag zur Erweiterung der Open-Data-Initiativen zu bewerten. Die bestehenden Informationsfreiheitsgesetze des Bundes und der Länder sollten um verbindliche Verpflichtungen aller öffentlichen Stellen erweitert werden, von sich aus Informationen zu veröffentlichen. Hier finden sich bereits Regelungen in den Informationsfreiheitsgesetzen Bremens und Berlins sowie im Hamburgischen Transparenzgesetz. Diese verbindlichen Verpflichtungen aller öffentlichen Stellen soll zu mehr Transparenz, Teilhabe und Zusammenarbeit der Bürgerinnen und Bürger, Wirtschaft und Wissenschaft und des Staates führen.

Im Rahmen der gesetzlichen Regelungen sind konkrete gesetzliche Vorgaben zum ungehinderten Zugang und zur angemessenen Verwendung der Daten erforderlich. Im Hinblick auf die Regelungen in Bremen und Hamburg sollten die Regierung des Landes Schleswig-Holstein und die Kommunen dazu übergehen, den freien Zugang zu Informationen proaktiv zu gestalten. Das bestehende IZG-SH ermöglicht bereits Informationsregister. Für Umweltinformationen ergibt sich die Verpflichtung der proaktiven Veröffentlichung aus § 11 IZG-SH. Im Bereich der Geodaten besteht im Land schon eine derartige Geodateninfrastruktur.

Mit öffentlichen Mitteln erhobene Datenbestände sollten auch der Öffentlichkeit zur Verfügung gestellt werden. Eine kostenlose Bereitstellung von Daten fördert die Weiterverwendung von Daten. Mit deren Nutzung können über Innovationen und neue Geschäftsmodelle wirtschaftliche Impulse gesetzt werden, die dem Land – seiner Wirtschaftskraft, der Beschäftigung und letztlich dem Haushalt – zugutekommen.

Die Informationsfreiheitsbeauftragten vertreten den Standpunkt, dass öffentliche Daten von den zuständigen öffentlichen Stellen grundsätzlich kostenfrei zur Verfügung gestellt werden müssen. Dabei soll es keine Rolle spielen, welche Absicht mit der Datenverwendung verbunden ist. Durch die Erhebung der Verwendungsabsicht darf die Voraussetzungslosigkeit des Zugangs zu Informationen nicht durch die Hintertür ausgehebelt werden. Niemand soll sich für sein Informationsinteresse rechtfertigen müssen.

Für Schleswig-Holstein sollten die gewonnenen Erkenntnisse zur Geodateninfrastruktur berücksichtigt werden. Es finden Gespräche des Innenministeriums mit dem zentralen IT-Dienstleister Dataport und den Kollegen in Bremen und Hamburg statt.

12.2 Informationsfreiheit in der Verwaltung

Informationsfreiheit in der Verwaltung des Landes Schleswig-Holstein bedeutet derzeit vor allem einen voraussetzungslosen, einfachen und unkomplizierten Anspruch auf Zugang zu den bei einer Behörde vorhandenen Informationen. Nach den dem ULD vorliegenden Erfahrungen werden die Anträge nach dem IZG-SH in den meisten Behörden, Gemeinden, Kreisen und Ämtern unverzüglich und vollständig beschieden und die entsprechenden Informationen zur Verfügung gestellt. Fragen kommen in erster Linie auf bei Verträgen der öffentlichen Hand, Vergabeunterlagen und Bauakten. Hier muss das ULD oft nachfragen, die ergangene Rechtsprechung erläutern und Auslegungshilfen geben. Diese Unterstützung genügt in den meisten Fällen, um den Anfragenden im gesetzlichen Rahmen den Informationszugang zu eröffnen.

Im Sinne von Open Data sollte die Verwaltung künftig verstärkt proaktiv Daten, die keinen Einschränkungen unterliegen, veröffentlichen und so mehr Transparenz in die behördlichen Entscheidungsprozesse bringen.

12.3 Stellungnahme oder internes Arbeitspapier?

Ein Bürger wandte sich mit der Bitte um Herausgabe einer Stellungnahme zu einem Arbeitskreis der Verwaltung an eine Stadt. Nach § 9 Abs. 2 Nr. 2 IZG-SH sind interne Mitteilungen der informationspflichtigen Stelle, die zum Schutz des behördlichen Entscheidungsprozesses erforderlich sind, während des laufenden Entscheidungsprozesses nicht zu veröffentlichen. Stellungnahmen dienen jedoch nicht der unmittelbaren Vorbereitung eines behördlichen Entscheidungsprozesses und fallen daher auch nicht unter die gesetzliche Einschränkung. Stellungnahmen der Verwaltung sind also, soweit sie keinen anderweitigen Einschränkungen unterliegen, nach dem IZG-SH offenzulegen. Maßgeblich ist nicht der Begriff „Stellungnahme“, sondern der Verwendungszweck des Schriftstücks. Unerheblich ist auch, dass es sich bei dem Schriftstück um eine rein interne Information handelt. Eine informationspflichtige Stelle kann sich auch nicht darauf berufen, dass die begehrten Informationen offiziell nicht vorhanden sind, wenn die Informationen tatsächlich vorliegen.

12.4 IZG-SH und Einsicht in Steuerakten

Das ULD erhielt einige Eingaben zum Steuerrecht mit der datenschutzrechtlich begründeten Forderung der Steuerpflichtigen nach Einsicht in ihre eigenen abgeschlossenen Steuerunterlagen (Tz. 4.8.1). Deren entsprechende Anträge gegenüber den Finanzämtern wurden mit der Begründung abgelehnt, die AO sehe keinen Auskunftsanspruch vor. Einige der Petenten stützten ihren Antrag dann auf das IZG-SH, welches jedermann Anspruch auf Zugang zu den bei einer Behörde vorhandenen Informationen einräumt. Die eigene Steuerakte ist eine bei einer Behörde vorhandene Information. Diese Ansprüche wurden ebenfalls zurückgewiesen mit der Begründung, das IZG-SH sei lediglich ein Auffangrecht, welches neben Spezialgesetzen nicht anwendbar sei bzw. zurücktreten müsse. Das Oberverwaltungsgericht (OVG) Nordrhein-Westfalen fällte hierzu im Juni 2011 eine Grundsatzentscheidung und bestätigte die Anwendbarkeit des Informationsfreiheitsrechts auf Steuerakten. Dieser rechtlichen Bewertung schloss sich das für Schleswig-Holstein zuständige OVG mit Urteil vom 6. Dezember 2012 an. Das OVG Schleswig entschied, dass § 3 IZG-SH auch einen Anspruch auf Zugang zu Steuerdaten gibt.

Was ist zu tun?

Das Finanzministerium des Landes sollte eine Information an die Finanzämter herausgeben, dass Bürgerinnen und Bürger generell einen Rechtsanspruch auf Einsicht in ihre Steuerakte haben.

12.5 Zugang zu Kaufverträgen

Im Zusammenhang mit dem IZG-SH hatten wir zu beurteilen, ob Informationen zu laufenden Verhandlungen über Kaufverträge an Dritte zu übermitteln und ob diese Informationen nach Abschluss der Verhandlungen offenzulegen sind.

Bei Kaufverträgen, die eine Behörde mit einer natürlichen Person oder einer juristischen Person des Privatrechts schließt, handelt es sich um bei einer informationspflichtigen Stelle verfügbare Informationen. Die Veräußerung von Liegenschaften ist z. B. insgesamt dem fiskalischen Handeln einer öffentlichen Stelle zuzuordnen. Der Veräußerungsvorgang unterteilt sich nicht in eine vorgeschaltete öffentlich-rechtliche Entscheidungsfrage und eine nachgelagerte privatrechtliche Abwicklungsphase. Das Verwaltungsgericht (VG) Köln hat am 7. April 2011 klargestellt, dass der Staat und seine Einrichtungen bei privatrechtlichem Handeln Zuordnungsobjekt von Normen des öffentlichen Rechts bleiben, und erläutert: „Was zum Schutz der Wettbewerbsposition privater Immobilienunternehmen erforderlich ist – wie etwa die Gewährleistung größtmöglicher Vertraulichkeit – ist nicht automatisch in jedem Fall auch zum Schutz der Wettbewerbsposition einer öffentlichen Stelle erforderlich. Dies gilt etwa im Hinblick auf öffentlich-rechtliche Bindungen der Beklagten, zu denen auch die Vorschriften des IFG gehören."

Die gesamte Tätigkeit einer öffentlichen Behörde dient dem öffentlichen Interesse. Transparenz herzustellen in Bezug auf die öffentlichen Interessen dienender Verwaltungstätigkeit ist gerade das Ziel, das der Gesetzgeber mit dem IZG-SH verfolgt. Geschäftspartnern kann und muss dies bekannt und bewusst sein, wenn sie sich auf einen Vertrag mit einer öffentlichen Stelle einlassen. Sie können sich wegen der bestehenden gesetzlichen Bindungen nicht darauf verlassen, dass von einer öffentlichen Stelle, die dem IZG-SH unterliegt, die möglicherweise im Privatrechtsverkehr übliche weiter reichende Vertraulichkeit eingehalten werden kann. Die Anwendung des IZG-SH kann daher auch nicht als Vertrauensbruch bewertet werden. Mit den Worten des VG Köln: „Wer beabsichtigt, mit dem Staat in geschäftliche Beziehungen einzutreten, darf unabhängig vom Regime des Informationsfreiheitsgesetzes vernünftigerweise nicht erwarten, dass bereits das Kaufinteresse als solches geheim gehalten wird."

Das VG Köln führt weiterhin aus, dass Dritte nur insoweit den Informationszugang beeinflussen können, als Informationen betroffen sind, an deren Geheimhaltung sie ein berechtigtes Interesse haben, namentlich an Betriebs- und Geschäftsgeheimnissen. Eine öffentliche Stelle kann jedoch für sich keine eigenen Betriebs- und Geschäftsgeheimnisse geltend machen. Der Schutz von Betriebs- und Geschäftsgeheimnissen stützt sich nach der Rechtsprechung des Bundesverfassungsgerichts auf die in Art. 12 Abs. 1 Grundgesetz niedergelegte Berufsfreiheit sowie auf den in Art. 14 Abs. 1 Grundgesetz enthaltenen Schutz des Eigentums. Artikel 12 und 14 Grundgesetz schützen das Berufs- und eigentumsbezogene Verhalten einzelner Personen oder Unternehmen am Markt. Öffentliche Stellen können sich hierauf nicht berufen.

Es ist möglich, dass ein Kaufvertrag Betriebs- und Geschäftsgeheimnisse enthält. Sollte dies der Fall sein, ist zu prüfen, ob der Anspruch des Antragstellers hierdurch ausgeschlossen wird. Nach § 10 Satz 5 IZG-SH ist in diesen Fällen eine Drittbeteiligung erforderlich; der Betroffene muss gefragt werden und selbst im Einzelnen darlegen, dass ein Betriebs- und Geschäftsgeheimnis vorliegt. Weiterhin ist eine Abwägung mit den öffentlichen Interessen an der Bekanntgabe der Informationen vorzunehmen, die einzeln begründet werden muss.

Das VG Düsseldorf hat mit Urteil vom 15. Oktober 2008 zu Recht ausgeführt, dass zumindest der Gesamtpreis bei einem Kaufvertrag nach Abschluss der Verhandlungen offenzulegen ist. An der Kenntnis des Kaufpreises besteht regelmäßig ein überwiegendes öffentliches Kontrollinteresse, wie es vom IZG-SH verfolgt wird. Vertragspartner können deshalb durch besondere Klauseln im Vertrag nicht verhindern, dass Grundstückskaufverträge veröffentlicht werden. Dies würde den Intentionen des Informationszugangsrechts widersprechen.

13

KERNPUNKTE

Nordsee Akademie

Inhouse-Kurse

Sommerakademie 2013

13 DATENSCHUTZAKADEMIE Schleswig-Holstein

Die kontinuierliche Nachfrage nach Weiterbildungsveranstaltungen der DATENSCHUTZAKADEMIE Schleswig-Holstein zeigt das stetige Interesse an qualifiziertem Datenschutz in Verwaltung und Betrieben sowie an wirksamen Datensicherheitsmaßnahmen in sozialen, schulischen und medizinischen Einrichtungen sowie bei dem Einsatz neuer Medien.

Neu * Neu * Neu * Neu * Neu * Neu

Datenschutz macht Schule

Mit dem Kursangebot „Entscheide DU – sonst tun es andere für Dich!“ trägt die DATENSCHUTZAKADEMIE dazu bei, Schülern und Schülerinnen ein Rüstzeug für datensicheren Umgang mit den neuen Medien zu geben. 23 Klassen mit insgesamt 500 Schülerinnen und Schülern wurden 2011 auf diese Weise erreicht. 2012 waren es schon 900 Schülerinnen und Schüler.

Neu * Neu * Neu * Neu * Neu * Neu

Im Schulungsjahr 2011 fanden 30 reguläre Kurse in Kiel und in der Nordsee Akademie in Leck statt, in denen 379 Teilnehmende von 12 Dozentinnen und Dozenten der DATENSCHUTZAKADEMIE zu vielfältigen Themen zum Datenschutz, zur Datensicherheit und zur Informationsfreiheit geschult wurden. 2012 war die Zahl der Teilnehmenden 355.

Sieben Absolventen des neuen „Power-Lehrgangs Datenschutz & Datensicherheit“ können sich nach erfolgreicher theoretischer und praktischer Prüfung „Systemadministrator mit Datenschutzzertifikat“ nennen. Mit dem Erwerb dieses Zertifikats können sie nachweisen, dass sie Einsatz und Betrieb von IT-Systemen unter datenschutzrechtlichen Aspekten sicher beherrschen. Die Systemadministratoren mit Datenschutzzertifikat verbessern ihre eigene persönliche und berufliche Qualifikation und geben ihren Arbeitgebern bzw. Auftraggebern die Sicherheit, dass die vorgeschriebenen technischen, organisatorischen und datenschutzrechtlichen Vorschriften bei der Systemadministration berücksichtigt werden. Nach einer schöpferischen Pause 2012 wird der Power-Lehrgang 2013 mit verbessertem Programm wieder starten.

Im Rahmen der „DATENSCHUTZAKADEMIE vor Ort“ nahmen in Inhouse-Sonderkursen 2011 weitere 419 Personen und im Jahr 2012 325 Personen an Fortbildungen zu folgenden Themen teil:

- IT-Grundschutz nach BSI
- Datenschutz in der Landesverwaltung
- Datenschutz in der Beratungsarbeit
- Datenschutz für Schulleiter
- Personalaktenrecht
- Einführung in den Sozialdatenschutz
- Datenschutz im SGB II
- Datenschutz in einer Beschäftigungs- und Qualifizierungsgesellschaft
- Datenschutz in der Arbeitsvermittlung
- Datenschutz und Datensicherheit im Bereich der Informationstechnologie
- Datenschutz am Arbeitsplatz
- Datensicherheitsrecht, Datenschutzkontrolle und Datenschutzaudits
- Datenschutz in der gerichtlichen Geschäftsstelle
- Beschäftigtendatenschutz
- Datenschutz in Verbänden
- Datenschutz in der Systemadministration
- Informationssicherheit für IT-Verantwortliche

Diese Inhouse-Veranstaltungen wurden in Auftrag gegeben von

- der Landesverwaltung Schleswig-Holstein,
- dem IT-Planungsstab im Innenministerium Schleswig-Holstein,
- dem Deutschen Paritätischen Wohlfahrtsverband (DPWV),
- den Mürwiker Werkstätten,
- der Beschäftigungs- und Qualifizierungsgesellschaft Flensburg (bequa),
- dem Institut für Qualitätsentwicklung an Schulen Schleswig-Holstein (IQSH),

- Dataport,
- der Beschäftigungs- und Qualifizierungsgesellschaft Ostholstein,
- dem Jobcenter Hansestadt Lübeck,
- dem Jobcenter Ostholstein,
- dem Jobcenter Kiel,
- dem Jobcenter Segeberg,
- der ARGE Stormarn,
- der Wirtschaftsakademie Schleswig-Holstein,
- dem Ministerium für Landwirtschaft, Umwelt und ländliche Räume (MLUR/MELUR),
- dem Amt Hohe Elbgeest,
- dem Landespolizeiamt Schleswig-Holstein,
- dem Landesamt für zentrale Aufgaben und Technik der Polizei, Brand- und Katastrophenschutz Mecklenburg-Vorpommern (LPBK M-V),
- dem Amtsgericht Flensburg,
- dem Landesjagdverband Schleswig-Holstein,
- der Technischen Universität Hamburg-Harburg,
- dem AOK Bundesverband.

Zur alljährlich am letzten Montag im August stattfindenden Sommerakademie der DATENSCHUTZAKADEMIE Schleswig-Holstein konnten im neuen Atlantic Hotel in Kiel sowohl 2011 als auch 2012 jeweils ca. 500 Gäste begrüßt werden. 2012 musste wegen der hohen Zahl der Anmeldungen vorzeitig die Zulassung gestoppt werden. Mit den Themen „Optimierte Verantwortungslosigkeit“ und „Sozialere Netzwerke im Internet – durch Datenschutz“ wurden hochaktuelle Themen aufgegriffen und fachkundig auf breiter Basis diskutiert.

Durch die Angebote der DATENSCHUTZAKADEMIE befassten sich somit in den Jahren 2011 und 2012 insgesamt 3.885 Personen auf ganz unterschiedlichen Ebenen mit Fragen von Datenschutz und Datensicherheit.

- Aus dem Schulungsbetrieb

Aufgrund der großen Nachfrage wurden die 2011 eingeführten Schülerkurse „Entscheide DU – sonst tun es andere für dich!“ 2012 mit steigenden Interessentenzahlen weitergeführt (siehe Kasten). Anregungen aus der Schulungsarbeit und aktuelle datenschutzpolitische Prioritäten führten zur Aufnahme weiterer wichtiger Themen.

Als arbeitsintensiv und anspruchsvoll gestaltete sich der 2011 neu eingeführte „Power-Lehrgang Datenschutz & Datensicherheit“. 20 Teilnehmer trafen sich in acht 7-stündigen Workshops im ULD, um sich ein qualifiziertes Wissen zum technisch-organisatorischen Datenschutz mit dem Schwerpunkt auf Client-Server-Umgebungen unter Windows 2003/2008 zu erwerben. Die externe Festplatte, auf der sich mehrere Übungsumgebungen (VMware Images von Server-Client-Betriebssystemen) befinden, ging zum Kursende in den Besitz der Teilnehmer über. Im von den Dozenten für die Kursdauer bereitgestellten E-Learning-Forum konnten untereinander Diskussionen geführt und Fragen zum Lehrinhalt gestellt werden.

Diese Erfahrungen mit E-Learning-Methoden gingen in die Vorbereitungen für neue Kurse in diesem Lernmodus ein, die 2011 erstmals eingeführt wurden: Der Kurs „Netzwerksicherheit“ (NET) wurde 2011 als E-Learning-Kurs mit einem Präsenztermin angeboten. Der weitere Arbeitsaufwand von vier bis fünf Tagen konnte von den Teilnehmenden zeit- und ortsvariabel erledigt werden. Der Betreuungsaufwand seitens der Dozentinnen und Dozenten ist allerdings erheblich. Der Kurs „LINUX als Serversystem sicher einsetzen“ (LINUX) konnte deshalb leider nicht stattfinden.

Nicht durchgeführt wurde auch das ambitionierte Projekt „Zukunftswerkstatt“, in dem kreativ, anspruchsvoll und unkonventionell Themen diskutiert werden sollten unter dem Motto: „Datenschutz neu denken!“

Die bewährten IT-Sicherheitskurse (unter Berücksichtigung der BSI-Grundschutztools) wurden weiter ausgebaut. Dazu gehören „IT-Sicherheitsmanagement“ (ITS), „Mit dem BSI-Grundschutztool zum IT-Sicherheitskonzept“ (BSI-GST) sowie „IT-Grundschutz nach BSI, Praktische Umsetzung in einer Organisation“ (BSI-Praxis), welche die Absolventen befähigen, die Sicherheit von Verfahren oder Geschäftsprozessen und die Verwaltung von IT-Verbünden von Organisationen mithilfe der IT-Grundschutzmethode umzusetzen.

Die seit jeher gut eingeführten und besuchten Grundlagenkurse der DATENSCHUTZAKADEMIE werden weiterhin gut angenommen. Dies sind „Datenschutzrecht/Datensicherheit für behördliche Datenschutzbeauftragte“ (DR/DT), „Einführung Datenschutz im Schulsekretariat“ (ES) und „Führung von Personalakten“ (PA). 2012 wurde der Kurs „Rechtsfragen des Landesdatenschutzgesetzes“ (LDSG-R) neu aufgelegt.

Weitere Schwerpunkte der Akademiearbeit bilden traditionell die Kurse zum betrieblichen Datenschutz. In den Eintageskursen „Grundkurs Bundesdatenschutzgesetz“ (BDSG-I), „Betriebliches Datenschutzmanagement nach dem Bundesdatenschutzgesetz“ (BDSG-II) und „Technischer Datenschutz/ Systemdatenschutz nach dem BDSG“ (SIB) werden den betrieblichen Datenschutzbeauftragten die Grundzüge des für die Wirtschaft geltenden Datenschutzrechts vermittelt.

Großen Zuspruch erfuhr der 2011 neu eingerichtete dreitägige Lehrgang „Betrieblicher Datenschutz – Kompakt“ (BDK), der die Inhalte der drei oben genannten Kurse in handlungsoptimierter und praxisbezogener Form zusammenfasst und so den Absolventen einen guten Start in ihre Tätigkeit als betriebliche Datenschutzbeauftragte gibt. Von ursprünglich zwei Terminen 2011 wurde er 2012 auf drei Termine erweitert und wird 2013 mit vier Terminen starten.

Trotz der zunehmenden Sensibilisierung im medizinischen Bereich in Bezug auf ständige Neuerungen im Gesundheitswesen erfahren die Kurse „Datenschutz im Krankenhaus“ (DK) und „Datenschutz in der Arztpraxis“ (AR) nicht die wünschenswerte Resonanz. Sie werden 2013 zum Kurs „Datenschutz im Medizinbereich“ (MED) zusammengefasst. Dagegen herrscht im Sozialbereich lebhafte Nachfrage: Jobcenter, Pflegedienste und Behinderteneinrichtungen buchen regelmäßig für ihre Mitarbeiterinnen und Mitarbeiter Fortbildungsveranstaltungen zu Themen des Sozialdatenschutzes.

Das Jahresprogramm der DATENSCHUTZAKADEMIE finden Sie unter

https://www.datenschutzzentrum.de/akademie/programm/

auf der Homepage des Unabhängigen Landeszentrums für Datenschutz (ULD).

Index

A

ABC4 Trust **122**
Abgabenordnung **70**
Adressdaten **119**, **141**
Adresshandel **37**, **119**
Akteneinsicht **42**, **50**
Anonymisierung **129**, **143**
Anti Doping Agentur (NADA) **85**
Anti-Doping Agency (WADA) **85**
Antiterrordatei **44**, **54**
Antiterrordateigesetz (ATDG) **44**, **45**
AOK Schleswig-Holstein **56**
Arbeitnehmer **19**, **147**
Arbeitsgemeinschaft (ARGE) **56**
Arbeitslosengeld **56**
Artikel-29-Datenschutzgruppe **118**, **139**, **154**
@rtus **38**, **39**
Auftragsdatenverarbeitung **28**, **33**, **85**, **156**
Auskunft **48**, **51**, **70**, **74**, **91**
Auskunfteien **80**, **82**
Auskunftssperre **42**
Ausländerverwaltung **54**
Ausländerzentralregister (AZR) **55**
Authentifizierung **118**
Authentisierung **103**, **124**

B

BAföG21 **102**
Banken **78**, **86**, **87**, **91**
Beratung **23**, **107**
Beschäftigtendatenschutz **19**
Betreuungsakten **60**
Bilddaten **29**, **113**, **128**
Bonitätsabfrage **82**, **83**
Botnetz **128**
Bring Your Own Device (BYOD) **147**
Browser **148**
Bundesamt für Sicherheit in der Informationstechnik (BSI) **133**
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI) **136**
Bundesdatenschutzgesetz (BDSG) **76**, **80**, **89**
Bundeskriminalamt **39**, **82**
Bundesmeldegesetz (BMG) **36**
Bundesverfassungsgericht **47**, **54**, **70**
Bußgeld **24**, **37**, **87**

C

Chipkarte **124**
Clearingstelle **64**, **100**
Cloud Computing **84**, **124**, **125**, **154**
Code of Conduct **77**

D

Dataport **11**, **32**, **97**, **102**, **103**, **133**, **134**
DATENSCHUTZAKADEMIE Schleswig-Holstein **163**
Datenschutzaudit **131**
  Kreis Plön **132**
  KVSH **131**
  Nordbits **133**
  Statistikamt Nord **134**
  ZIAF **133**
Datenschutz-Auskunftsportal **125**
Datenschutzbeauftragter
  behördlicher **37**, **45**, **98**, **101**, **105**, **106**
  betrieblicher **20**
Datenschutz-Grundverordnung **19**, **144**, **153**, **156**, **157**
Datenschutz-Gütesiegel **135**
  Anforderungskatalog **137**
  Prüfstellen **136**
  Rezertifizierung **135**
  Sachverständige **136**
  Zertifizierung **135**
Datenschutzmanagement **98**
Datenschutz-Schutzziele **9**, **124**, **137**, **154**
Datenschutzverordnung Schule (DSVO Schule) **66**
Datensicherheit **32**, **34**, **78**, **131**
Datensparsamkeit **76**, **99**
Datenspeicherung **38**
Datenübermittlung **80**
Datenvermeidung **76**
De-Mail **27**, **136**
Dokumentation **30**, **31**, **38**, **52**, **53**

Dopingbekämpfung **85**
DOS – Datenschutz in Online-Spielen **126**

E

E-Government **27**, **34**, **159**
Einwilligung **37**, **40**, **61**, **63**, **65**, **74**, **83**, **88**, **113**
Elektronische Gesundheitskarte (eGK) **27**, **65**
Elektronische Signatur **31**, **32**, **55**
Elektronischer Einkommensnachweis (ELENA) **55**
Elektronischer Identitätsnachweis (eID) **34**, **124**
Elektronisches Lastschriftverfahren (ELV) **80**
E-Mail-Postfächer **106**
Energieversorgungsunternehmen **108**
Europa **153**
Europäische Kommission **117**
Europäische Union (EU) **23**
European Privacy Seal (EuroPriSe) **137**, **138**
  Gutachter **138**, **140**
  Rezertifizierung **141**, **143**
  Zertifizierung **141**
  Zertifizierungskriterien **138**
  Zertifizierungsverfahren **139**

F

Facebook **66**, **111**, **112**, **113**, **115**
Facebook Insights **111**, **115**
Facebook-Fanpage **12**, **66**, **111**
Facebook-Reichweitenanalyse **12**, **111**
Finanzamt **71**
Finanzministerium **30**
Flugdaten **44**
forumSTAR **103**
Funkchips **78**
FutureID **123**

G

Gebühren **101**
Gebühreneinzugszentrale (GEZ) **119**
Geodaten **29**
Geodateninfrastrukturgesetz (GDIG) **29**
GES-3D – Multi-Biometrische 3D-Gesichtserkennung **127**
Geschäftsgeheimnis **76**
Gesetz über kommunale Zusammenarbeit (GkZ) **33**
Gesichtserkennung **112**, **115**, **127**
Google **148**, **155**
Grundbuch **52**

H

Hashwert **49**
Hausarztzentrierte Versorgung **61**
Hausbesuche **118**
Hinweis- und Informationssystem der Versicherungswirtschaft (HIS) **73**

I

Identitätsmanagement **121**, **157**
IEC **157**
Informationsfreiheit **9**, **159**, **160**
Informationsfreiheitsgesetz (IFG) **9**, **10**
Informationssicherheitsleitlinie (ISMS) **100**
Informationszugangsgesetz (IZG-SH) **9**, **10**, **159**, **160**
Inkassobüro **28**
INPOL **43**
Internetfernsehen (IPTV) **116**
Internetgesetzgebung **15**
Intervenierbarkeit **124**, **154**
IP-Adresse **115**
ISO **133**, **157**
ISO 27001 **133**
IT-Labor **147**
IT-Produkt **138**, **141**, **143**
IT-Standard **99**

J

Jugendamt **58**, **59**, **60**
Justizverwaltung **46**
Justizvollzugsanstalten **53**

K

Kassenärztliche Vereinigung Schleswig-Holstein (KVSH) **131**
Kommunalverwaltung **98**
Konferenz der Datenschutzbeauftragten des Bundes und der Länder **15**, **18**, **42**
Kontrollen **104**
KoPers **31**, **102**
KoSIT **99**

Kraftfahrt-Bundesamt (KBA) **34**
Krankenhäuser **64**, **75**
Krankenhausinformationssystem (KIS) **135**
Krankenkassen **27**
Krebsregister **62**, **63**
Kreditkartendaten **51**
Kreis Plön **132**
Kundendaten **87**, **90**

L

Landesdatenschutzgesetz (LDSG) **9**
Landesnetz Bildung (LanBSH) **67**
Landtag **12**
Leistungskontrolle **94**
Löschung **55**, **113**

M

Mandantenfähigkeit **97**
Medizinischer Dienst der Krankenversicherung (MDK) **56**
Meldebehörde **36**
Meldedaten **60**
Melderecht **60**
Melderegister **36**, **42**
Meldewesen **36**, **100**
MESTA **48**
Mobilfunk **92**
MonIKA **128**
Monitoring **128**, **139**
Mozilla **148**

N

NADIS **43**
Near Field Communication (NFC) **78**
Neuer Personalausweis (nPA) **27**, **34**, **123**, **124**
Nichtverkettbarkeit **124**, **154**
Nordbits **133**
Nutzerdaten **111**, **116**

O

Online Behavioural Advertising (OBA) **117**
Online-Banking **118**
Online-Dienste **128**
Online-Spiele **126**
Open Data **159**
Outsourcing **28**

P

Patientenarmbänder **64**
Patientendaten **61**, **65**, **131**
Patientengeheimnis **61**, **64**
Personalakten **31**, **32**
Personalaktendaten **30**
Personalverwaltung **102**
Polizei **38**, **43**, **45**, **46**
PrimeLife **121**
Privacy and Identity Management for Europe (PRIME) **121**
Privacy-ABCs **122**
Projekte
- ABC4Trust **122**
- Datenschutz-Auskunftsportal **125**
- DOS – Datenschutz in Online-Spielen **126**
- FutureID **123**
- GES-3D – Multi-Biometrische Gesichtserkennung **127**
- MonIKA **128**
- PrimeLife **121**
- SurPRISE **127**
- TClouds **124**

Protokolldaten **49**
Protokollierung **53**
Pseudonymisierung **129**, **143**

R

Registry Information Service on European Residents (RISER) **141**
Reichweitenanalyse **12**, **17**, **42**
Rundfunkänderungsstaatsvertrag **118**
Rundfunkgebühren **118**

S

Safe Harbor **115**, **155**
Schnittstellensicherheit **149**
Schuldnerverzeichnis **51**
Schule **66**, **67**, **68**, **69**
Schülerdaten **66**, **67**
Schweigepflicht **57**, **64**, **77**
Schweigepflichtentbindungserklärung **62**, **74**, **77**

Sicherheitsbehörden **41**
Sicherheitsüberprüfungen **40**
Sicherungsverwahrungsvollzugsgesetz **50**
Smart Meter **108**
Smartphone **66**, **67**, **121**
Social Media **16**, **17**, **25**
Social Plugins **12**, **17**
Sommerakademie **164**
Sozialdaten **58**
Spam-Mail **128**
Sparkassen **78**
Speicherung **38**, **48**, **55**, **74**, **75**, **77**
Standardisierung **157**
Statistikamt Nord **134**
Steuerakten **160**
Steuergeheimnis **27**
Steuerunterlagen **71**, **160**
Steuerverwaltung **70**
Stiftung Datenschutz **18**
Strafverfahren **42**, **49**
SurPRISE **127**
Systemdatenschutz **97**

T

TClouds **124**
Techniker Krankenkasse (TK) **57**
Telekom **116**, **138**
Telekommunikation **47**
Telekommunikationsdaten **66**
Telekommunikationsgeheimnis **127**
Telekommunikationsüberwachung **40**, **46**
Telemediengesetz (TMG) **24**
Terrorismusbekämpfungsgesetz (TBG) **44**
Therapieunterbringungsvollzugsgesetz **50**
TKÜ-Zentrum Nord **40**
Tracking **117**, **121**, **148**
Transparenz **11**, **87**, **100**, **105**, **108**, **159**, **160**
Transparenzgesetz **11**, **159**

U

Überwachung **47**
ULD-Innovationszentrum (ULD-i) **121**
Umweltinformationsgesetz (UIG) **9**, **10**
US-Sicherheitsbehörden **153**, **155**, **156**

V

Verfahren **30**, **105**, **112**
Verfahrensverzeichnis **105**
Verfassungsschutz **38**, **44**
Versicherungen **74**, **75**, **76**
Verwaltung **27**, **98**, **160**
Videoüberwachung **68**, **93**, **94**
Visa-Warndatei **54**
Volkszählungsurteil **39**
Vorabkontrolle **101**
Vorratsdatenspeicherung **55**

W

W3C (World Wide Web Consortium) **117**, **157**
Werbung **90**, **111**, **117**, **118**
Windows 8 **150**
Windows Server 2012 **150**
Wirtschaft **73**

X

XTA **100**

Z

Zahlungsinformationssystem für Agrarfördermittel (ZIAF) **133**
Zeitwirtschaftssystem **30**
Zertifizierung **139**
Zweckverband **32**, **33**

ULD

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein

Schleswig-Holsteins
Servicezentrum für Datenschutz
und Informationszugang

https://www.datenschutzzentrum.de/material/tb/