Tätigkeitsbericht 2009

des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

Berichtszeitraum: 2008, Redaktionsschluss: 15.02.2009
Landtagsdrucksache 16/2439

(31. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz)

Dr. Thilo Weichert
Leiter des Unabhängigen Landeszentrums
für Datenschutz Schleswig-Holstein, Kiel

Impressum

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Holstenstraße 98
24103 Kiel

Mail: mail@datenschutzzentrum.de
Web: www.datenschutzzentrum.de

Satz und Lektorat: Gunna Westphal, Kiel

Illustrationen: Reinhard Alff, Dortmund

Umschlaggestaltung: Martin Papp, Eyekey Design, Kiel

Druck: Pirwitz Druck, Kiel

Inhaltsverzeichnis

1	**Datenschutz in Schleswig-Holstein**	**7**
1.1	Bewegung aus dem hohen Norden	7
1.2	Datenschutzbeauftragte beim Datenschutzbeauftragten	9
1.3	Unabhängiges Datenschutzzentrum Nord?	10
2	**Datenschutzgesetzgebung auf Bundesebene**	**12**
2.1	Defizit Arbeitnehmerdatenschutz	12
2.2	Defizit Bundesdatenschutzgesetz	13
2.3	Defizit Datenschutz-Audit	15
2.4	Internationale Regulierung als nationale Aufgabe	16
3	**Telefonie im Landeshaus**	**17**
4	**Datenschutz in der Verwaltung**	**18**
4.1	Allgemeine Verwaltung	18
4.1.1	Bundesmeldegesetzentwurf – Ein Rückschritt für Schleswig-Holstein?	18
4.1.2.	Online-Melderegisterauskunft wird zum Erfolgsmodell	19
4.1.3	Schranken bei Melderegisterauskünften an gewerbliche Adressvermittler	20
4.1.4	Übermittlung von gesperrten Meldedaten zu Wahlwerbezwecken	22
4.1.5	Spendenaufruf der Feuerwehr – aber bitte nicht mit Meldedaten	23
4.1.6	Der neue „elektronische“ Personalausweis	24
4.1.7	Praxis kommunaler Bürgerbüros	26
4.1.8	Neues Landesbeamtengesetz in Vorbereitung	27
4.2	Polizei und Verfassungsschutz	29
4.2.1	Landesverwaltungsgesetz (LVwG) – Erfahrungen mit dem neuen Polizeirecht	29
4.2.2	Online-Durchsuchung für Polizei und Verfassungsschutz	31
4.2.3	Landeskriminalamt überprüft für Deutsche Bundesbank Fremdpersonal	33
4.2.4	Die Polizei bei der Kommunalwahl im Einsatz	34
4.2.5	Die unendliche Geschichte: Kontrolle der Abteilung 3 des Landeskriminalamtes	35
4.2.6	Landesverfassungsschutzgesetz kontra Verfassung	36
4.2.7	Antiterrordatei – Wer kontrolliert die Protokolldaten?	38
4.2.8	Arbeitszeugnisse in Sicherheits- bzw. Sicherheitsüberprüfungsakten	39
4.2.9	DIANA beim Verfassungsschutz in Schleswig-Holstein	40
4.3	Justizverwaltung	40
4.3.1	Neues in Sachen Vorratsdatenspeicherung	40
4.3.2	Telefonieren im Strafvollzug	42
4.3.3	Vernichtung von Gefangenenpersonalakten – Eine lästige Pflicht?	43
4.3.4	Kieler Sicherheitskonzept Sexualstraftäter (KSKS)	44
4.3.5	Regelmäßige HIV-Infektionsmeldung über Gefangene für die Justiz?	46
4.3.6	„Freiwillige“ Rechnerdurchsuchung durch Interessenverband	47
4.4	Verkehr	48
4.4.1	Kontrollen von Kopfstellen der Kfz-Zulassungs- und Fahrerlaubnisbehörden	48
4.4.2	Fachaufsicht über Kfz-Zulassungsbehörden weiter auf Tauchstation	48
4.4.3	Update: Anbindung Fahrerlaubnisbehörden – Kraftfahrt-Bundesamt (KBA)	49

4.5	Soziales	50
4.5.1	Anforderung von Kontoauszügen – Bundessozialgericht bestätigt ULD	50
4.5.2	Wenn Mitarbeiter in Behördenrechnern privat recherchieren können	51
4.5.3	Wenn Mitarbeiter von Hartz-IV-Behörden einfach zu viel wissen wollen	53
4.5.4	eGK – die Einführung verschiebt sich weiter	54
4.5.5	Qualitätskontrolle des Mammografie-Screenings über das Krebsregister?	55
4.5.6	Unzulässige Adressbeschaffung der gesetzlichen Krankenkassen	57
4.5.7	Kindeswohlgefährdung – Kinderschutz braucht Datenschutz!	58
4.5.8	Kontrollierende Einladungen zur freiwilligen Kinderuntersuchung	59
4.5.9	Bestattungsgesetz des Landes	62
4.5.10	Datenerhebungsbefugnis der Heimaufsicht	63
4.5.11	ELENA-Gesetzentwurf auf den Weg gebracht	64
4.6	Schutz des Patientengeheimnisses	65
4.6.1	Entwurf eines Gendiagnostikgesetzes des Bundes	65
4.6.2	Versagung der Einsicht in Patientenakte beim Betriebsarzt	66
4.6.3	Einhaltung von Sicherheitsstufen bei der Vernichtung von konventionellen Datenträgern	67
4.7	Steuerverwaltung	68
4.7.1	Einführung der Steueridentifikationsnummer	68
4.7.2	Änderung des Kirchensteuergesetzes	69
4.7.3	Zusendung falscher Steuerunterlagen	69
4.7.4	Anforderungen an die Führung eines Fahrtenbuches	70
4.7.5	Rolf Uwe Frank Maier-Schulz – zur Erforderlichkeit des ganzen Namens	71
4.7.6	Kontoverbindungsdaten beim Finanzamt	71
5	**Datenschutz in der Wirtschaft**	**73**
5.1	BDSG-Novellen	73
5.1.1	Gesetzentwurf zum Auskunfteibereich und zum Scoring	73
5.1.2	Gesetzentwurf zur Datenverarbeitung zu Werbezwecken	74
5.2	Geodaten – Regeln für die wirtschaftliche Nutzung	75
5.3	Lebensmitteldiscounter – der nichts wissen wollte und doch alles wusste	77
5.4	Bei Anruf Betrug – illegaler Handel mit Adress-, Telefon- und Bankdaten	80
5.5	Neues aus der Versicherungswirtschaft: Licht und Schatten	83
5.5.1	Auf dem Weg zu branchenweiten Verhaltensregeln?	83
5.5.2	Hinweis- und Informationssystem – Kein Land in Sicht!	85
5.5.3	Finanzdienstleistungsaufsicht kontra Datenschutz	87
5.6	Dubioses Geschäft mit Zeitschriftenabos	88
5.7	Videoüberwachung – Best of	89
5.7.1	Webcam zum Kaffee – eine beliebte Mischung	89
5.7.2	Videoüberwachung im Rauchmelder	91
5.7.3	Bild und Ton im Bordell	91
5.7.4	Videoüberwachung im Bus – Weitergabe an die Presse	92
5.8	Einzelfälle	93
5.8.1	Mülltonnen – Spiegel funktionierender Datenvernichtung	93

5.8.2	Wertpapierhandelsgesetz – die umfangreichen Kundenfragebögen	94
5.8.3	Laptop auf Abwegen	95
5.8.4	Werbewiderspruch – mit guten Augen klar im Vorteil	96
5.8.5	Es gibt kein Konzernprivileg	96
5.8.6	Veröffentlichung von Spielergebnissen im Internet	97
5.8.7	Radio-Gewinnspiel – Rückruf trotz Rufnummernunterdrückung?	98
5.8.8	Creditreform – Aufforderung zum Datenabgleich an Betroffene	99
5.8.9	Unberechenbare Fotobestellung	100
5.8.10	Der Rechtsanwalt und sein Freund	101
5.8.11	Ein Rechtsanwalt, der zu viel wusste	102
6	**Systemdatenschutz**	**103**
6.1	Wer testet, sündigt nicht	103
6.2	Die neue Datenschutzverordnung	107
6.3	Die Europäische Dienstleistungsrichtlinie	109
6.4	OSCI-Transport 2.0 und SAFE: es gibt einiges zu tun	112
6.5	Kontodatenskandal – Datenverarbeitung im ULD	114
6.6	Einsatz privater Geräte	115
6.7	IP-Adressen 1: Grundsätzliches	117
6.8	IP-Adressen 2: Umsetzung in Schleswig-Holstein	119
6.9	Modularisierung der Dokumentation – sinnvoll nicht nur beim Geoserver	120
6.10	ISMS Dataport	123
6.11	Zielarchitektur Basis-Infrastruktur bei Dataport	124
6.12	Internetnutzung: Privat oder rein dienstlich?	125
6.13	Überwachung der Internetnutzung von Mitarbeitern	128
6.14	Kontrollen vor Ort	131
6.14.1	Prüfungen bei Stadtverwaltungen: Lob für Heiligenhafen	131
6.14.2	Amtshilfe bei einer Prüfung	131
7	**Neue Medien**	**133**
7.1	Kundendaten? Google doch mal!	133
7.2	Google Analytics Services – Webtracking auf dem Prüfstand	134
7.3	Google Street View	135
7.4	Rottenneighbor.com – Nachbarn an den Pranger!	137
8	**Modellprojekte und Studien**	**140**
8.1	ULD-i – das Innovationszentrum Datenschutz & Datensicherheit	140
8.2	Datenschutzdiskurse im „Privacy Open Space“	140
8.3	Neue Datenschutzkonzepte im Identitätsmanagement	142
8.4	Die Zukunft von Identität: Fortschritte im Exzellenznetzwerk FIDIS	143
8.5	AN.ON – Anonymität online in den Wirren der Vorratsdatenspeicherung	145
8.6	PRISE – Datenschutz für Sicherheitstechnik	146
8.7	DOS – Datenschutz in Online-Spielen	148
8.8	Das Virtuelle Datenschutzbüro festigt seine Position	149
8.9	„Twinning Light“ mit Malta erfolgreich abgeschlossen	150
8.10	Datenschutz für Biobanken	151
8.10.1	bdc\Audit – Auditierung von Biobanken	151
8.10.2	BMB-EUCoop	152

8.11	RISER (Registry Information Service on European Residents)	152
8.12	IM Enabled	154
8.13	EuroPriSe (European Privacy Seal)	155
9	**Audit und Gütesiegel**	**158**
9.1	Bundesauditgesetz – gute Absicht, schlecht gemacht	158
9.2	Datenschutz-Audits	159
9.2.1	Neue Hinweise zur Durchführung eines Datenschutz-Behördenaudits	159
9.2.2	Zahlstellen und InVeKoS-Agrar-Förderprogramm (ZIAF)	161
9.2.3	Ministerium für Bildung und Frauen	163
9.2.4	Kreis Plön	164
9.2.5	Auditverfahren Unfallkasse Nord	165
9.3	Datenschutz-Gütesiegel	166
9.3.1	Abgeschlossene Gütesiegelverfahren	166
9.3.2	Sachverständige	168
9.4	EuroPriSe	169
9.4.1	Zertifizierungskriterien	169
9.4.2	Zertifizierungsverfahren	170
9.4.3	Zulassung von Gutachtern	171
9.4.4	Abgeschlossene EuroPriSe-Verfahren	172
9.4.5	Laufende EuroPriSe-Verfahren	174
10	**Aus dem IT-Labor**	**175**
10.1	Der mobile Blackberry	175
10.2	Virtualisierung	177
10.3	Multifunktionsgeräte und Digitalkopierer	178
10.4	Systeme ohne Herstellersupport	180
10.5	Google Chrome	181
10.6	„Ich weiß, was du gestern gelesen hast!“	182
10.7	Personal Firewalls	183
11	**Europa und Internationales**	**185**
11.1	Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit	186
11.2	Innereuropäischer Datenaustausch à la „Schwedische Initiative“	188
12	**Informationsfreiheit**	**189**
12.1	EU-Transparenzinitiative und das Agrar- und Fischereifonds-Informationen-Gesetz	189
12.2	Was kostet die Sanierung des Holstentores?	190
12.3	Ein gesunder Insolvenzverwalter wendet sich an eine Krankenkasse	190
12.4	Keine Wahl bei der Wahlkreiseinteilung?	191
12.5	Die Geschäftsgeheimnisse des Bundes	192
12.6	Informationsfreiheit auf dem Friedhof	193
12.7	Wer hat mich verraten?	194
12.8	Informationsfreiheit für 1-Euro-Jobber	194
12.9	„Vorhandene“ Informationen im Internet	195
13	**DATENSCHUTZAKADEMIE – Nie war sie so wertvoll wie heute!**	**196**
	Index	**204**

1 Datenschutz in Schleswig-Holstein

Das letzte Jahr war für den Datenschutz in Schleswig-Holstein in vieler Hinsicht ein **ruhiges Jahr**. Abgesehen von der teilweise zweifellos kritikfähigen Novelle des Landesverfassungsschutzgesetzes (Tz. 4.2.6) gab es auf landespolitischer Ebene wenig Aufregung und wenige Konfliktpunkte. Für das Unabhängige Landeszentrum für Datenschutz (ULD) blieben auch größere innerorganisatorische Herausforderungen aus, da die Dienststelle schon in den Vorjahren ihre Standbeine gefestigt hat. Zu unseren Aufgaben gehört Folgendes: Kontrollen im öffentlichen wie im nicht öffentlichen Bereich, Bearbeitung von Petitionen, Beratung von Bürgerinnen und Bürgern sowie Daten verarbeitenden Stellen und Politik, Öffentlichkeitsarbeit – dies alles (in Bezug auf öffentliche Stellen) nicht nur zum Thema Datenschutz, sondern auch zur Informationsfreiheit (Tz. 12). Weitere Tätigkeiten sind: Aus- und Fortbildung (Tz. 13), Wissenstransfer in die Wirtschaft durch das ULD-i (Tz. 8.1), Erstellung von Gutachten, Durchführung von Projekten (Tz. 8) und – mit zunehmender Wichtigkeit – von Audit- und Gütesiegelverfahren (Tz. 9). Ein personeller Einschnitt war im Februar 2008 der Wechsel von Johann Bizer als stellvertretender Dienststellenleiter in den Vorstand von Dataport und seine Nachfolge durch eine Informatikerin aus dem eigenen Hause: Marit Hansen.

Die relativ ruhigen datenschutzpolitischen Rahmenbedingungen im Land waren für das ULD nötig, um angesichts der angespannten personellen Situation die von außen kommenden Bedürfnisse einigermaßen erfüllen zu können. Die Meldungen von **gravierenden Datenschutzverstößen** erschütterten die gesamte Republik, hatten in den meisten Fällen direkte Bezüge zu Schleswig-Holstein und forderten das ULD – oft über die Grenzen des Zumutbaren. Nur durch eine hohe Identifikation der Mitarbeiterinnen und Mitarbeiter mit ihrer Arbeit und deren ungewöhnlich starkes Engagement konnte – gepaart mit Improvisationsgeschick und im Ergebnis hoffentlich weitgehend erfolgreich – versucht werden, den Anforderungen, die auf das ULD durch Bürgerinnen und Bürger, Verwaltung und Wirtschaft, anderen Datenschutzeinrichtungen und Presse einstürmten, gerecht zu werden.

1.1 Bewegung aus dem hohen Norden

Die Anforderungen an das ULD wurden vorrangig von betroffenen Bürgerinnen und Bürgern sowie Daten verarbeitenden Stellen in Schleswig-Holstein gestellt. Die Zahl der Eingaben im Sozialbereich steigerten sich z. B. 2008 im Vergleich zum Vorjahr um ein Drittel, im Medizinbereich gar um 60 %. Die Anforderungen kamen aber oft auch von **außerhalb des Landes**, ohne dass sich das ULD dem hätte entziehen können. Denn die nationalen und internationalen Entwicklungen haben direkte Auswirkungen auf den Grundrechtsschutz der schleswig-holsteinischen Bevölkerung und auf die hier tätigen Institutionen: Viele nationalen Meldungen und Ereignisse zwangen das ULD zum Tätigwerden, etwa als von exzessiven Mitarbeiterbespitzelungen in einem Konzern zu lesen war, der auch im hohen Norden eine große Filiale betreibt, als die Änderung des dritten Abschnitts des Bundesdatenschutzgesetzes (BDSG) in Angriff genommen wurde, mit absehbar gravierenden Auswirkungen auf die heimische Wirtschaft, oder als wir von einem –

in dem Ausmaß bisher nicht vorstellbaren – Missbrauch von Kontodaten und illegalen Datennutzungen für Werbezwecke erfuhren, wovon Zigtausende Frauen und Männer in Schleswig-Holstein betroffen sind.

Die in unserer Informationsgesellschaft praktizierte Form personenbezogener Datenverarbeitung kennt **keine Landesgrenzen** und immer weniger nationale Grenzen. Dies zwingt Datenschutzbehörden bundesweit, in Europa und in mancher Hinsicht sogar global zusammenzuarbeiten und zu versuchen, Entwicklungen auf nationaler und internationaler Ebene zu beeinflussen. Statt sich dabei treiben zu lassen, ist das ULD schon seit Jahren bestrebt, eine gestaltende Rolle zu spielen. Dies zahlt sich immer wieder aus. Nur zwei Beispiele: Durch unsere frühe Beschäftigung mit dem Thema Kredit-Scoring (28. TB, Tz. 8.8) war und ist es dem ULD jetzt einfach möglich, die Behandlung eines Bundesgesetzentwurfes zu diesem Thema qualifiziert zu begleiten. Die Einführung von Gütesiegel und Audit im Jahr 2000 erlaubt es dem Land Schleswig-Holstein, einen wesentlichen Beitrag für die Entwicklung auf Bundesebene und in anderen europäischen Ländern zu leisten.

Im Vordergrund steht immer die **Arbeitsteilung**. Keine Datenschutzbehörde kann in allen Bereichen die gleiche hohe rechtliche und technische Expertise bereithalten und einbringen. Die Kooperationen des ULD im Düsseldorfer Kreis (DK), dem bundesweiten Zusammenschluss der Aufsichtsbehörden im nicht öffentlichen Bereich, in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSB-K) sowie in der Konferenz der Informationsfreiheitsbeauftragten (IFK) sind erfolgreich und weitgehend reibungsfrei. So war es möglich, über Stellungnahmen, z. B. gegenüber dem Bundesgesetzgeber, dem Bundesverfassungsgericht, einzelnen Branchen sowie Ländergrenzen überschreitend aktiven Daten verarbeitenden Stellen, über Veranstaltungen und Prüfaktionen gemeinsam wesentlichen Einfluss zugunsten von Datenschutz und Informationsfreiheit zu nehmen. Teilweise haben wir im ULD hierbei die Initiative und Führung übernommen, so z. B. über die Wahrnehmung der Vorsitze der Arbeitsgruppe Versicherungswirtschaft des DK und des Arbeitskreises Sicherheit der DSB-K. In den meisten Arbeitsbereichen überlassen wir die Leitung den Kolleginnen und Kollegen im Bund, in anderen Ländern oder auch – im internationalen Bereich – in anderen Staaten. Doch auch in diesen Bereichen bedarf es – um bestmögliche kollektive Ergebnisse zu erzielen – der aktiven und qualifizierten Beiträge aller Datenschutzbehörden, also auch des ULD.

Es lässt sich feststellen: Die arbeitsteilige **föderale Organisation des Datenschutzes** in Deutschland ist problem- und bürgernah, qualifiziert und effektiv. Sie wird derzeit noch ein wenig behindert durch die in vielen Bundesländern weiterhin bestehende organisatorische Spaltung von öffentlichem und nicht öffentlichem Bereich. Allein aus europarechtlichen Gründen und im Interesse der verfassungsrechtlich geforderten Unabhängigkeit der Datenschutzbehörden wurde diese Spaltung in vielen Bundesländern aufgehoben, so zuletzt in Rheinland-Pfalz. Auch die organisatorische Verbindung von Informationsfreiheit und Datenschutz erweist sich – trotz der sich scheinbar widerstreitenden Zielsetzungen – als äußerst nutz-

bringend: Es geht um die Optimierung dieser beiden Seiten der gesellschaftlichen und individuellen Selbstbestimmung im Interesse der Menschen und in organisatorischer Unabhängigkeit.

1.2 Datenschutzbeauftragte beim Datenschutzbeauftragten

Auch für das ULD gelten das Landesdatenschutzgesetz (LDSG) und die Datenschutzverordnung (DSVO). Die Datenschutzdienststelle kann danach einen Datenschutzbeauftragten bestellen. Doch ist das in einer Behörde, deren Hauptaufgabe die **Überwachung der Gesetze** und Vorschriften über den Datenschutz darstellt, überhaupt notwendig? Nach den Erfahrungen der behördlichen Datenschutzbeauftragten des ULD lässt sich diese Frage eindeutig mit Ja beantworten, auch wenn sich die Arbeitsschwerpunkte von denen der Datenschutzbeauftragten anderer Behörden im Land unterscheiden.

Ein großer Vorteil bei deren Tätigkeit besteht in der **hohen Sensibilisierung** aller ULD-Mitarbeiterinnen und -Mitarbeiter in Bezug auf den Datenschutz. Weder bei der Leitung noch in den einzelnen Referaten muss Überzeugungsarbeit geleistet werden. Diesen Startvorteil haben andere Datenschutzbeauftragte im Land oft nicht. Häufig wird der Datenschutz – auch auf Leitungsebene – immer noch als lästige Pflichtübung angesehen.

Die Arbeit der ULD-Datenschutzbeauftragten ist eine Bereicherung für unseren „Datenschutzalltag“. Neben ihren gesetzlichen Standardaufgaben, wie z. B. das Führen des Verfahrensverzeichnisses, ist sie konsequent in alle datenschutzrelevanten **Arbeitsprozesse eingebunden**. Dies gilt z. B. für die interne technische Ausgestaltung der IT-Infrastruktur wie auch für Verfahren mit Außenbezug, etwa für die Verarbeitung der Kontendaten beim Adresshandelskandal (Tz. 6.5). Damit die Datenschutzbeauftragte nicht einfach „vergessen“ wird, wurden Arbeitsabläufe im ULD entsprechend angepasst, optimiert und standardisiert.

Die „**datenschutzkonforme Dokumentation** nach LDSG und DSVO“ ist die Aufgabe jeder Behörde. Sie erfordert eine behördeninterne Zusammenarbeit zwischen Datenschutzbeauftragtem, Administration, Referatsleitungen und Dienststellenleitung. Auch bei uns ergibt sich immer wieder Optimierungsbedarf. Die Verbesserungsmöglichkeiten aus eigenen Erfahrungen können dann einfließen in Handreichungen, Beratungen und Schulungen, z. B. die Praxisforen der DATENSCHUTZAKADEMIE, für alle Behörden im Land. So wurde die Dokumentation des ULD durch die Datenschutzbeauftragte und das Technikreferat an die überarbeitete, seit Anfang 2009 geltende Datenschutzverordnung (DSVO) angepasst (Tz. 6.2). Die Ergebnisse werden in einer geeigneten Form veröffentlicht.

Das ULD **profitiert** – ebenso wie jede andere Behörde – von seiner Datenschutzbeauftragten. Denn die oder der Datenschutzbeauftragte hinterfragt, berät, koordiniert, kontrolliert, ist manchmal unbequem, meistens aber konstruktiv und fordert Arbeiten ein, die ansonsten im Dienstgeschäft einfach untergehen. Ja, auch der Datenschutz braucht eine Datenschutzbeauftragte!

1.3 Unabhängiges Datenschutzzentrum Nord?

Der Koalitionsvertrag von CDU und Bündnis 90/Die Grünen von Hamburg enthält die Aussage, dass ein gemeinsamer Datenschutzbeauftragter von Hamburg und Schleswig-Holstein angestrebt werde. Daraus wird vorläufig nichts.

Die Kooperation der Freien und Hansestadt Hamburg und dem Land Schleswig-Holstein hat in einigen Bereichen schon dazu geführt, dass eine gemeinsame Einrichtung für bestimmte Verwaltungsaufgaben zuständig ist. Vor allem im **Datenverarbeitungs- und Medienbereich** wurden über Fusionen einheitliche Strukturen geschaffen: 2003 wurde ein Statistikamt Nord für beide Länder gegründet. 2004 ging Dataport als Zusammenschluss des Landesamtes für Informationstechnik Hamburg und der Datenzentrale Schleswig-Holstein an den Start. 2007 folgte die Medienanstalt Hamburg-Schleswig-Holstein.

So war es für das ULD nicht überraschend, als es 2004 vom Innenministerium Schleswig-Holstein über **Gespräche mit Hamburg** zu einer möglichen gemeinsamen Datenschutzbehörde informiert wurde. Vonseiten des ULD wurde hierzu Interesse und Offenheit signalisiert. Den Risiken, die mit einer Einrichtung an zwei Standorten verbunden sind, stehen Synergien bei der gemeinsamen Aufgabenerledigung gegenüber. Viele Formen der Datenverarbeitung erfolgen unbeeindruckt von Verwaltungsgrenzen. Die ersten Pläne verschwanden jedoch bald wieder in ministeriellen Schubladen.

Nach den **Bürgerschaftswahlen in Hamburg** im Februar 2008 vereinbarten die beiden Regierungspartner CDU und Bündnis 90/Die Grünen in ihrem Vertrag über die Zusammenarbeit, einen gemeinsamen Datenschutzbeauftragten mit Schleswig-Holstein anzustreben, der auch für die Informationsfreiheit zuständig sein solle. Diesen Bestrebungen widersetzte sich der damalige Hamburgische Datenschutzbeauftragte Wegen der nötigen Verantwortung gegenüber den jeweiligen Parlamenten sei eine gemeinsame Einrichtung verfassungsrechtlich bedenklich. Sie widerspräche der föderalen Struktur der Bundesrepublik. Außerdem käme als gemeinsamer Sitz nur Hamburg in Betracht. Diese schroffe Zurückweisung führte dazu, dass auch die Verantwortlichen in Schleswig-Holstein das erhitzte Eisen nicht anfassen wollten. Das Thema kühlte sang- und klanglos wieder ab.

Diese Entwicklung wurde vom ULD zur Kenntnis genommen. Zweifellos brächte eine derartige organisatorische Änderung einige Unruhe in beide Dienststellen. Doch nehmen die Überschneidungen der Tätigkeitsfelder immer mehr zu. Angesichts der massiven Dauerbelastung beider Stellen könnte durch eine Zusammenlegung mit der gemeinsamen Aufgabenerledigung wahrscheinlich eine gewisse Entlastung bewirkt werden. Letztlich kommt es bei der Fusion von solch sensiblen Organisationen auf zwei Bedingungen an: Es muss ein einheitliches hohes Niveau im Datenschutzrecht bestehen; eine Vereinheitlichung auf niedrigem Niveau wäre ein Bärendienst für den Grundrechtsschutz. Zudem müssen beide Behörden zur Zusammenarbeit auf Augenhöhe bereit sein. Die erste Voraussetzung wird mit dem Koalitionsvertrag Hamburgs ausdrücklich angestrebt. Die Kooperationsbereitschaft

muss wohl durch eine engere Zusammenarbeit der beiden Organisationen noch gefördert werden. In vielen Bereichen gibt es schon einen guten Austausch und eine **funktionierende Arbeitsteilung**.

Was ist zu tun?
Die Fusion der Datenschutzbehörden ist vorläufig aufgeschoben, muss aber nicht aufgehoben sein. Zunächst steht eine Intensivierung der Zusammenarbeit an. Über eine rechtliche Fusion wird erst wieder in einigen Jahren gesprochen werden können.

2 Datenschutzgesetzgebung auf Bundesebene

2.1 Defizit Arbeitnehmerdatenschutz

Die letzten Monate haben den von den Datenschutzbeauftragten seit Jahren angemeldeten Datenschutzbedarf auch für Nichtexperten offensichtlich werden lassen: Die bei der Telekom öffentlich gewordenen Datenschutzverstöße zeigten technisch-organisatorische und strukturelle Defizite. Die unzulässige **Beobachtung von Mitarbeitern** durch einen in der gesamten Republik agierenden Lebensmitteldiscounter offenbarte ein mangelndes datenschutzrechtliches Problembewusstsein und ungenügende Sanktionsfurcht (Tz. 5.3). Skandale kommen selten allein: In zeitlicher Nähe wurden aus dem Einzelhandel in unterschiedlichen Ländern weitere Datenschutzverstöße bekannt, die darauf hinwiesen, dass nicht nur für eine Unternehmensgruppe, sondern für große Teile einer Branche Datenschutz noch ein unbekanntes und unbeackertes Feld ist.

Das Fehlen eines sich direkt an Arbeitgeber adressierenden **Arbeitnehmerdatenschutzgesetzes** wurde offenbar. Die praktischen Probleme der rechtlichen Bewertung von klassischen Abläufen in Betrieben wurden schlaglichtartig erkennbar: Die weitverbreitete Videoüberwachung von Arbeitnehmern lässt sich über die Regelung im Bundesdatenschutzgesetz nur begrenzt legitimieren. Dabei wird die spezifische Abhängigkeit zum Arbeitgeber bisher völlig ignoriert. In vielen Unternehmen, teilweise selbst in internationalen Konzernverbünden, wird mit „Einwilligungen“ gearbeitet, bei denen es keine Freiwilligkeit gibt. Die Nutzung von Telekommunikations- und Telemediendiensten durch Arbeitnehmer zwingt Arbeitgeber zu einem komplexen Regelungsgeflecht, um sich einerseits nicht rechtswidrig zu verhalten, andererseits die eigenen Direktionsbefugnisse nicht aufzugeben. Heimliche und damit unzulässige Gesundheits- und Drogenkontrollen finden nicht nur in Einzelfällen statt. Der Rückgriff auf die arbeitsrechtliche Rechtsprechung sowie betriebliche Vereinbarungen können in vielen Bereichen die schlimmsten Persönlichkeitsbeeinträchtigungen im Arbeitsverhältnis abwenden. Rechtssicherheit für die Beteiligten – Arbeitgeber wie Arbeitnehmer – wird damit aber nicht geschaffen.

So offensichtlich der Bedarf an arbeitsspezifischen Datenschutzregelungen ist, so verblüffend ist, wie dieser **durch die Politik ignoriert** wird. Die Bundesregierungen hatten seit dem Volkszählungsurteil im Jahr 1983 über Jahre hinweg solche Regelungen versprochen. Einige Male bestand die konkrete Hoffnung, dass die vorliegenden Schubladenentwürfe des zuständigen Ministeriums das Licht eines Gesetzgebungsverfahrens erblicken würden. Doch im Ergebnis war die Lobbyarbeit der Arbeitgeber so effektiv, dass sich keine Regierung auf den absehbaren Konflikt einlassen wollte. Die aktuelle Regierungskoalition auf Bundesebene hat dieses Gesetzgebungsprojekt erstmals nicht mehr in ihren Absichtskatalog aufgenommen.

Die **Ablehnung durch die Arbeitgeber** stand derweil immer offensichtlicher im Widerspruch zu den eigenen objektiven Interessen an einem sozial verträglichen und zugleich effektiven IT-Einsatz in den Unternehmen. Mit den teilweise rigiden Vorgaben der Arbeitsrechtsprechung wird beim Einsatz neuer Technologien nicht hinreichend Rechtssicherheit geschaffen. Dass nun gleich eine Vielzahl von Verstößen keine ernsthaften politischen Aktivitäten auslöste, lässt sich nur mit schwerer Resignation und Hoffnungslosigkeit erklären, die alle Kräfte erfasst hat, die für einen Ausgleich von Arbeitgeber- und Arbeitnehmerinteressen beim betrieblichen IT-Einsatz eintreten. Rationale Gründe für eine weitere Untätigkeit gibt es nicht.

Die Datenschutzbeauftragten haben den Arbeitnehmerdatenschutz zum Thema des Europäischen Datenschutztages Ende Januar 2009 gewählt. Die Sommerakademie Ende August 2009 wird sich dem Thema „**Arbeitnehmer – Freiwild der Überwachung?**“ widmen. Vielleicht können wir damit Impulse setzen, die in der nächsten Legislaturperiode zu einer vernünftigen Regulierung führen.

2.2 Defizit Bundesdatenschutzgesetz

In zwei Bereichen hat das Bundeskabinett für das Bundesdatenschutzgesetz (BDSG) Vorschläge vorgelegt. Der erste befasst sich mit Kredit-Scoring und Auskunfteien, der zweite mit dem sogenannten Permission Marketing und dem Datenschutz-Audit.

Der Referentenentwurf zu **Scoring und Auskunfteien** vom September 2007 war zunächst systematisch wie inhaltlich ein Desaster. Es hat sich gelohnt, diesen Entwurf konstruktiv zu kritisieren. Im Juli 2008 wurde ein Regierungsentwurf beschlossen, der insgesamt eine brauchbare Antwort darauf enthält, wie bei der Erfassung von Kreditrisiken der Verbraucherschutz gewahrt werden kann. In der Finanzwirtschaft hatte sich allmählich eine intransparente Praxis der Verbraucherbenotung eingeschlichen. Spätestens seit 2006 ist nach der Veröffentlichung unseres Gutachtens zum Kredit-Scoring (28. TB, Tz. 8.8) nicht mehr zu bestreiten, dass diese Praxis Betroffenenrechte verletzt und weitgehend rechtswidrig ist.

Der Entwurf legalisiert den Einsatz der Scoring-Methode; der von der Wirtschaft hierfür zu bezahlende Preis ist eigentlich nur **erhöhte Transparenz**. Alle vorangegangenen Versuche, die Finanzdienstleister zu einer freiwilligen Selbstverpflichtung zu veranlassen, blieben erfolglos. Der vorliegende moderate Entwurf der Bundesregierung wird von den Wirtschaftsverbänden und den maßgebenden Unternehmen dennoch weiter heftig bekämpft. Es ist schon verblüffend, mit welcher Dreistigkeit diese Unternehmen einerseits den Verbraucher gläsern machen und sich andererseits weigern, sich hierbei in die Karten schauen zu lassen. Die Benotung der Menschen bezüglich ihrer Kreditwürdigkeit birgt ein gewaltiges Diskriminierungspotenzial und existenzielle Risiken für die Betroffenen bei zugleich fragwürdiger Aussagekraft. Öffentliche Kontrolle von Banken und etwas Selbstkritik stünde der Branche – gerade in der aktuellen Krisenzeit – gut zu Gesicht und brächte einen großen Gewinn für die informationelle Selbstbestimmung der Verbraucher (Tz. 5.1.1).

https://www.datenschutzzentrum.de/scoring/20080620-bdsg-e.html

Mit 17.000 über die Verbraucherzentrale Schleswig-Holstein vermittelten Datensätzen aus einem Callcenter wurde ein Kontodatenskandal öffentlich, der schließlich dem ULD aus unterschiedlichen Quellen über 7 Millionen illegal gehandelte Datensätze bescherte (Tz. 5.4 und Tz. 6.5). Dieses Mal konnte der Bundespolitik nicht der Vorwurf des Zögerns gemacht werden. Es wurde noch im Dezember 2008 ein Gesetzentwurf vorgelegt, der bei der Datennutzung für Werbezwecke die bisherige Widerspruchsregelung durch das Einwilligungserfordernis ersetzt. Dieses sogenannte **Permission Marketing** ist die adäquate Antwort darauf, dass der Austausch von Personendaten für Werbezwecke immer undurchsichtiger und invasiver und gleichzeitig die schutzwürdigen Verbraucherinteressen immer mehr ignoriert werden.

Sicher war und ist der Handel mit Kontodaten schon vor der Gesetzesnovelle illegal. Doch das, was inzwischen als legale Datennutzung für Werbezwecke praktiziert wird, missachtet derart die informationelle Selbstbestimmung der Menschen, dass die Novelle überfällig ist. Wieder überraschten die **Vehemenz des Widerstands** und die falschen Argumente großer Teile der Wirtschaft bei ihrer öffentlichen Lobbyarbeit gegen den Entwurf. Eine ganze Branche, die sich Dialogmarketing nennt, behauptet genau zu wissen, welche Werbung die Menschen wollen, und weigert sich, diese Betroffenen um Erlaubnis zu bitten bzw. mit diesen in den Dialog zu treten. Nach einer gesetzlich zugestandenen Übergangsphase werden die Unternehmen feststellen, dass die geplante Gesetzesänderung auch für sie von Vorteil ist. Diese trennt die schwarzen Schafe klar von den weißen im Gewerbe. Über den Dialog mit den Verbrauchern wird letztlich eine qualifiziertere Werbung möglich (Tz. 5.1.2).

www.datenschutzzentrum.de/wirtschaft/20081125-permission-marketing.html

Was bleibt, sind die vielen weiteren Defizite des BDSG. Als dieses Gesetz im Jahr 2001 wegen europarechtlicher Vorgaben überarbeitet wurde, waren sich alle Beteiligten über den vorläufigen Charakter des bisher Erreichten bewusst. Es war erklärter Wille des Bundesgesetzgebers, in einer zweiten Stufe eine **Modernisierung des Datenschutzrechtes** vorzunehmen: Anpassung an die technische Entwicklung, systematische Neuordnung und Erhöhung der Verständlichkeit, Einführung marktwirtschaftlicher Instrumente sowie Anerkennung des Datenschutzes als Verbraucherschutz. Passiert ist seitdem in dieser Hinsicht praktisch nichts. Inzwischen pfeifen es die Spatzen von den Dächern: Das BDSG wird den technischen Herausforderungen des Internets nicht mehr gerecht (30. TB, Tz. 2). Der Einsicht sollten endlich Taten folgen. Nur so kann die nötige Rechtssicherheit für alle Beteiligten geschaffen werden, die das Internet zum Rückgrat eines florierenden E-Commerce und eines vertrauenswürdigen E-Governments macht.

https://www.datenschutzzentrum.de/bdsg-novellierung/

Anlässlich der Entscheidung über die Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalen hat das Bundesverfassungsgericht im Februar 2008 aus dem allgemeinen Persönlichkeitsrecht ein „**Grundrecht auf Vertraulichkeit**

und Integrität informationstechnischer Systeme“ abgeleitet. Damit hat es nicht nur rechtliche, sondern auch technische Kompetenz demonstriert und gezeigt, dass es adäquate rechtliche Antworten auf die Verlagerung vieler vertrauensbedürftiger Lebensbereiche in die Welt der Informationstechnik gibt. Dieses Urteil sollte ein weiterer Anlass für den Bundesgesetzgeber sein, seine Hausaufgaben zu machen und der vom Bundesverfassungsgericht festgestellten Schutzpflicht für seine Bürgerinnen und Bürger gerecht zu werden. Dabei genügt es nicht, staatliche Eingriffe in diesen neu geschaffenen Grundrechtsbereich zu verhindern und im äußersten Notfall sauber gesetzlich geregelt zu erlauben (Tz. 4.2.2). Vielleicht wichtiger ist es noch, durch gesetzliche Regelungen die Menschen dazu rechtlich, technisch und strukturell in die Lage zu versetzen, sich der Invasion in diesen neu geschaffenen Schutzbereich, insbesondere durch private Angreifer, zu erwehren.

www.datenschutzzentrum.de/grundrecht/neues-grundrecht.pdf

2.3 Defizit Datenschutz-Audit

Seit 2001 verspricht eine Regelung im BDSG das Audit als **präventive marktwirtschaftliche Methode** zur Verbesserung des Datenschutzes. Seit 2001 werden vom ULD erfolgreich Datenschutz-Gütesiegel und Auditzertifikate verliehen. Seitdem steigt die Nachfrage nach diesen Instrumenten wie auch die positive Erfahrung hiermit. Nichts läge näher, die bisherige schleswig-holsteinische Praxis, die inzwischen europaweit anerkannt wird, in einen normativen Rahmen zu gießen und so die nötige Rechtssicherheit für IT-Anbieter, Daten verarbeitende Stellen, Verbraucher, Aufsichtsbehörden und die Öffentlichkeit zu schaffen.

Stattdessen legte zunächst das Bundesinnenministerium und dann die Bundesregierung einen Auditgesetzentwurf vor, der **an Praxisferne kaum zu überbieten** ist: ein bürokratisches und zugleich äußerst konfliktträchtiges Verfahren Einsetzung eines teilweise fachfremden, sich gegenseitig blockierenden Ausschusses, keine Transparenz über die durchgeführten Kontrollen und die eingesetzten datenschutzfreundlichen Techniken und Verfahren, keine Anreize für einen möglichst hohen Datenschutzstandard, keine unabhängige Qualitätskontrolle – letztendlich kein Anlass für Vertrauen und Marktvorteil. Die Anleihen hat man nicht im Technikrecht gesucht, etwa bei der Zertifizierung des Bundesamtes für die Sicherheit in der Informationstechnik (BSI), sondern, so tatsächlich die Kabinettsvorlage, beim „ökologischen Landbau“. Ein Billigsiegel liegt weder im Interesse der Verbraucher noch der Wirtschaft Das ULD hat dem federführenden Bundesinnenministerium immer wieder seine Unterstützung angeboten. Das Unterstützungsangebot besteht weiterhin (Tz. 9.1).

2.4 Internationale Regulierung als nationale Aufgabe

Die Verarbeitung unserer Daten erfolgt nicht nur in den engen Grenzen separierter informationstechnischer Systeme und auch nicht räumlich in den nationalen Grenzen, sondern global. Diesen globalen Charakter unserer IT-Struktur machen sich viele nutzbar, um sich der Verantwortung von verursachten Persönlichkeitsgefährdungen und -verletzungen zu entziehen (Tz. 7.4). Allgemein anerkannt ist, dass das Internet kein rechtsfreier Raum sein darf, aus dem heraus bzw. in dem ohne Verfolgungs- und Sanktionsrisiko Straftaten begangen werden können. Es wurde ein internationales Instrumentarium geschaffen, um „Cyber Crime“ zu bekämpfen. Verblüffend ist, dass von politischer Seite bisher keine ernsthaften Anstrengungen erkennbar sind, um ein verbindliches **internationales Regelwerk** zur Wahrung der Privatsphäre im Internet zu schaffen (Tz. 11).

Hindernis bei der Entwicklung eines solchen Regelwerkes sind die immer noch weit auseinandergehenden Vorstellungen von Datenschutz und von digitaler Privatsphäre in den **unterschiedlichen Kulturen** und das teilweise gänzliche Fehlen von Regelungen zum Datenschutz auf nationaler Ebene. Dies sollte die Vereinten Nationen nicht daran hindern, den Datenschutz global voranzubringen und internationale Empfehlungen zu erarbeiten, aus denen sich eine internationale Konvention entwickeln kann. Möglicherweise ist es sinnvoll, den Geltungsbereich von spezifischen Regelungen auf das Internet zu beschränken. Hierbei wird nicht zu verhindern sein, dass zunächst nur ein minimaler Schutzstandard vereinbart werden kann, was aber gegenüber dem bisherigen ungeregelten Zustand eine Verbesserung wäre. Die Bundesregierung sollte mit dieser Zielsetzung die Initiative ergreifen.

Zusätzlich zu den notwendigen globalen Bestrebungen für mehr Datenschutz sollten die höher technisierten Nationen mit einer vergleichbaren Datenschutzkultur weitergehende **multinationale Regelungen** ausarbeiten, bei denen nicht nur materielle Aspekte, sondern auch Verfahren und Standards festgelegt werden müssen, z. B. die Sicherung der Unabhängigkeit der Datenschutzkontrolle, die Verständigung auf eine einheitliche Sprache bei der Kommunikation oder die Festlegung von Verfahrensabläufen. Dabei muss eine eurozentristische Sicht vermieden werden, ohne dass hinter dem Datenschutzniveau Europas zurückgeblieben wird.

3 Telefonie im Landeshaus

Die Einführung einer neuen Telefonlösung im Haus des Landtages stellt sich dem ULD als gut geführtes Projekt dar, in dem Fragen des Datenschutzes und der Datensicherheit von Anfang an berücksichtigt werden.

Der Landtag beschloss, die technischen und organisatorischen Rahmenbedingungen für das Bereitstellen von Apparaten und den Betrieb einer Telefonanlage neu zu ordnen. Das ULD war von der Landtagsverwaltung bereits in der Planungsphase beratend hinzugezogen worden. Die wesentlichen Merkmale einer datenschutzfreundlichen Lösung wurden frühzeitig festgelegt und flossen in die **Ausschreibungsanforderung** ein. Danach müssen sämtliche administrativen Tätigkeiten an der Anlage revisionssicher protokolliert werden. Als weitere Sicherheitsmerkmale wurden z. B. die Grundzüge der Firewallarchitektur festgelegt. Auf sicherheitskritische Sonderfunktionen und Leistungsmerkmale wurde bewusst verzichtet. Die Administration erfolgt durch den Landtag selbst, sodass ein direkter Zugriff auf das System besteht und schwer kontrollierbare Mängel bei Dienstleistern keine negativen Auswirkungen auf Funktionalität und Datenschutz haben können. Die vorausschauende Projektplanung machte bei der Umsetzung lediglich in Einzelpunkten Korrekturen notwendig, sodass einem erfolgreichen Start der neuen Telefonielösung nichts im Wege stand.

Besonders datenschutzfreundlich ist die **Verarbeitung der Gebührendaten**. Diese findet nämlich gar nicht statt. Der Landtag hat mit dem Telekommunikationsanbieter eine „Flatrate“ vereinbart. Eine Erhebung der Gebührendaten wie die Telefonnummern der anrufenden und gerufenen Teilnehmer kann entfallen – aus Sicht des ULD eine mustergültige, weil datensparsame Lösung.

Das ULD hat die Landtagsverwaltung bei der Erstellung der für eine ordnungsgemäße Datenverarbeitung notwendigen Dokumentation beraten und sowohl die Herstellerdokumentation als auch IT- und **Sicherheitskonzept des Landtages** geprüft. Das für den Datenschutz im Landtag zuständige Datenschutzgremium wurde intensiv mit einbezogen.

Was ist zu tun?
Eine gute Projektorganisation ist die Voraussetzung für einen datenschutzfreundlichen Betrieb. In Zukunft müssen die getroffenen technischen und organisatorischen Maßnahmen regelmäßig überprüft werden. Zwischen dem ULD und der Landtagsverwaltung wurde hierzu eine regelmäßige Beratung vereinbart.

4 Datenschutz in der Verwaltung

4.1 Allgemeine Verwaltung

4.1.1 Bundesmeldegesetzentwurf – Ein Rückschritt für Schleswig-Holstein?

Die Aussichten für die Verabschiedung eines Bundesmeldegesetzes noch in dieser Legislaturperiode stehen schlecht. Hauptstreitpunkt ist die Frage der Notwendigkeit eines zentralen Bundesmelderegisters. Daneben sind eine Reihe von Detailregelungen fragwürdig, die aktuell in unserem Landesmeldegesetz praxisorientiert gelöst sind.

Im Rahmen der Föderalismusreform ist das Melderecht in die ausschließliche Gesetzgebungskompetenz des Bundes übergegangen. Mit dem vom Bundesinnenministerium Ende 2007 erarbeiteten Referentenentwurf war neben der notwendigen Vereinheitlichung des Melderechts die Einführung eines bundesweiten elektronischen Abrufs von Meldedaten für öffentliche wie auch private Stellen geplant. Umstritten ist, ob dafür ein neues zentrales **Bundesmelderegister** benötigt wird und wie es gegebenenfalls organisiert sein muss, insbesondere, wer die Verantwortung für die darin enthaltenen Daten trägt. Da eine Einigung über den Entwurf nicht in Sicht ist, rechnen wir nicht damit, dass der Gesetzentwurf noch in dieser Legislaturperiode verabschiedet wird.

Die Notwendigkeit bundesweiter elektronischer Abrufe von Meldedaten wird von uns nicht infrage gestellt. Allerdings sollte der Aufwand dafür so gering wie möglich gehalten werden. Fehlerquellen, wie sie sich bei der Einführung der Steueridentitätsnummerndatei gezeigt haben, sollen gar nicht erst entstehen können. Unter dem Gesichtspunkt der Datensparsamkeit muss die Frage erlaubt sein, weshalb schleswig-holsteinische Meldedaten zusätzlich in einem bundeseigenen Register gespeichert werden sollen, die bereits in einer landesweiten Spiegeldatenbank der Kommunen für jedermann zum Abruf zur Verfügung stehen. Heutzutage kommt es nicht mehr darauf an, bei welchen Stellen Daten vorgehalten werden, sondern ob die Daten ausreichend **elektronisch erschlossen** und vernetzt und wie sie dort geschützt sind.

Der Umstand, dass nicht alle Bundesländer über eine entsprechende Spiegeldatenbank verfügen, spricht nicht zwangsläufig für ein zentrales Bundesmelderegister. In diesen Ländern sind vielfach bereits **dezentrale Lösungen** im Einsatz, die in gleicher Weise wie die landesweiten Spiegeldatenbanken Meldedaten elektronisch zum Abruf bereithalten. Zur Erleichterung des bundesweiten Abrufs müssten diese Rechner nur miteinander vernetzt werden. Dies kann auch über eine zentrale Stelle geschehen.

Als Alternative zu einer dezentralen elektronischen Lösung kann der Bund Kommunen ohne elektronisches Auskunftsregister die notwendige technische Infrastruktur in Form einer Spiegeldatenbank zur Verfügung stellen, in der die Meldedaten **auftragsweise** vorgehalten werden. So wäre ein bundesweiter Online-Abruf von Meldedaten für alle Meldebehörden zu realisieren, ohne dass die Daten

doppelt in einem neu aufzubauenden Bundesmelderegister gespeichert werden müssten.

Der Entwurf eines Bundesmeldegesetzes enthält eine Vielzahl weiterer Regelungen, die aus Sicht der Länderinnenminister wie auch der Datenschutzbeauftragten noch diskussionsbedürftig sind. Im Rahmen der Stellungnahme des Landes Schleswig-Holstein zum Entwurf hat allein das hiesige Innenministerium in Abstimmung mit uns weit mehr als **30 Änderungsvorschläge** an das Bundesinnenministerium adressiert.

Was ist zu tun?
Bei Neuregelung des Melderechts sind redundante Datenspeicherungen zu vermeiden. Der Bund muss die in den Ländern vorhandene technische Infrastruktur einbeziehen. Kritik und Vorschläge aus den Ländern mit ihrer langen praktischen Erfahrung im Melderecht sollten aufgegriffen werden.

4.1.2. Online-Melderegisterauskunft wird zum Erfolgsmodell

Der Online-Abruf von Meldedaten ging 2008 endlich in den Echtbetrieb. Zumindest in den wesentlichen Punkten konnte in Mustertest- und Freigabeverfahren die Rechtmäßigkeit festgestellt werden. Es bleibt erheblicher funktionaler Verbesserungsbedarf.

Beim Online-Abruf von Meldedaten muss zwischen dem Abruf durch Behörden und dem durch private Stellen in Form einfacher Melderegisterauskünfte unterschieden werden. Für die sogenannte **Behördenauskunft** können sich bundesweit alle öffentlichen Stellen nach sorgfältiger Authentifizierung bei Dataport freischalten lassen. Zusätzlich soll bei Abfragen die für das Verfahren notwendige feste IP-Adresse der Auskunft suchenden Stelle abgeprüft werden. Erfolgte Datenübermittlungen werden im Volltext protokolliert. Dies ermöglicht endlich die Beachtung der im Melderecht vorgesehenen Nachberichtspflicht. Die anfragende Stelle wird dabei per Mail automatisch unterrichtet, wenn sich Meldedaten nach der Auskunftserteilung nachträglich ändern, z. B. weil ein Bürger seinen Umzug erst verspätet angezeigt hat.

Online-**Datenabrufe durch private Stellen** haben sich bisher noch nicht am Markt durchgesetzt. Die Ursachen dafür liegen auf der Hand:

- Anfragen können nur manuell durch Eingabe am Bildschirm gestellt werden. Dies bedeutet bei Massenanfragen einen hohen Aufwand sowie eine hohe Fehlerquote durch das manuelle Übertragen der Daten. Für Großkunden kann bei Etablierung hinreichender Sicherheitsvorkehrungen die Möglichkeit geschaffen werden, Anfragen durch Übermittlung elektronischer Dateien zu stellen. Für den elektronischen Datenaustausch sollte eine Schnittstelle im XMeld-Format angestrebt werden.
- Wird über das Portal eine Anfrage gestellt, muss zuerst die Meldebehörde ausgewählt werden, in deren Datenbestand gesucht werden soll. Viele Meldebehörden sind für mehrere Gemeinden zuständig. Für anfragende Stellen ist es

sehr schwierig, aus dem bekannten Wohnort auf die zuständige Meldebehörde zu schließen. Es fehlt bisher ein Gemeinde- bzw. Postleitzahlenverzeichnis, das eine Zuordnung zu der jeweilig zuständigen Meldebehörde ermöglicht.

- Weichen Suchdaten von den im Register gespeicherten Daten ab, muss eine Negativauskunft erteilt werden. Dies gilt selbst bei Fehlern in der Schreibweise des Straßennamens. Hier könnte für jede Kommune ein Straßenverzeichnis hinterlegt und als Auswahlmenü angeboten werden. Im Rahmen einer Plausibilitätsprüfung könnten anfragende Stellen auf Fehler aufmerksam gemacht werden.
- Jede Anfrage wird einzeln abgerechnet und per Lastschriftverfahren eingezogen. Dies ist für Großkunden nicht akzeptabel, da jede Zahlung einzeln in deren Buchführung übernommen werden muss. Eine Monatsabrechnung mit entsprechendem Leistungsnachweis wäre wohl die Lösung.

Die **Städte Reinbek und Norderstedt** haben bei der Einführung der dargestellten Abrufverfahren eine Vorreiterrolle übernommen und jeweils ein Mustertest- und Freigabeverfahren durchgeführt. Gemeinsam mit dem Innenministerium haben wir diese Verfahren begleitet. Die entstandenen Unterlagen können von anderen Kommunen angefordert werden. Sie sind geeignet, auch für Test- und Freigabeverfahren anderer Module eine systematische Hilfestellung zu geben.

Die Bereitstellung ihrer Meldedaten für den Online-Abruf ist für jede Meldebehörde freiwillig. Bis zum Redaktionsschluss haben sich etwa 85 % der Meldebehörden im Land beteiligt. Eine Teilnahme zumindest am Behördenauskunftsverfahren kann **vom ULD dringend empfohlen** werden, nicht nur wegen der möglichen Einspareffekte, sondern weil im automatisierten Verfahren eine bessere Qualität der Datenverarbeitung erreicht werden kann: Übertragungsfehler können reduziert werden; die notwendige Vollprotokollierung erteilter Auskünfte dürfte nur so zu gewährleisten sein; schließlich ist wohl nur das automatisierte Verfahren in der Lage, die gesetzlich vorgeschriebene Nachberichtspflicht gegenüber den anfragenden Stellen zu erfüllen.

Was ist zu tun?
Dataport sollte als Auftragnehmer der Kommunen die technischen Nachbesserungen am Verfahren umgehend realisieren. Mit der Freischaltung zumindest für die Behördenauskunft lassen sich Mehrwerte bei Wirtschaftlichkeit und Datenschutz erzielen.

4.1.3 Schranken bei Melderegisterauskünften an gewerbliche Adressvermittler

Privater Adressdatenhandel hat sich zu einem lukrativen Markt entwickelt. Einer schrankenlosen Einbeziehung von Meldedaten steht allerdings das Melderecht entgegen. Auf unsere Anregung hat das Innenministerium den Meldebehörden empfohlen, keine Melderegisterauskünfte mehr an Adressvermittler zu erteilen, wenn diese die Meldedaten nicht nur an ihre Auftraggeber weitergeben, sondern zusätzlich für eigene Zwecke speichern.

Ein Bürger eröffnet bei einer Bank ein Konto. Diese möchte die angegebene **Anschrift verifizieren**. Sie beauftragt deshalb einen gewerblichen Adressvermittler mit der Einholung einer einfachen Melderegisterauskunft. Der Adressvermittler leitet die Auskunft der Meldebehörde nicht nur an die Bank weiter, sondern speichert die Angaben zusätzlich in einer eigenen Datenbank, verbunden mit dem Qualitätsmerkmal „melderegistergeprüft".

Bei späteren Anfragen zur gleichen Person beantwortet der Adressvermittler die Anfragen aus seinem eigenen Register wie eine Meldebehörde (sogenanntes **Adress-Pooling**), allerdings ohne dabei an die qualitativen Anforderungen des Melderechts gebunden zu sein. Selbst Listenauskünfte oder ein Weiterverkauf von Daten zu Werbezwecken wären nicht ausgeschlossen. Bei dem Bankkunden füllt sich z. B. plötzlich der Briefkasten mit Werbemüll, ohne dass er die Ursache dafür erkennen kann. Die Dimension wird deutlich, wenn man sich die Anzahl der Melderegisterauskünfte an gewerbliche Adressvermittler und deren Bestände an Datensätzen, zum Teil im zweistelligen Millionenbereich, ansieht. In der öffentlichen Berichterstattung wird schon von Schattenmelderegistern gesprochen.

Wir haben uns des Problems gemeinsam mit dem Innenministerium angenommen. Die Prüfung ob eine über das konkret bestehende Auftragsverhältnis hinausgehende Nutzung von Meldedaten durch Adressvermittler zur Unzulässigkeit der Melderegisterauskunft führt, ergab Folgendes: Das Melderecht enthält zwar keine besondere Zweckbindung für die Daten beim Empfänger nach der Erteilung von Melderegisterauskünften. Gleichwohl handelt es sich beim Melderegister um **kein öffentliches Register**, welches für jedermann beliebig verfügbar ist. So sind z. B. Listenauskünfte über eine Vielzahl von Personen unzulässig, soweit sie nicht zweifelsfrei im öffentlichen Interesse stehen. Auf diese Weise soll eine massenhafte Verwendung von Meldedaten, etwa zu Werbezwecken, verhindert werden.

Das Melderecht hat einfache Meldeauskünfte bewusst als Ermessensentscheidung ausgestaltet. Eine Prüfung schutzwürdiger Interessen Betroffener ist für jede einzelne Auskunft ausdrücklich vorgeschrieben. Dabei ist zu prüfen, ob im Rahmen der Auskunftserteilung das **staatliche Monopol über die Meldedaten** zum Schutz der Persönlichkeitsrechte der Betroffenen aufrechterhalten bleibt und ob die gesetzlichen Zugangsvoraussetzungen zu den Daten beim Empfänger nicht unterlaufen werden.

Eine Zugangsvoraussetzung ist, dass der Antragsteller die gesuchte Person durch Angabe von Vor- und Familiennamen, Geburtsdatum sowie der zuständigen Meldebehörde oder durch eine alte Anschrift **eindeutig identifizieren** kann und eine Gebühr entrichtet. Allein die Notwendigkeit zur eindeutigen Identifikation setzt im Grunde voraus, dass ein Kontakt zwischen Auskunftsuchendem und Betroffenem besteht, was als Indiz für ein berechtigtes Interesse des Auskunftsuchenden an der Auskunft gewertet werden kann. Adressvermittler könnten ohne die Identifikationsdaten der Auftraggeber gar keine Meldedaten einholen. Die zu entrichtende Gebühr ist ein weiteres Zugangshemmnis.

Für die **Schutzbedürftigkeit der Meldedaten** spricht auch die mit der Einführung der Online-Melderegisterauskunft etablierte Pflicht zur Verschlüsselung sowie das ausdrücklich gesetzlich geregelte Widerspruchsrecht für Betroffene gegen die Auskunftserteilung über das Internet. Wäre das Melderegister vom Gesetzgeber als öffentliches Register – vergleichbar dem Telefonbuch – gewollt, wären solche Schutzmaßnahmen schlicht überflüssig. Eine weitere Qualitätsverschiebung erfolgt bei Listenauskünften z. B. für Werbezwecke. Diese sind im Melderecht eindeutig nicht gewollt, können aber bei einer Datenspeicherung durch Adressvermittler nicht verhindert werden. Ein Widerspruch Betroffener gegen die Datenübermittlung über das Internet würde bei Adressvermittlern keine Wirkung entfalten.

Für Adressvermittler steht naturgemäß die Erteilung möglichst vieler Auskünfte im Vordergrund. Unzulängliche Identitätsprüfungen begründen die **Gefahr von Falschauskünften**, die z. B. bei der zwangsweisen Einziehung von Forderungen bei namensgleichen unbescholtenen Dritten zu erheblichen Nachteilen und Belastungen für diese führen können. Ähnliches gilt bezüglich der fehlenden Aktualität der bei den Adressvermittlern gespeicherten Daten.

Eine Melderegisterauskunft darf nur erteilt werden, soweit die **schutzwürdigen Betroffeneninteressen** nicht beeinträchtigt werden. Eine solche Beeinträchtigung ist bei der Auskunftserteilung an Adressvermittler, die Meldedaten zusätzlich für eigene Zwecke speichern, gegeben. Entsprechende Auskunftsanträge sind folglich abzulehnen, wenn der Adressvermittler nicht die Gewähr dafür bietet, dass kein Adress-Pooling stattfindet.

Was ist zu tun?
Bei der Tätigkeit der Adressvermittler ist zu beobachten, ob sie ihre Zusagen zur Verwendung der Meldedaten einhalten. Sollten die getroffenen Regelungen zum Schutz der Betroffenen nicht genügen, müsste über klärende gesetzliche Regelungen nachgedacht werden.

4.1.4 Übermittlung von gesperrten Meldedaten zu Wahlwerbezwecken

Die automatisierte Verarbeitung von Meldedaten wurde in den letzten Jahren immer komplexer. Test und Freigabe neuer Module und Softwareversionen sowie eine ausreichende Schulung der Mitarbeiter wurden dabei häufig vernachlässigt. So wurden bei einer kreisfreien Stadt Meldedaten von Personen zu Wahlwerbezwecken an eine politische Partei übermittelt, die einer solchen Datenübermittlung ausdrücklich widersprochen hatten bzw. für die eine Auskunftssperre eingetragen war.

Bürgerinnen und Bürger hatten Wahlwerbebriefe einer politischen Partei erhalten, obwohl sie zuvor gerade gegenüber der Meldebehörde der Datenübermittlung für Wahlwerbezwecke widersprochen hatten. Es erwies sich, dass von der Stadt eine sogenannte „**Erstwählerliste**“ erstellt worden war, wobei der Mitarbeiter sich – leider – darauf verließ, dass das Auswerteprogramm im Rahmen der Plausibilitätsprüfung sämtliche Widersprüche und Auskunftssperren herausfiltern würde.

Der genaue Umfang der fehlerhaften Datenübermittlungen konnte im Nachhinein nicht mehr festgestellt werden, da auch die vorgeschriebene Protokollierung der Datenübermittlungen weder im automatisierten Verfahren, noch durch Kopie der übermittelten Listen erfolgt war. Es ist davon auszugehen, dass es sich nicht nur um Einzelfälle handelte.

Die Ursachen für die rechtswidrigen Datenübermittlungen waren schnell gefunden. Das eingesetzte Auswerteprogramm hätte so gestaltet sein müssen, dass **Widerspruchs- und Auskunftssperrefälle** nur in eine Auswertung einfließen, wenn dies durch einen entsprechenden Eingabebefehl ausdrücklich ausgewählt wird. Tatsächlich mussten die fraglichen Daten im vorliegenden Fall durch besonderen Befehl herausgenommen werden, was versäumt wurde. Die notwendige Änderung wurde mittlerweile bei Dataport in Auftrag gegeben; bei einem rechtzeitigen Test und Freigabeverfahren für das Auswerteprogramm hätte der Fehler leicht erkannt und beseitigt werden können. Dies gilt auch für die unzureichende Protokollierung von Auswertungen, die zumindest helfen kann, entstandene Schäden zu erkennen und so weit wie möglich zu begrenzen.

Monieren mussten wir zudem die nicht ausreichende **Schulung der Mitarbeiter**. Bei sachgerechter Anwendung hätte das Auswerteprogramm durchaus richtige Ergebnisse liefern können. Die fehlende automatisierte Protokollierung hätte durch Fotokopien oder einen Zweitausdruck der Liste ersetzt werden können. Spekulative Hoffnungen, die EDV werde die Auswertung schon korrekt vornehmen, erweisen sich immer wieder als unbegründet. Sind Mängel bei Test, Freigabe und Schulung in der Anwendung der Melderechtssoftware bekannt, so muss zumindest das erzeugte Ergebnis sorgfältig geprüft werden, bevor die Meldedaten an Dritte herausgegeben werden. Uns blieb die undankbare Aufgabe, die unzulässigen Datenübermittlungen zu beanstanden, verbunden mit der Erwartung, dass die Stadt nicht nur für den konkreten Fall, sondern generell für das automatisierte Meldeverfahren ihre Lehren zieht.

Was ist zu tun?
Im Berichtszeitraum wurde die automatisierte Datenverarbeitung der Meldebehörden massiv ausgeweitet. Die Behörden müssen dieser Ausweitung durch verstärkten Personaleinsatz für Test und Freigabe der Software sowie Schulungen Rechnung tragen. Die Meldeämter stehen auch in der Verantwortung für die Effekte ihrer automatisierten Datenverarbeitung.

4.1.5 Spendenaufruf der Feuerwehr – aber bitte nicht mit Meldedaten

Die Verwendung von Meldedaten zu Werbezwecken ist nach dem Melderecht unzulässig. Dies gilt auch für öffentliche Stellen, selbst wenn die Werbung einer „guten Sache“ dient. Die Weitergabe von Meldedaten an die örtliche Feuerwehr zur Versendung eines Spendenaufrufs für ein Kameradschaftsfest war rechtswidrig.

Eine Stadt war der Auffassung, sie könne zur Durchführung eines Spendenaufrufs eine sogenannte Gruppenauskunft aus dem Melderegister an die Feuerwehr ertei-

len. Das dafür erforderliche öffentliche Interesse sah sie darin, dass mit den Spendengeldern die geleistete Arbeit der Feuerwehr im abgelaufenen Einsatzjahr gegenüber den Bürgern dargestellt werde. Nach dem Brandschutzgesetz sind freiwillige Feuerwehren **öffentliche Feuerwehren** und damit gemeindliche Einrichtungen ohne eigene Rechtspersönlichkeit. Die Datenverarbeitung war folglich unmittelbar der Stadt als Behörde zuzurechnen.

Eine Gruppenauskunft, wie von der Stadt geltend gemacht, kam nicht in Betracht, da diese nur an private Stellen gesetzlich vorgesehen ist. Zudem wäre das dafür notwendige **öffentliche Interesse** nicht vorhanden gewesen. Ein Kameradschaftsabend der Feuerwehr liegt im Interesse der Teilnehmer, nicht aber in dem der Allgemeinheit. Dass die geleistete Arbeit der Feuerwehr im abgelaufenen Einsatzjahr dargestellt werden sollte, war jedenfalls dem Spendenaufruf nicht zu entnehmen.

Die stadtinterne Weitergabe von Meldedaten ist nur zulässig, wenn die Daten zur Aufgabenerfüllung des Empfängers erforderlich sind. Die **Aufgaben und Befugnisse der Feuerwehr** sind im Brandschutzgesetz geregelt. Dort ist nichts über die Durchführung von Kameradschaftsabenden zu lesen. Nach unserer Beanstandung hat die Stadt – nach erneuter Überprüfung – zugesagt, künftig keine Meldedaten mehr für solche Zwecke zu verwenden. Außerdem hat sie für eine unverzügliche Löschung der weitergegebenen Daten Sorge getragen.

Was ist zu tun?
Meldebehörden sollten bei Listenauskünften auch im öffentlichen Bereich sorgfältig den Zweck der Datenverarbeitung beim Empfänger hinterfragen. Die anfragende Stelle muss darlegen, inwieweit sie die Daten für ihre rechtmäßige Aufgabenerfüllung benötigt.

4.1.6 Der neue „elektronische“ Personalausweis

Ab November 2010 soll der Personalausweis nicht nur mit elektronisch gespeichertem Lichtbild und – auf freiwilliger Grundlage – mit elektronisch gespeicherten Fingerabdrücken auf dem Funkchip ausgestattet werden; er soll auf Wunsch auch als elektronischer Identitätsnachweis in der Online-Welt dienen.

Sowohl der elektronische Identitätsnachweis als auch die optionale elektronische Signatur könnten endlich bestehende Probleme bei Rechtsgeschäften über das Internet lösen. Beide technische Verfahren dienen dazu, mithilfe kryptografischer Methoden Nachweise über Identitätsattribute des Personalausweisinhabers bei der

Kommunikation über heutige Netze zu erbringen. Allerdings müssen beide Verfahren so gestaltet werden, dass sie für Bürger **transparent und leicht zu handhaben** sind und diese auf die ordnungsgemäße und sichere Verwaltung der dafür notwendigen Daten vertrauen können.

Der elektronische Personalausweis soll so funktionieren, dass unter Kontrolle des Nutzers nur bestimmte Daten offenbart werden, z. B. das Alter. Besonders interessant ist, dass verschiedene Anbieter, die sich einen solchen Nachweis zeigen lassen, diese Daten nicht zusammenführen können, da **im Sinne eines nutzergesteuerten Identitätsmanagements** (Tz. 8.3) jeweils verschiedene Identifikatoren verwendet werden. Wir werden uns mit der genauen Ausgestaltung der Systeme weiter beschäftigen, damit nicht ähnliche Probleme entstehen wie bei der Einführung des ePasses (30. TB, Tz. 4.1.3). Man muss sich bewusst machen, dass der elektronische Personalausweis Bestandteil eines umfassenderen IT-Systems ist, bei dem – wie bei allen IT-Systemen – regelmäßig das Niveau der Sicherheit neu zu bewerten ist. Hier stellt sich die Frage, wie man mit festgestellten Sicherheitsrisiken umgehen soll, die während der 10-jährigen Gültigkeit der Ausweise bekannt werden.

Mit dem neuen Personalausweisrecht soll die Möglichkeit geschaffen werden, die Signatur als zusätzliches Datum auf dem Ausweis zu speichern. Bisher nicht beabsichtigt ist jedoch, den Bürgerinnen und Bürgern über die übliche Beratung durch die Personalausweisbehörden hinaus Unterstützung zukommen zu lassen. Sie müssen sich also selbst bei einem elektronischen Signaturanbieter um die **Vergabe einer Signatur** bemühen. Dieses Vorgehen war bei den schon vorhandenen Vergabemodellen bisher wenig erfolgreich, wie sich aus der Anzahl der vergebenen Signaturen unschwer ablesen lässt.

Personalausweise sind eine staatliche Infrastrukturleistung zur eindeutigen Identifizierung der Bürger, künftig auch im Bereich der automatisierten Datenverarbeitung. Es wäre deshalb durchaus eine Alternative, die Ausgabe der Signatur den Personalausweisbehörden selbst als eigene Aufgabe zu übertragen, so wie dies auch beim elektronischen Identitätsnachweis vorgesehen ist. Das **Vertrauen der Bürger** in die ordnungsgemäße Handhabung der Signatur würde mit der Ausgabe durch die hoheitliche Verwaltung jedenfalls deutlich gestärkt. Zudem würde der zusätzliche Verwaltungsaufwand für die separate Beantragung entfallen.

Welche **Alternativen** gibt es? Die Bürger sollten bei der Beantragung der Signatur nicht allein gelassen werden, z. B. durch die Möglichkeit, gemeinsam mit der Ausstellung des Personalausweises auch die Signatur zu beantragen. Die Personalausweisbehörden könnten auftragsweise und gegen Gebühr als Vermittler tätig werden. Sollte beispielsweise die Bundesdruckerei auch weiterhin für die Vergabe von Signaturen zur Verfügung stehen, wäre sogar eine Kooperation möglich, bei der im Rahmen der Herstellung der Personalausweise bereits die Signatur zusätzlich mit abgespeichert wird. Die Möglichkeit einer separaten Beantragung der Signatur würde damit nicht zwingend beeinträchtigt.

Unabhängig von der letztlich gewählten Verfahrensvariante kommt auf die Personalausweisbehörden eine erhebliche **Beratungsaufgabe** zu. Die meisten Bürger

werden nicht nur Fragen zum konkreten Verfahren haben, sondern sich zusätzlich über Möglichkeiten, Vorteile und Risiken der Signatur informieren wollen. Dies gilt auch für den vorgesehenen elektronischen Identitätsnachweis und für **etwaige Sicherheitsrisiken** bei Verwendung des Ausweises. Insoweit entsteht zunächst ein erheblicher Schulungsbedarf für die Mitarbeiterinnen und Mitarbeiter in den Personalausweisbehörden. Es ist nicht zu übersehen, dass mit den neuen Aufgaben auch das Anforderungsprofil der Beschäftigten einem erheblichen Wandel unterliegt.

Darüber hinaus müssen geeignete technische und organisatorische Sicherheitsmaßnahmen bei der Verarbeitung von Anträgen auf Erteilung des elektronischen Personalausweises beachtet werden. Für den ePass hat das Bundesministerium des Innern (BMI) erst im Jahr 2008 hierzu Handreichungen für Meldebehörden herausgegeben. Beim elektronischen Personalausweis sollte die Datensicherheit bereits 2009 im Pilotbetrieb in den Meldebehörden berücksichtigt werden.

Was ist zu tun?
Bei der Ausgestaltung des Verfahrens für die Beantragung eines neuen Personalausweises sollte die Vergabe der elektronischen Signatur mit einbezogen werden, um den Aufwand für den Bürger und damit eine wichtige Hemmschwelle so niedrig wie möglich zu halten. Die Kommunen müssen im Hinblick auf ihre Beratungspflicht rechtzeitig den Schulungsaufwand für die Mitarbeiter einplanen.

4.1.7 Praxis kommunaler Bürgerbüros

Bürgerbüros haben mittlerweile eine große Verbreitung in Städten und Gemeinden Schleswig-Holsteins gefunden. Der Datenschutz wird nicht immer optimal beachtet. Mindeststandards müssen jedoch in jedem Fall eingehalten werden.

Die Rechtslage ist eindeutig. Durch **technische und organisatorische Maßnahmen** ist sicherzustellen, dass Besuchern eines Bürgerbüros personenbezogene Daten Dritter nicht zur Kenntnis gelangen können. Die Maßnahmen sind zu treffen, die nach dem Stand der Technik und der Schutzbedürftigkeit der Daten erforderlich und angemessen sind. In der Praxis haben sich drei Problembereiche herauskristallisiert:

- der Wartebereich,
- der Bearbeitungsbereich und
- bei größeren Bürgerbüros der Anmeldebereich.

Im **Wartebereich** sind Besucher, wenn sie sich nicht unterhalten, oft gelangweilt. Sie achten sogar besonders darauf, ob und gegebenenfalls wann ein Beratungsgespräch beim Sachbearbeiter beendet wird, um den Anschluss nicht zu verpassen. Deshalb muss der Wartebereich deutlich von dem eigentlichen Beratungsbereich abgetrennt werden. Eine auf den Wartebereich ausgerichtete musikalische Unter-

malung, z. B. das Abspielen eines Radiosenders, kann helfen, die Gefahr der Kenntnisnahme von Beratungsgesprächen zu reduzieren.

Im **Bearbeitungsbereich** kann meist eine zufällige Kenntnisnahme einzelner Worte Dritter nicht ausgeschlossen werden. Dies mag bei Daten mit geringerer Sensibilität hingenommen werden, soweit den Dritten keine Kenntnisnahme zusammenhängender Sachverhalte ermöglicht wird. Zwischen den Bearbeiterplätzen sollte deshalb ein möglichst großer Abstand gewählt werden. Als zusätzliche Abschottung können mobile Trennwände oder Blumenkübel aufgestellt werden. Die Besucher sollten während der Beratung keinen Blickkontakt untereinander haben. Für die Bearbeitung besonders sensibler Fälle muss ein gesonderter Raum zur Verfügung stehen.

Im **Anmeldebereich** werden die Bürger häufig bereits nach Namen und Anliegen befragt. Dies kann für die Verteilung auf bestimmte Bearbeitungsplätze geboten sein. Allerdings sollte eine solche Datenerhebung nur auf freiwilliger Grundlage vorgenommen werden. Am Empfangstresen sind Markierungen für Abstandsflächen anzubringen; die Löschung der Daten sollte spätestens nach Verlassen des Bürgerbüros erfolgen.

Bei jedem Bürgerbüro sollte nach Neueinrichtung oder nach wesentlichen Änderungen ein Test- und Freigabeverfahren durchgeführt werden, bei dem mit gesundem Menschenverstand vor Ort geprüft wird, ob bzw. in welchem Umfang ein Mithören oder eine sonstige Kenntnisnahme von Daten Dritter möglich ist. Diese Prüfung ist aktenkundig zu machen. Anschließend ist die Beseitigung festgestellter Mängel zu überwachen.

Was ist zu tun?
Bei der Einrichtung von Bürgerbüros muss für Kommunen eine datenschutzrechtliche Überprüfung gemäß den vorgenannten Hinweisen zum Standard gehören. Hat bei bereits eingerichteten Bürgerbüros noch keine Prüfung stattgefunden, sollte diese unverzüglich nachgeholt werden.

4.1.8 Neues Landesbeamtengesetz in Vorbereitung

Der Entwurf zur Neufassung des Landesbeamtengesetzes enthält eine umfassende Novellierung des für Schleswig-Holstein geltenden Beamtenrechts. Unser besonderes Augenmerk gilt den Vorschriften zum Personalaktenrecht. Bis auf die Zweckbestimmung bei Aufsichts- oder Revisionsaufgaben konnte im Rahmen der Ressortabstimmung in allen wesentlichen Punkten Einvernehmen mit dem ULD erzielt werden.

Nach der Föderalismusreform war die grundlegende Novellierung des Landesbeamtenrechts nötig. Dem dient der Entwurf eines Beamtenrechtsneuregelungsgesetzes. Aus datenschutzrechtlicher Sicht ist das Verfahren bei amtsärztlichen Untersuchungen sowie das sogenannte Personalaktenrecht besonders von Interesse. In guter und konstruktiver Zusammenarbeit mit dem Innenministerium konnte

eine Reihe von Verbesserungen im Verhältnis zur bisherigen Rechtslage erreicht werden. Die Änderungen bringen eine deutliche Entbürokratisierung und **Vereinfachung bei der Personaldatenverarbeitung**.

Eine wichtige Neuregelung erlaubt künftig, Personalakten ganz oder in Teilen ausschließlich elektronisch zu führen. Dabei darf es in der Praxis im Vergleich zur Papierakte nicht zu einer Reduzierung bei der Datensicherheit sowie bei den Rechten der Betroffenen kommen. Ausschließlich **elektronisch geführte Akten** bieten sich in den Bereichen an, die schon bisher von automatisierter Datenverarbeitung geprägt sind, etwa bei der Arbeitszeiterfassung oder der Urlaubsgewährung. Der Gesetzentwurf enthält leider keine Detailregelungen und insofern keine Verordnungsermächtigung. Es ist daher naheliegend, Einzelheiten zur Revisionsfähigkeit und Vertraulichkeit der Daten sowie zu den Rechten Betroffener in Vereinbarungen zwischen Dienststelle und Personalrat aufzunehmen, um so eine Allgemeinverbindlichkeit der Regelungen für die jeweilige Dienststelle zu erreichen.

In der Diskussion mit dem Innenministerium blieb nur ein wesentlicher Punkt offen: Unterlagen, die zum Zweck der **Aufsicht oder Rechnungsprüfung** angelegt werden, dienen nach dem Entwurf von der Person und dem Dienstverhältnis sachlich zu trennenden Zwecken und werden deshalb nicht mehr als Bestandteil der Personalakte angesehen. Dies widerspricht dem Beamtenstatusgesetz, wonach zur Personalakte alle Unterlagen gehören, die die Beamtin oder den Beamten betreffen, soweit sie mit dem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten). Aus unserer Sicht wirken sich Fehler, die bei der Rechnungsprüfung festgestellt werden, direkt auf das Dienstverhältnis aus, ebenso wie Entscheidungen von aufsichtsberechtigten Stellen, die für den jeweiligen Personalfall in der Regel verbindlich sind. Das Landesdatenschutzgesetz stellt insoweit bisher klar: „Die Verarbeitung der Daten zur Ausübung von Aufsichts- und Kontrollbefugnissen sowie zur Rechnungsprüfung gilt nicht als Verarbeitung für andere Zwecke.“ Diese Regelung hat sich für die unterschiedlichsten Verwaltungsbereiche bewährt. Ein Grund für eine abweichende Sonderregelung ist nicht erkennbar. In der Praxis haben sich aus der Anwendung des Personalaktenrechts für diese Bereiche keine Probleme ergeben. Die Akten mussten lediglich formal als Personalteil- bzw. -nebenakten gekennzeichnet sowie in das entsprechende Verzeichnis in der Grundakte aufgenommen werden.

Was ist zu tun?
Der Gesetzgeber sollte Unterlagen, die bei der Aufsichts- oder Revisionstätigkeit anfallen, nicht aus dem Schutzbereich des Personalaktenrechts herausnehmen.

4.2 Polizei und Verfassungsschutz

Das **neue Polizeirecht**, mit dem sich das ULD in vorangegangenen Jahren im Rahmen der Gesetzgebung auseinandergesetzt hat, ist mittlerweile in Kraft getreten. Es ist für die Polizei wie für das ULD Grundlage der täglichen Praxis. Inzwischen konnten erste Erfahrungen gemacht werden (Tz. 4.2.1).

Als echter **Dauerbrenner** begleitet uns das polizeiliche Verfahren @rtus, das weiter ausgebaut werden soll und zudem in der bestehenden Fassung genügend Raum für Verbesserungen bietet (Tz. 4.2.1). Ein weiterer Dauerbrenner wurde die Kontrolle bei der Abteilung für Staatsschutz im Landeskriminalamt, die – mittlerweile im fünften Jahr – immer noch nicht abgeschlossen werden konnte (Tz. 4.2.5).

Im Bereich **Verfassungsschutz** beschäftigten uns Eingaben von Betroffenen (Tz. 4.2.8), die Einführung eines neuen IT-Verfahrens (Tz. 4.2.9) und der Gesetzentwurf für eine Änderung des Landesverfassungsschutzgesetzes (Tz. 4.2.6).

Die **Gremien der Datenschutzbeauftragten** des Bundes und der Länder befassten sich mit Fragen der polizeilichen Datenverarbeitung auf nationaler und europäischer Ebene. Die Arbeitsgruppe INPOL und die Unterarbeitsgruppe Europa des Arbeitskreises Sicherheit verfolgen das Ziel, durch eine frühzeitige Beratung die nationale wie die grenzüberschreitende Datenverarbeitung der Polizei in Informationsverbünden datenschutzgerecht zu gestalten. Die Unterarbeitsgruppe Europa hat beispielsweise die Zusammenarbeit der Polizeien und der Strafverfolgungsbehörden der EU-Mitgliedstaaten nach dem Rahmenbeschluss zur sogenannten Schwedischen Initiative näher beleuchtet und einen Beschluss der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vorbereitet (Tz. 11.1 und Tz. 11.2).

4.2.1 Landesverwaltungsgesetz (LVwG) – Erfahrungen mit dem neuen Polizeirecht

Das Landesverwaltungsgesetz wurde im Jahr 2007 novelliert und hat nun erste Bewährungsproben zu bestehen gehabt.

- **Das Ende der Kfz-Kennzeichenerfassung**

Mit dem neuen Polizeirecht wurde u. a. die Kfz-Kennzeichenerfassung in Schleswig-Holstein eingeführt. Die Regelung hierzu war nicht nur von uns im Hinblick auf Normenklarheit, Verhältnismäßigkeit und Gesetzgebungskompetenz kritisiert worden (30. TB, Tz. 4.2.1), sondern war auch Gegenstand einer **Verfassungsbeschwerde** vor dem Bundesverfassungsgericht. Dieses hat die angegriffene Vorschrift für nichtig erklärt. Die Regelung genügt nicht dem Gebot der Normenbestimmtheit und Normenklarheit, da sie weder den Anlass noch den Ermittlungszweck benennt, dem die Erhebung und der Abgleich der Daten dienen sollen. Darüber hinaus, urteilten die Karlsruher Richter, verstößt sie in ihrer unbestimmten Weite gegen das verfassungsrechtliche **Gebot der Verhältnismäßigkeit**. Sie ermög-

licht schwerwiegende Eingriffe in das Recht auf informationelle Selbstbestimmung, ohne die für derart eingriffsintensive Maßnahmen grundrechtlich geforderten gesetzlichen Eingriffsschwellen hinreichend zu normieren.

Unmittelbar nach dem Karlsruher Richterspruch verkündete der Innenminister das **Ende der Kfz-Kennzeichenerfassung** in Schleswig-Holstein. Einen erneuten Vorstoß, die gesetzliche Regelung an die Vorgaben aus Karlsruhe anzupassen, solle es nicht geben. Beweggrund für diese Entscheidung war auch das deutliche Missverhältnis zwischen Aufwand und Ertrag der Maßnahme. Mit einer äußerst geringen Trefferzahl hatte sich das Kfz-Scanning als ungeeignetes Instrument zur Abwehr von Gefahren für die öffentliche Sicherheit erwiesen.

Was ist zu tun?
Die Entscheidung des Innenministers zeigt besonnenes und sachorientiertes Handeln in der Sicherheitspolitik. Viele andere grundrechtsrelevante Maßnahmen sollten einer ähnlich kritischen fachlichen Prüfung unterzogen werden.

- **Neuerungen bei @rtus**

Die Datenverarbeitung der Polizei in Schleswig-Holstein befindet sich im Umbruch. Das Verfahren @rtus ist zwischenzeitlich landesweit im Einsatz. Es haben sich einige Schwachstellen gezeigt, die ausgebessert werden müssen. Parallel arbeitet die Polizei daran, @rtus auszubauen. Das Verfahren soll, so jedenfalls die Planungen, um einen Teil „**Analyse und Auswertung**“ ergänzt werden. In dieser Datei sollen personenbezogene Daten aus @rtus gespeichert und im Rahmen der Sachbearbeitung für die genannten Zwecke genutzt werden. Die Anwendung soll nur einem kleinen Kreis von Experten zur Verfügung stehen. Es ist weiterhin vorgesehen, dass auch die Lageberichte mit diesem Verfahren vereinheitlicht und zentral zur Verfügung gestellt werden sollen.

- **Auskunft für die Betroffenen**

Das Verfahren der Auskunftserteilung an Betroffene wurde in einer Arbeitsgruppe der Polizei an der auch das ULD teilnehmen konnte, analysiert und lief bis zum Ende des Jahres 2008 in einem Pilotverfahren. Es geht darum, Beteiligungsprozesse innerhalb der Polizeidienststellen festzulegen und den Umfang der zu erteilenden Auskunft zu bestimmen, sodass die Betroffenen möglichst konkret erfahren, welche Daten über sie aus welchem Anlass, in welchem Verfahren und für welche Dauer gespeichert sind. Zudem ist eine Lösung gefunden worden, dass die Bürgerinnen und Bürger bei einer Auskunft darüber informiert werden, ob Polizeibehörden anderer Länder oder des Bundes Daten in der gemeinsamen Verbundanwendung INPOL beim BKA gespeichert haben. Die Betroffenen haben das Recht zu erfahren, in welchem Zusammenhang ihre Daten an andere Stellen übermittelt wurden. Die Polizei strebt an, **eine Stelle** bei der Landespolizei für die Auskunftserteilung zu benennen, die nach außen gegenüber den Betroffenen in Erscheinung tritt. An welche Polizeibehörde der Betroffene sein Auskunftsersuchen richtet, ist dabei unerheblich.

4.2.2 Online-Durchsuchung für Polizei und Verfassungsschutz

Das Bundesverfassungsgericht hat im Februar 2008 die Befugnisnorm zur sogenannten Online-Durchsuchung im nordrhein-westfälischen Verfassungsschutzgesetz für nichtig erklärt. Mit dieser Entscheidung hat es die Anforderungen für die Maßnahme, die vor allem im Bund seit einigen Jahren kontrovers diskutiert wird, festgelegt.

Das Bundesverfassungsgericht hat die nordrhein-westfälische Regelung zur Online-Durchsuchung verworfen; eine generelle Unzulässigkeit folgt aus dieser Entscheidung indes nicht. Vielmehr wurden in dem Urteil die **Voraussetzungen einer solchen Maßnahme** festgelegt, unter denen eine Online-Durchsuchung zulässig sein kann. Damit war im Bund der Startschuss für eine eigene Regelung zur Online-Durchsuchung gefallen. Diese Kompetenz soll das Bundeskriminalamt (BKA) zum Zweck der Abwehr terroristischer Gefahren erhalten. Eine entsprechende Regelung wurde eilig in das Gesetzgebungsverfahren zur Änderung des Bundeskriminalamtsgesetzes (BKAG) aufgenommen. In Bayern sind Befugnisse zur Online-Durchsuchung für die Polizei und den Verfassungsschutz bereits in Kraft.

Um den Eingriffscharakter der Online-Durchsuchung zu beschreiben, musste das Bundesverfassungsgericht eigens eine neue Ausprägung aus dem allgemeinen Persönlichkeitsrecht ableiten: das **Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme**. Dies schützt, anders als das Recht auf informationelle Selbstbestimmung, nicht die einzelnen Verarbeitungen personenbezogener Daten, sondern das informationstechnische System selbst, mit dem personenbezogene Daten verarbeitet werden. Das Bundesverfassungsgericht hat die besondere Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung, aber auch die Persönlichkeitsgefährdungen, die mit dieser Nutzung verbunden sind, und ein daraus folgendes erhebliches Schutzbedürfnis erkannt und richtig analysiert. Der Einzelne ist darauf angewiesen, dass der Staat mit Blick auf die ungehinderte Persönlichkeitsentfaltung den berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme entspricht. Diesem Schutzbedürfnis tragen nach Auffassung des Gerichts das Recht auf Unverletzlichkeit der Wohnung, das Fernmeldegeheimnis sowie das Recht auf informationelle Selbstbestimmung nicht ausreichend Rechnung. Diese Schutzlücke soll durch das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme geschlossen werden.

Die Maßnahme der Online-Durchsuchung kann mit diesem Grundrecht unter bestimmten engen Voraussetzungen zulässig sein, sowohl zu Zwecken der Gefahrenabwehr als auch zur Strafverfolgung. Sie müssen aber auf einer verfassungsmäßigen gesetzlichen Grundlage beruhen, die hinreichend normenklar und bestimmt sowie verhältnismäßig ist. Dabei ist zu berücksichtigen, dass es sich bei

einem heimlichen Zugriff auf einen Rechner oder ein anderes informationstechnisches System mit dem Ziel der längerfristigen Überwachung um einen besonders **intensiven Grundrechtseingriff** handelt. Dies liegt vor allem an dem Umfang und der Vielfältigkeit des Datenbestands, der sich den Ermittlern bei einem Zugriff auf das System erschließt, an der Heimlichkeit der Maßnahme sowie daran, dass infolge des Zugriffs Gefahren für die Integrität des Rechners entstehen können. Angesichts der hohen Eingriffsintensität kann die Verhältnismäßigkeit der Maßnahme nur sichergestellt werden, wenn deren Einsatz im präventiven Bereich auf die Abwehr konkreter Gefahren für überragend wichtige Rechtsgüter beschränkt bleibt. Darüber hinaus sind geeignete Verfahrensvorkehrungen, wie die Anordnung der Maßnahme durch einen Richter, zu treffen und die Unantastbarkeit des Kernbereichs privater Lebensgestaltung zu sichern.

Bei Einhaltung dieser Anforderungen kann das Instrument der Online-Durchsuchung zwar verfassungskonform eingesetzt werden, doch verbleiben **Risiken**, die auch durch den Gesetzgeber nicht ausgeräumt werden können. Die erste Schwierigkeit wird schon die Auswahl des Zielsystems bereiten. Gerade bei einer Infiltration über das Internet ist man nicht davor gefeit, versehentlich das falsche IT-System zu infiltrieren, da dynamisch mit dem Internet verbundene Rechner sich in der Regel nicht hinreichend sicher eindeutig adressieren lassen. Ist die Infiltration erfolgreich, wird es den Ermittlern möglich, das gesamte infiltrierte System gezielt zu manipulieren. Dies hat insbesondere Einfluss auf den Informationsgehalt der mittels Online-Durchsuchung aufgefundenen Daten. Dass diese vom Betroffenen selbst stammen, kann aufgrund der Manipulierbarkeit des Zielsystems nicht mehr mit Sicherheit festgestellt werden. Außerdem können durch die Installation von Softwarekomponenten, die zum Zweck der Durchsuchung und Überwachung auf den Rechner aufgebracht werden, Sicherheitslücken entstehen, die auch durch unbefugte Dritte ausgenutzt werden können. Solche Sicherheitslücken können durch Deinstallation der Software nicht vollständig geschlossen werden.

Schließlich ist darauf hinzuweisen, dass die Unantastbarkeit des **Kernbereichs privater Lebensgestaltung** bei der Online-Durchsuchung technisch nicht gewährleistet werden kann. Es mag verfassungsrechtlich noch hinnehmbar sein, in diesen Fällen erhobene Daten aus dem Kernbereich bei einer Auswertung zu filtern und zu löschen. Die Unantastbarkeit des Kernbereichs ist allerdings bereits bei der Erhebung entsprechender Daten verletzt. Angesichts der begrenzten Erkenntnismöglichkeiten bei dieser hochinvasiven Methode bei professionalisierten Kriminellen spricht vieles dafür, auf die Online-Durchsuchung völlig zu verzichten.

Was ist zu tun?
Die Online-Durchsuchung ist verfassungsrechtlich zwar möglich. Doch ist deren Durchführung zwangsläufig mit gesetzlich nicht regulierbaren Risiken verbunden. Der schleswig-holsteinische Gesetzgeber sollte daher von einer Einführung dieses Instruments weiterhin Abstand nehmen.

4.2.3 Landeskriminalamt überprüft für Deutsche Bundesbank Fremdpersonal

Bei der Fußballweltmeisterschaft 2006 ist das sogenannte Akkreditierungsverfahren als ein Personenüberprüfungsverfahren gegen den Widerstand der Datenschützer in der Praxis eingeführt worden. Dieses „Musterverfahren" wird zunehmend in anderen Bereichen eingesetzt. Es hatte sich ja bestens bewährt …

Anlässlich der **Fußballweltmeisterschaft 2006** hielten es die Verantwortlichen für erforderlich, ein Akkreditierungsverfahren einzuführen. Es war damals aus Zeitgründen nicht möglich, eine andere Lösung zu finden, und es sollte ein Verfahren zwischen Bundes- und Landesbehörden sein, das ausnahmsweise bei dieser Großveranstaltung eingesetzt wurde. Im Rahmen dieses Verfahrens mussten sich Journalisten, Servicepersonal und weitere Personen, die in den Stadien ihrem Beruf nachgehen wollten, überprüfen lassen. Das ULD hatte das Landeskriminalamt (LKA) und die Verfassungsschutzbehörde frühzeitig darauf hingewiesen, dass es sich hierbei um eine Überprüfung ohne gesetzliche Grundlage und mit erheblichen Eingriffen in Grundrechte handelt, die lediglich auf eine Einwilligungserklärung der Betroffenen gestützt wird. Das Innenministerium setzte sich über diese Bedenken hinweg und gab den beteiligten Stellen grünes Licht. Das ULD beanstandete diese Akkreditierungsverfahren förmlich (29. TB, Tz. 4.2.5).

Die Befürchtungen des ULD, dass sich hieraus nach und nach ein **Standardverfahren** für eine Vielzahl von sogenannten Zuverlässigkeitsüberprüfungen entwickeln könnte (30. TB, Tz. 4.2.3), scheinen sich zu bewahrheiten. Auch die Deutsche Bundesbank ist auf die Idee gekommen, außerhalb des Anwendungsbereichs des Sicherheitsüberprüfungsgesetzes ihr Fremdpersonal überprüfen zu lassen. Die Deutsche Bundesbank und das LKA Schleswig-Holstein haben eine Vereinbarung geschlossen, wonach das LKA kriminalpolizeiliche wie auch staatsschutzrelevante Erkenntnisse aus den Kriminalakten und den INPOL-Verbunddateien an die Deutsche Bundesbank zur Bewertung übermittelt. Die Betroffenen erhalten zuvor einen Erklärungsbogen, in dem sie ihren Namen, Geburtsdatum und -ort, die Wohnsitze der letzten fünf Jahre, Ausweis-/Passnummer sowie eine Erklärung zur Staatsbürgerschaft – freiwillig – eintragen „müssen". Der Vordruck enthält auch Angaben zur Notwendigkeit der Überprüfung und zur Datenverarbeitung. Die Betroffenen erhalten keine Kenntnis über die vorliegenden und an die Deutsche Bundesbank als Entscheidungsgrundlage übermittelten Daten. Es fehlt jede Aufklärung über etwaige rechtliche Möglichkeiten, ob und wie sie sich gegen die Maßnahmen wehren können. Alle drei Jahre findet eine Wiederholungsüberprüfung statt – ob mit oder ohne Kenntnis des Betroffenen ist dem Erklärungsbogen nicht zu entnehmen. Dies ist in jeder Hinsicht eine Überprüfung mit erheblichem Überraschungspotenzial für die Betroffenen!

Wir haben im Vorfeld der Einführung des Verfahrens in Schleswig-Holstein das Innenministerium des Landes auf die **Unzulässigkeit des Verfahrens** hingewiesen – ohne Erfolg. Dem ULD blieb keine andere Möglichkeit, als das Verfahren zu beanstanden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigte die Kritik an dieser Form der Datenerhebung und -nutzung.

http://www.bfdi.bund.de/cln_007/nn_1207020/DE/Oeffentlichkeitsarbeit/Entschliessungssammlung/DSBundLaender/75DSK__Arbeitnehmerdaten.html

Was ist zu tun?
Zuverlässigkeitsüberprüfungen dürfen ohne gesetzliche Grundlage nicht stattfinden. Das Votum des Gesetzgebers ist einzuholen, bevor sich weitere Stellen an der Idee der Personenüberprüfung auf Basis angeblich informierter Einwilligungen begeistern und das Verfahren zur alltäglichen Gewohnheit wird.

4.2.4 Die Polizei bei der Kommunalwahl im Einsatz

Zwei Bürger wollten am Abend der Kommunalwahl 2008 im Kieler Rathaus die Veröffentlichung des Wahlergebnisses verfolgen. Am Eingang wurden sie abgewiesen und erhielten Hausverbot. Ein Polizeibeamter hatte die beiden als Angehörige der alternativen Szene erkannt.

Die beiden Menschen wandten sich ans ULD, weil sie am Abend der Kommunalwahl 2008 ein **Hausverbot für das Kieler Rathaus** erhalten hatten, wo die Auszählung der Stimmen stattfand. Hieran wollten die Petenten teilnehmen. Im Eingangsbereich des Rathauses erfolgten Einlasskontrollen. Nach Angaben der Polizei war es an den Wochenenden zuvor zu Auseinandersetzungen zwischen rechten und linken Gruppierungen in der Innenstadt gekommen. In ihrer Lagebewertung ging sie von der Möglichkeit einer offenen Konfrontation bis hin zu körperlichen Auseinandersetzungen aus. Die Polizei und die Stadt Kiel verabredeten, dass ein Polizeibeamter seine Bewertung der eintretenden Personen an den Bediensteten der Stadt weitergibt und dieser dann aufgrund des Hausrechtes vorgeht.

Unsere Prüfung ergab, dass die Bewertung der einen Person erfolgte, ohne dass der Polizeibeamte diese überhaupt namentlich kannte. Die Person sei dem **antifaschistischen Bündnis zuzurechnen**. In den Dateien der Polizei sind keine Daten über die Person gespeichert. Es handelte sich um eine dienstliche Kenntnis, teilte uns das Landespolizeiamt mit. Auch die Bewertung der zweiten Person basierte nicht auf gespeicherten Angaben. Die Person sei dem Polizeibeamten langjährig als eine Hauptperson der alternativen Szene bekannt. Beide Hausverbote wurden durch die Stadt Kiel in eigener Verantwortung ausgesprochen, betont die Polizei in ihrer Stellungnahme. Gestützt waren die städtischen Verfügungen ausschließlich auf den Informationen der Polizei.

Das Gemeinde- und Kreiswahlgesetz garantiert die **Öffentlichkeit der Wahlhandlungen** und der Feststellung des Wahlergebnisses. Der Wahlvorstand kann Personen, die die Ordnung und Ruhe stören, aus dem Wahlraum verweisen. Eine solche Entscheidung hatte der Wahlvorstand nicht getroffen; die Selektion aller Besucher war im Vorfeld erfolgt.

Im Wortlaut:
§ 29 Gemeinde- und Kreiswahlgesetz

Die Wahlhandlungen und die Feststellung des Wahlergebnisses sind öffentlich. Der Wahlvorstand kann Personen, die die Ordnung und Ruhe stören, aus dem Wahlraum verweisen.

Die Polizei und das ULD sind sich uneinig über die anwendbare Rechtsgrundlage für die erfolgte Datenübermittlung. Wir meinen, dass die Mitteilung an die Stadt als Ordnungsbehörde gemacht wurde. In jedem Fall waren die von der Polizei übermittelten Daten objektiv nicht geeignet, die Hausverbote zu begründen. Der Grundsatz der Verhältnismäßigkeit wurde verletzt. Die polizeiliche Beurteilung der Personen war eine subjektive Bewertung. Die Betroffenen hatten mit ihrem Verhalten keinerlei Anlass für eine Speicherung in einer Datei der Polizei gegeben, hatten weder eine Gefahr verursacht, noch eine Straftat begangen. Die **Teilnahme an Demonstrationen** musste unberücksichtigt bleiben, zumal es sich dabei um eine zulässige Grundrechtsausübung handelt, aus der den Betroffenen keine Nachteile erwachsen dürfen. Die erfolgte Mitteilung der Informationen über die Teilnahme der Petenten an Demonstrationen war rechtswidrig und wurde vom ULD beanstandet.

Was ist zu tun?
Bei Einsätzen der Polizei, bei denen spontan grundrechtsrelevante Entscheidungen getroffen werden müssen, bedarf es eines sorgfältigen Vorgehens. Es reicht für einen Eingriff in geschützte Rechte von Bürgerinnen und Bürgern nicht, dass einem Polizeibeamten die Person von Demonstrationen bekannt ist. Weitergegeben werden dürfen nur „polizeifeste Daten“.

4.2.5 Die unendliche Geschichte: Kontrolle der Abteilung 3 des Landeskriminalamtes

Bei den beiden Dateien „Innere Sicherheit Schleswig-Holstein“ und „Warndatei rechts“ gibt es nur kleine Fortschritte.

„Es war einmal“, so beginnen viele Märchen. Im Landeskriminalamt benötigen Angelegenheiten manchmal eine so lange Zeit, dass es viel guter Hoffnung bedarf, um an ein gutes Ende zu glauben. Die Verarbeitung in der Datei „Innere Sicherheit Schleswig-Holstein“ (ISSH und der „Warndatei rechts“ wurde vom ULD vor etwa vier Jahren wegen **fehlender Errichtungsanordnungen** beanstandet. Das Landeskriminalamt (LKA) hat nun – nach dem Nachbohren des ULD wie des Innenministeriums – begonnen, den bisherigen Absichtserklärungen Taten folgen zu lassen und die Errichtungsanordnungen zu erstellen.

In der **Datei ISSH** werden Daten von Personen erfasst, die einer politisch motivierten Straftat verdächtig sind, sofern Wiederholungsgefahr besteht und dies zur Aufklärung oder Verhütung einer künftigen Straftat erforderlich ist. Außerdem werden Sachverhaltsinformationen zu sämtlichen politisch motivierten Straftaten gespeichert. Daraus sollen z. B. Auswertungen, Statistiken und Führungsentscheidungen erstellt werden. Die Daten sollen zudem zu Zwecken der Prävention und Repression zur Verfügung stehen.

Wir bezweifeln, dass sich das Datenmaterial und die **aktuelle technische Dateigestaltung** für die Erreichung aller genannten Zwecke eignen. Das LKA scheint diese Besorgnis zu teilen, weil es in den vergangenen Jahren immer wieder überlegte, ein anderes Verfahren oder eine neue Software einzusetzen. Wir baten das LKA im Interesse einer Klärung der Erforderlichkeiten und der Realisierung von Datensparsamkeit und Datenvermeidung um Konkretisierung der Zwecke. Das ULD signalisierte, bei positivem Ausgang der internen Prüfung das gesamte Verfahren auditieren zu können. Der Entwurf einer Errichtungsanordnung bestärkte uns in unserer kritischen Sicht. Fragen zur Rechtsgrundlage, zur Zweckbeschreibung, zu den Personen, die gespeichert werden dürfen, zur Datenübermittlung und zur Speicherungsdauer – alles Aspekte, die normalerweise vor der Implementierung einer DV-Anwendung geklärt sein müssen – sind eine valide Grundlage, sich über das bestehende Verfahren Rechenschaft abzulegen und über eine bessere und datensparsamere neue technische Plattform bzw. über eine neue Software nachzudenken. Die Chance zur Verbesserung sollte nicht durch weiteres jahrelanges Zuwarten vergeben werden.

Auch der erste Entwurf einer Errichtungsanordnung für die „**Warndatei rechts**“ hat bei uns Bedenken zur Geeignetheit aufkommen lassen. Die Zweckbeschreibung lässt die konkret verfolgten Ziele nicht erkennen. Für strategische oder statistische Auswertungen, zur Unterstützung von Führungsentscheidungen und kriminologischer Forschung bedarf es keiner personenbezogenen Datenverarbeitung, es genügt ein anonymisierter Datenbestand. Durch die Erfassung unzähliger verschiedener persönlicher Daten entsteht eine Diskrepanz zwischen Zweck und Mittel. Auffällig ist auch das Fehlen technisch-organisatorischer Sicherungen. Die revisionsfeste Protokollierung der Abrufe aus der Datei ISSH ist Standard, doch leider noch nicht bei der „Warndatei rechts“.

Was ist zu tun?
Das LKA sollte die Erstellung der Errichtungsanordnungen zur Hinterfragung und Optimierung der beiden Staatsschutzdateien nutzen.

4.2.6 Landesverfassungsschutzgesetz kontra Verfassung

Der Beobachtungsauftrag der Verfassungsschutzbehörde soll erweitert werden. Sie soll umfangreiche neue Befugnisse bekommen, u. a. die auf Bundesebene bereits bestehenden, stark umstrittenen Auskunftsrechte über Telekommunikationsverkehrsdaten, Konto- und Reisebewegungen.

Lange Zeit war es still in Schleswig-Holstein bei der Sicherheitsgesetzgebung. Doch nun beschloss der Landtag ein Gesetz mit Befugnissen für die Verfassungsschutzbehörde, die es im Bund und in anderen Ländern längst gibt. Nicht dass diese sich dort bewährt hätten – im Gegenteil: Im Bund wurden diese Befugnisse des **Terrorismusbekämpfungsgesetzes** kurz nach den Anschlägen vom 11. September 2001 zwar durch das Terrorismusbekämpfungsergänzungsgesetz erweitert (29. TB, Tz. 4.2.7). Im Einzelnen handelt es sich hierbei um Auskunftsrechte gegenüber Luftfahrtunternehmen, Kreditinstituten, Finanzdienstleistern sowie Telekommunikations- und Telediensteanbietern über Reisebewegungen, Konten und Kontobewegungen sowie um Verkehrsdaten über die Nutzung von Telekommunikation und Telemedien. Doch hat es eine unabhängige wissenschaftliche Evaluation dieser für den Bund seit sieben Jahren bestehenden Befugnisse nicht gegeben, Eignung und Erforderlichkeit sind mehr als fragwürdig. Dies hinderte die Landesregierung nicht daran, die Befugnisse auch für die Verfassungsschutzbehörde Schleswig-Holstein vorzuschlagen. Weshalb diese hier jetzt zur Bekämpfung des Terrorismus erforderlich sind, obwohl es bisher auch ohne ging, beantwortet der Gesetzentwurf nicht.

In einzelnen Punkten hält sich das Gesetz an sein erklärtes Ziel, das Verfassungsschutzrecht **in „moderater Weise“** anzupassen und gleichzeitig den Grundrechtsschutz zu stärken. Es wird versucht, die nachrichtendienstlichen Mittel abschließend zu regeln; auf die Einführung der Online-Durchsuchung (Tz. 4.2.2) wird verzichtet.

In anderen Punkten geht das Gesetz allerdings über das verfassungsrechtlich Akzeptable hinaus, so bei der Nutzung der sogenannten Vorratsdaten und bei der unzureichenden Regelung zum Schutz des Kernbereichs privater Lebensgestaltung. Das Gesetz ermächtigt die Verfassungsschutzbehörde, bei Telekommunikationsunternehmen und Internetprovidern die „auf Vorrat“ gespeicherten **Verkehrsdaten über Telefon- und Internetverbindungen** (Tz. 4.3.1) abzufragen. Gegen die Vorratsdatenspeicherung sind Verfassungsbeschwerden vor dem Bundesverfassungsgericht anhängig. Die Entscheidung in der Hauptsache steht zwar noch aus, doch im Verfahren des einstweiligen Rechtsschutzes hat das Bundesverfassungsgericht durch einstweilige Anordnung die Nutzung der Vorratsdaten für die Verfassungsschutzbehörden eingeschränkt. Die schleswig-holsteinischen Regelungen entsprechen den bayerischen, die das Bundesverfassungsgericht für nicht anwendbar erklärt hat. Seine Hinweise in der Eilentscheidung zu der weiten und offenen Regelung der Schutzgüter sowie zu den niedrigen Gefahren- und Verdachtsschwellen deuten darauf hin, dass die Regelung im Hauptsacheverfahren keinen Bestand haben wird.

Die Regelung zum Schutz des **Kernbereichs privater Lebensgestaltung** genügt unseres Erachtens ebenfalls nicht den verfassungsrechtlichen Anforderungen. Wie vom ULD angeregt, gilt die Norm für alle nachrichtendienstlichen Mittel. Die gesetzlichen Vorkehrungen gegen ein Eindringen in den Kernbereich, also gegen das Erheben höchst persönlicher Daten, sind allerdings unzureichend. Heimliche Ermittlungen sollen nur dann ausgeschlossen sein, wenn Anhaltspunkte dafür bestehen, dass durch sie **allein** Informationen aus dem Kernbereich privater Lebensgestaltung erhoben werden. Dies bedeutet, dass heimliche Ermittlungen

auch im Kernbereich der privaten Lebensgestaltung stets zulässig sind, wenn neben den Kernbereichsinformationen voraussichtlich auch andere Informationen erlangt werden. Natürlich ist dies der Regelfall. Üblicherweise werden bei Gesprächen im Kernbereich mit intimen Informationen auch banale Inhalte ausgetauscht. Der Schutz vor einer Erhebung von Kernbereichsinformationen hat eine zentrale Bedeutung, da in den „unantastbaren" Kernbereich privater Lebensgestaltung eingedrungen wird. Der im Gesetz vorgesehene Schutz reduziert diesen auf äußerst unwahrscheinliche Fallgestaltungen und hebelt ihn damit aus. Insofern wird es eine Klärung durch das Bundesverfassungsgericht geben; wortgleiche Regelungen sind Gegenstand von Verfassungsbeschwerden.

www.datenschutzzentrum.de/allgemein/080722-verfassungsschutzg-e.htm

Was ist zu tun?
Das Gesetz sollte geändert werden, um die verfassungsrechtlichen Bedenken auszuräumen.

4.2.7 Antiterrordatei – Wer kontrolliert die Protokolldaten?

Beim Bundeskriminalamt (BKA) wird die Antiterrordatei betrieben. Das BKA hat nach dem Gesetz die Zugriffe auf die Datei zu speichern. Streit besteht über die Frage, wer in welchem Umfang zu Kontrollzwecken auf die Protokolldaten zugreifen darf.

Sowohl der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) als auch die Landesbeauftragten für den Datenschutz sind im Gesetz als für die Kontrolle zuständige Stellen benannt. Der BfDI ist für die Kontrolle der Durchführung des Datenschutzes zuständig, während die Landesbeauftragten für die Kontrolle der Eingabe und der Abfrage von Daten durch die Landesbehörden verantwortlich sind. Nach Auffassung des BKA dürfen die kontrollierenden Stellen auf die Protokolldaten nur in dem Umfang zugreifen, wie dies für eine Kontrolle der Eingaben und Abfragen der jeweils kontrollierten Behörde erforderlich ist. Konsequenz dieser Rechtsauffassung wäre, dass jede kontrollierende Stelle stets **nur einen Ausschnitt der Protokolldaten** zu sehen bekäme. Der BfDI hätte danach nur Zugriff auf die Daten, die bei der Eingabe oder dem Abruf durch Bundesbehörden protokolliert wurden, das gleiche gälte für die Landesbeauftragten für den Datenschutz in Bezug auf die teilnehmenden Landesbehörden.

Im Wortlaut:
§ 10 Abs. 1 Antiterrordateigesetz

Die Kontrolle der Durchführung des Datenschutzes obliegt nach § 24 Abs. 1 des Bundesdatenschutzgesetzes dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Die datenschutzrechtliche Kontrolle der Eingabe und der Abfrage von Daten durch eine Landesbehörde richtet sich nach dem Datenschutzgesetz des Landes.

Kontrollen der Protokollierung durch Querschnittsprüfungen wären danach praktisch nicht möglich. Nach einhelliger Auffassung der Datenschutzbeauftragten des Bundes und der Länder greift der Ansatz des BKA zu kurz und wird den im Antiterrordateigesetz vorgesehenen **Verantwortlichkeiten nicht gerecht**. Das BKA trägt die Verantwortung für die Protokollierung der Zugriffe. Der BfDI ist zuständig für die Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften durch das BKA. Für die Kontrolle der Rechtmäßigkeit der Eingaben und Abrufe durch die teilnehmenden Behörden ist jeweils der für die Behörde zuständige Datenschutzbeauftragte des Bundes oder des jeweiligen Landes zuständig. Es bestehen also parallele Zuständigkeiten, die unterschiedliche Zugriffe auf die Protokolldaten erfordern. Dem BfDI ist zwecks Kontrolle der Protokollierung ein Zugriff auf den gesamten Protokolldatenbestand zu gewähren. Für Kontrollen der einzelnen Eingaben und Abrufe genügt ein entsprechender Ausschnitt. Dies wurde dem BKA und dem Bundesministerium des Innern mitgeteilt. Es ist nicht erkennbar, welches Ziel mit der Behinderung der Datenschutzkontrolle verfolgt wird.

Was ist zu tun?
Das BKA muss die Zuständigkeit des BfDI für die Kontrolle der ordnungsgemäßen Protokollierung als auch die Zuständigkeit der Landesbeauftragten für die Kontrolle der durch die Protokolldaten dokumentierten Eingaben und Abfragen anerkennen.

4.2.8 Arbeitszeugnisse in Sicherheits- bzw. Sicherheitsüberprüfungsakten

Die Verfassungsschutzbehörde darf bei Sicherheitsüberprüfungen von Bediensteten nicht alle Daten speichern, die sie zur Kenntnis nehmen darf. Es reicht bei einem Personalaktenabgleich zumeist eine Notiz in der Sicherheitsakte aus, dass eine Überprüfung der Angaben stattgefunden hat. Kopien aus Personalaktenunterlagen haben in Sicherheitsakten grundsätzlich nichts zu suchen.

Eine Mitarbeiterin der Verfassungsschutzbehörde des Landes hatte bei Einsicht in ihre Sicherheitsakte festgestellt, dass sich dort Kopien von Zeugnissen früherer Arbeitgeber befanden. Diese Kopien waren als Nachweis des zulässigen Abgleichs mit ihrer Personalakte gefertigt worden. Der Abgleich mit der Personalakte dient dazu, die **berufliche Vita zu belegen**. Die Frage ist jedoch, ob es erforderlich und somit zulässig ist, wie die Verfassungsschutzbehörde meinte, Kopien der Arbeitszeugnisse in die Sicherheitsakte zu nehmen. Wir haben erreicht, dass die Kopien der Arbeitszeugnisse aus der Akte des Verfassungsschutzes entfernt werden. Sofern sich aus den Arbeitszeugnissen relevante Angaben ergeben, die für die Durchführung der Sicherheitsüberprüfung aus dem Jahr 1983 erforderlich sind, werden diese nachträglich in der Sicherheitsakte dokumentiert, was rechtlich nicht zu beanstanden ist. Die Kopien selbst werden vernichtet.

Was ist zu tun?
Personenbezogene Daten dürfen nur für den Zweck verwendet werden, zu dem sie erhoben wurden, es sei denn, dass das Gesetz die Verwendung für einen anderen Zweck erlaubt. Personalaktendaten, insbesondere Zeugnisse, haben daher nichts in Unterlagen über Sicherheitsüberprüfungen zu suchen.

4.2.9 DIANA beim Verfassungsschutz in Schleswig-Holstein

Die schleswig-holsteinische Verfassungsschutzbehörde hat vor Einführung eines neuen internen Datenbankverfahrens das ULD umfassend beteiligt. Datenschutzrechtliche Anregungen wurden überwiegend umgesetzt – im Ergebnis für Verfassungsschutz und Datenschutz eine gewinnbringende Zusammenarbeit für die Grundrechte der Betroffenen.

Das ULD erhielt von der Verfassungsschutzbehörde den Entwurf der Errichtungsanordnung für eine neue Datei – DIANA. Die Details zu dem Verfahren wurden vom Innenministerium zur Verschlusssache (VS) deklariert. So viel kann dennoch mitgeteilt werden: Hinter der vielversprechenden Bezeichnung DIANA verbirgt sich ein Datenverarbeitungsverfahren, das der **Information und Analyse** von Daten der Verfassungsschutzbehörde dient. Die rechtlichen Bewertungen und Änderungsvorschläge des ULD wurden aufgegriffen und zum größten Teil umgesetzt. Es ging dabei um eine präzise Beschreibung des Zwecks der Datei, des Inhalts, des Umfangs, der Voraussetzungen der Speicherungen, der Übermittlung und Nutzung der Daten. Themen waren auch die Eingabe und Zugangsberechtigung, die Überprüfungsfristen bzw. die Speicherungsdauer, die Protokollierung und die Rechte betroffener Bürgerinnen und Bürger.

Was ist zu tun?
Eine frühzeitige Beteiligung des ULD an automatisierten Datenverarbeitungsverfahren nützt im Interesse der Sicherheit des Verfahrens sowohl der Daten verarbeitenden Stelle als auch den Betroffenen. Die hier gezeigte Zusammenarbeit kann gern auch in anderen Bereichen Schule machen.

4.3 Justizverwaltung

4.3.1 Neues in Sachen Vorratsdatenspeicherung

Schon kurz nach Inkrafttreten musste das Bundesverfassungsgericht die Vorratsdatenspeicherung – zunächst vorläufig – zurückstutzen. Eine endgültige Entscheidung über die europarechtliche und verfassungsrechtliche (Un)Zulässigkeit der Regelungen steht weiterhin aus. Die Befugnisse zum Zugriff auf die Vorratsdaten werden derweil kontinuierlich erweitert – auch in Schleswig-Holstein.

Anfang des Jahres 2008 ist die Vorratsspeicherung von Telekommunikationsverkehrsdaten **in Kraft getreten** (30. TB, Tz. 4.3.1 und Tz. 7.1). Seitdem müssen

die Anbieter von Telekommunikationsdiensten Angaben über Telefonverbindungen ihrer Kunden – z. B. die angerufenen Telefonnummern, Beginn und Ende des Telefonats, bei Mobiltelefonen auch die genutzte Funkzelle – für sechs Monate speichern. Die Daten sollen für Zwecke der Strafverfolgung und Gefahrenabwehr oder für die Aufgaben der Nachrichtendienste genutzt werden. Dies ist allerdings nur dann zulässig, wenn es hierfür eine spezielle gesetzliche Regelung gibt. Solche Regelungen gab es zunächst nur für Strafverfolgungsbehörden. Mittlerweile haben einige Länder entsprechende Regelungen auch für die Polizei- und die Verfassungsschutzbehörden eingeführt (Tz. 4.2.6).

Gegen die Regelungen zur Vorratsdatenspeicherung sind **Verfassungsbeschwerden** beim Bundesverfassungsgericht anhängig. Im Eilverfahren wurde beantragt, die Vorschriften zur Speicherpflicht bis zur Hauptsacheentscheidung auszusetzen. Das Bundesverfassungsgericht hat daraufhin im Wege der einstweiligen Anordnung die Anwendung der Regelungen erheblich eingeschränkt. Zwar dürfen die Daten weiterhin bei den Telekommunikationsunternehmen gespeichert werden. Ihre Übermittlung für Strafverfolgungszwecke ist aber nur noch für bestimmte Straftaten zulässig. Weggefallen ist damit u. a. die Möglichkeit, auf die Vorratsdaten zur Verfolgung jedweder mittels Telekommunikation begangener Straftaten zuzugreifen. Einschränkungen hat das Bundesverfassungsgericht auch bei den Übermittlungen für Zwecke der Gefahrenabwehr sowie für die Aufgabenerfüllung der Nachrichtendienste vorgenommen.

Das Bundesverfassungsgericht hat die Bundesregierung zudem aufgefordert, über die **Erfahrungen mit der Vorratsdatenspeicherung** zu berichten. Aus einem ersten Bericht geht hervor, dass im Zeitraum von Mai bis Juli 2008 bei 1.742 von insgesamt 4.356 Anordnungen ausschließlich auf die Vorratsdaten zurückgegriffen werden musste. Auch wenn der Erfassungszeitraum sehr kurz und die Zahlen daher nur bedingt aussagekräftig sind, ist schon zu erkennen, dass die Vorratsdatenspeicherung ein erhebliches Ausmaß hat.

In einer gemeinsamen **Stellungnahme gegenüber dem Bundesverfassungsgericht** haben die Landesbeauftragten für Datenschutz dargelegt, dass die Vorratsdatenspeicherung in verfassungswidriger Weise das durch Artikel 10 des Grundgesetzes geschützte Fernmeldegeheimnis verletzt:

- Die Maßnahme greift besonders intensiv in die Grundrechte der Betroffenen ein. Dies liegt vor allem an der erheblichen **Streubreite**, da jeder Telekommunikationsteilnehmer erfasst wird, und an der Möglichkeit, aus den gespeicherten Verkehrsdaten Kommunikations- und Bewegungsprofile zu bilden.
- Die Speicherung der Daten erfolgt **anlasslos**. Sie knüpft weder an ein Verhalten des Betroffenen noch an eine abstrakte Gefährlichkeit der ausgeübten Tätigkeit, also der Telekommunikation, an.

- Im Hinblick auf die erhebliche Eingriffsintensität sind die **Schwellen** für die Nutzung der Vorratsdaten **zu niedrig**. So soll die Nutzung der Vorratsdaten für die Verfolgung sämtlicher Straftaten zulässig sein, die mittels Telekommunikation begangen wurden. Dies können auch Bagatellstraftaten wie etwa eine Beleidigung sein. Damit geht die deutsche Regelung in unverhältnismäßiger Weise über die Vorgaben der EG-Richtlinie zur Vorratsdatenspeicherung hinaus.
- Es **fehlen effektive verfahrensrechtliche Regelungen**, die einer Überschreitung der gesetzlichen Zugriffsbefugnisse entgegenwirken und die Vertraulichkeit und Integrität der Vorratsdaten gewährleisten.

Ungeklärt ist auch die Verfassungsmäßigkeit der **Kostentragung**. Zwar hat der Bundestag mittlerweile ein Gesetz über die Entschädigung für die Kosten der einzelnen Auskunftserteilungen beschlossen. Eine Entschädigung für die Anschaffungskosten gibt es allerdings weiterhin nicht. Das Verwaltungsgericht Berlin hat diese Frage dem Bundesverfassungsgericht zur Entscheidung vorgelegt und unterdessen die Verpflichtung eines Telekommunikationsdiensteanbieters zur Vorratsdatenspeicherung vorläufig ausgesetzt. Entscheidend war für das Verwaltungsgericht der Umstand, dass das Unternehmen keinen Ersatz für die Aufwendungen zur Anschaffung der zum Betrieb erforderlichen Technik erlangen könne, falls das Bundesverfassungsgericht die Kostenregelung später für nichtig erklärt.

Was ist zu tun?
Solange die zur Vorratsdatenspeicherung aufgeworfenen Fragen nicht durch den Europäischen Gerichtshof und das Bundesverfassungsgericht geklärt sind, sollten die bestehenden Regelungen restriktiv angewendet und von einer Erweiterung der gesetzlichen Zugriffsbefugnisse auf die Daten abgesehen werden.

4.3.2 Telefonieren im Strafvollzug

Eine Justizvollzugsanstalt in Schleswig-Holstein betreibt in Zusammenarbeit mit einem privaten Unternehmen ein eigens für den Justizvollzug konzipiertes Telefonsystem, über das die Gefangenen Telefongespräche führen können. Dies ist – so das Ergebnis des ULD nach mehreren Eingaben – nicht nur von Vorteil.

Gefangene machten uns auf ein Telefonsystem aufmerksam, das ein privates Unternehmen für Justizvollzugsanstalten anbietet und das auch in Schleswig-Holstein eingesetzt wird. Das Telefonsystem bietet mehrere Vorkehrungen zum **Schutz vor Missbrauch**. Die Nutzung ist nur bei einem entsprechenden Guthaben und nur unter Eingabe einer PIN möglich. Bestimmte Telefonnummern können gesperrt werden. Eine weitere Sicherung ist optional: Das Angebot kann auf eine bestimmte Anzahl von Telefonnummern beschränkt werden, die von dem Nutzer anzugeben und von der Justizvollzugsanstalt freizugeben sind – eine sogenannte Weißliste.

Außerdem ermöglicht die Software, mit der das Telefonsystem betrieben wird, **Gespräche mitzuhören**, ihren Inhalt mitzuschneiden sowie die Verkehrsdaten der einzelnen Gespräche nach unterschiedlichen Kriterien auszuwerten. Diese Funktionalitäten werfen wegen der möglichen Grundrechtseingriffe Fragen auf. Einzig das Mithören von Telefongesprächen Gefangener ist unter bestimmten Voraussetzungen ausdrücklich gesetzlich erlaubt. Für die anderen Überwachungsmaßnahmen – Gesprächsmitschnitte sowie Auswertung der Telefonverbindungen – fehlen klare gesetzliche Befugnisse.

Neben den Überwachungs- und Auswertefunktionen des Telefonsystems haben wir das Zusammenspiel zwischen der Justizvollzugsanstalt und dem **privaten Anbieter** kritisch beleuchtet. Die vorgefundene Situation ist aus Datenschutzsicht nicht akzeptabel: Sämtliche Daten, die beim Betrieb des Telefonsystems anfallen – also die Bestandsdaten der Nutzer, die bei einzelnen Gesprächen anfallenden Verkehrsdaten sowie im Fall der Aufzeichnung von Gesprächen die Mitschnitte –, sind auf Servern des privaten Anbieters gespeichert. So ist dem privaten Unternehmen ein Zugriff auf alle, teilweise sehr sensiblen Daten möglich. Dies wird weder gesetzlichen Anforderungen noch der tatsächlichen Verantwortung der Justizvollzugsanstalt für die Verarbeitung der Telefondaten der Gefangenen gerecht. Die Justizvollzugsanstalt hat dies erkannt und den Anbieter aufgefordert, das System zu ändern.

Was ist zu tun?
Die Justizvollzugsanstalt sollte unsere Hinweise umsetzen. Das Verfahren muss datenschutzgerecht gestaltet werden. Gelingt dies, so kann die Lösung als Vorbild für datenschutzkonformes Telefonieren in anderen Anstalten dienen.

4.3.3 Vernichtung von Gefangenenpersonalakten – Eine lästige Pflicht?

Ein Strafgefangener setzte sich erfolgreich gegen die Nutzung von alten Gefangenenakten zur Wehr. Diese waren wegen Umbauarbeiten, krankheitsbedingter Personalengpässe und Ähnlichem nicht fristgerecht vernichtet worden. Sie standen weiterhin zur Gefangenenvollzugsplanung zur Verfügung.

Ein Strafgefangener informierte uns über offen auf dem Schreibtisch des Abteilungsleiters in der Justizvollzugsanstalt (JVA) liegende Vollzugsakten, die jeder zur Kenntnis erlangen könne. Die Akten seien zum Teil älter als zehn Jahre. Das ULD stellte fest, dass in der Tat **Gefangenenpersonalakten aus den Jahren 1994/1995** bei der Vollzugsplanung in Gesprächen mit dem Gefangenen genutzt wurden. Die Informationen aus der Akte seien aber nach Darstellung der JVA nicht in die aktuelle Vollzugsplanung einbezogen worden, da der Betroffene über Details seiner früheren Inhaftierung freiwillig berichtet habe.

Bei den Akten aus den Jahren 1994/1995 handelte es sich um Unterlagen, die von einer anderen JVA aus Schleswig-Holstein, in der der Häftling früher einmal einsaß, übersandt worden waren und bereits im Jahr 1996 zur Vernichtung anstan-

den. Diese sei „wegen in der Vollzugsanstalt durchgeführten Hochbau-, Umbau- und baulichen Erweiterungsmaßnahmen, verbunden mit einer massiven Arbeitsbelastung auch der Verwaltungsmitarbeiter, verbunden mit einem verhältnismäßig hohen Krankheitsstand in diesem Bereich“ für die Jahrgänge 1990 bis einschließlich 1997 unterblieben. Die Aufbewahrungsbestimmungen verlangen bei Gefangenenpersonalakten eine **Vernichtung nach zehn Jahren**.

Die unterlassene Vernichtung verstieß gegen die Aufbewahrungsbestimmungen; die Übermittlung der zu vernichtenden Akten an eine andere JVA war ein Verstoß gegen den Erforderlichkeitsgrundsatz, was wir beides beanstandeten. Kritisiert haben wir dabei auch, dass der Inhalt der Unterlagen durch Bedienstete der JVA zur Kenntnis genommen und der Zugang zu diesen Unterlagen nicht durch geeignete technische und organisatorische Maßnahmen verhindert wurde. Wir empfahlen geeignete **Maßnahmen zur Sicherstellung** der gesetzeskonformen Nutzung der Gefangenenpersonalakten und deren fristgerechten Vernichtung. Die Mitarbeiterinnen und Mitarbeiter wurden durch eine Hausverfügung der JVA aus dem gegebenen Anlass u. a. auf die strikte Einhaltung der Aufbewahrungsbestimmungen für Akten verpflichtet. Im Februar eines jeden Jahres soll der Leitung über die erfolgte Vernichtung der entsprechenden Unterlagen – unter Beifügung des Vernichtungsprotokolls – Bericht erstattet werden.

Was ist zu tun?
Die Vernichtungsbestimmungen für Akten müssen konsequent umgesetzt werden.

4.3.4 Kieler Sicherheitskonzept Sexualstraftäter (KSKS)

Verurteilte Sexualstraftäter können bei Verurteilung auf Bewährung oder nach ihrer Entlassung aus der Haft rückfallgefährdet sein. Um vor solchen Gefahren zu schützen, sollen Justiz und Polizei enger zusammenarbeiten. Der hierfür erforderliche Informationsfluss ist im Kieler Sicherheitskonzept Sexualstraftäter geregelt.

Die gemeinsame **Allgemeine Verfügung** des Ministeriums für Justiz, Arbeit und Europa, des Innenministeriums und des Ministeriums für Soziales, Gesundheit, Familie, Jugend und Senioren verpflichtet die Stellen des Justiz- und Maßregelvollzugs sowie Staatsanwaltschaften, Gerichte, Führungsaufsichtsstellen und Bewährungshelfer, Informationen über rückfallgefährdete Sexualstraftäter an eine beim Landeskriminalamt (LKA) eingerichtete Zentralstelle (sogenannte KSKS-Zentralstelle) zu übermitteln – mit einem Formular, in das bestimmte Angaben zu dem Verurteilten sowie zu Kontaktpersonen einzutragen sind. Ergänzend können Unterlagen beigefügt werden, nach dem Konzept z. B. auch besonders sensible ärztliche Gutachten. Die KSKS-Zentralstelle führt die von der Justiz übermittelten Daten mit vorhandenen eigenen Erkenntnissen über den Verurteilten zusammen und bewertet in eigener Zuständigkeit, ob von dem Verurteilten eine Gefahr für die öffentliche Sicherheit ausgeht. Bei einer Negativprognose informiert sie die für den Wohnsitz des Verurteilten zuständige Polizeibehörde und koordiniert die zu ergreifenden polizeilichen Maßnahmen sowie den Rückfluss der Informationen an die Justiz.

An der Erstellung des Konzepts war das ULD nicht beteiligt. Erst kurz vor dem geplanten Inkrafttreten der Allgemeinen Verfügung erfuhren wir inoffiziell von dem Vorhaben. Unsere datenschutzrechtliche Prüfung ergab, dass ein Informationsaustausch zwischen Justiz und Polizei zulässig sein kann, soweit eine **Gefahr für die öffentliche Sicherheit** vorliegt und die Informationen für den Empfänger, hier die Polizei, zur Abwehr dieser Gefahr erforderlich sind. Für KSKS bedeutet dies: Es dürfen nur Informationen über Verurteilte weitergeleitet werden, von denen mit hinreichender Wahrscheinlichkeit anzunehmen ist, dass sie erneut Sexualstraftaten begehen werden. Der Umfang der zu übermittelnden Informationen ist auf das zur Gefahrenabwehr erforderliche Maß zu beschränken. Dies ist insbesondere im Zusammenhang mit ärztlichen Gutachten und ähnlich sensiblen Informationen zu beachten. Würden sämtliche in der Justiz vorhandenen Unterlagen über den Verurteilten an die KSKS-Zentralstelle übermittelt und dort mit polizeilichen Informationen zusammengeführt, dann entstünde eine hochsensible umfassende Sammlung aller zu dieser Person bei Polizei und Justiz verfügbaren Informationen.

Eine ernsthafte Auseinandersetzung mit der Frage, für welche konkreten Zwecke diese Daten verwendet werden, ob und inwieweit diese Daten für **diese Zwecke erforderlich** sind bzw. ob es zu dem vorgesehenen Verfahren datensparsamere Alternativen gibt, lässt das Konzept leider vermissen. Die Erforderlichkeit der Übermittlung ist in der Allgemeinen Verfügung für alle Informationen nicht nachvollziehbar dargelegt, deren weitere Verwendung durch die Polizei ist nur grob beschrieben. So verbleiben erhebliche Zweifel an der Verhältnismäßigkeit des Verfahrens. Im Hinblick auf den Personenkreis, über den die Zentralstelle informiert werden soll, den Umfang der zu übermittelnden Daten und weitere einzelne Punkte ist KSKS überarbeitungsbedürftig.

Der Umgang mit den personenbezogenen Daten bei der KSKS-Zentralstelle und den gegebenenfalls einzubindenden Polizeidienststellen ist im Konzept bislang nur grob umrissen. Die **Einzelheiten der Datenverarbeitung**, etwa die Frage, ob hierfür, wie in einigen anderen Ländern, eine Datei errichtet werden soll, werden noch gesondert zu klären sein.

Was ist zu tun?
Das Meldeverfahren nach dem Kieler Sicherheitskonzept Sexualstraftäter sowie dessen Regelung in der Allgemeinen Verfügung sollten an die Empfehlungen des ULD angepasst werden. Bei der Weiterentwicklung des Konzepts ist das ULD zu beteiligen.

4.3.5 Regelmäßige HIV-Infektionsmeldung über Gefangene für die Justiz?

Bei Vorführungen im Strafprozess kommen Justizwachtmeister regelmäßig mit Gefangenen in Kontakt. Die Angst vor einer Ansteckung mit dem HI-Virus ist groß – doch ist die Information über eine HIV-Infektion eines Gefangenen ein tauglicher Schutz?

Um **Justizwachtmeister schützen** zu können, wollen die Gerichte vor den Vorführungen durch die Justizvollzugsanstalten über HIV-infizierte Gefangene informiert werden. Eine entsprechende Mitteilungspraxis wurde vor einigen Jahren eingestellt. Der Forderung der Gerichte nach Wiedereinführung dieser regelmäßigen Mitteilungen kommt das Ministerium für Justiz, Arbeit und Europa aufgrund datenschutzrechtlicher Bedenken nicht nach. Wir konnten dem Ministerium beipflichten.

Wie generell gilt auch hier, dass die zu übermittelnde Information für einen bestimmten Zweck erforderlich sein muss. Zweck der Übermittlung ist die Abwehr von Gefahren für die Gesundheit der Justizwachtmeister. Um eine Ansteckung mit dem HI-Virus zu vermeiden, ist eine Vorabinformation über solche Infizierungen nicht erforderlich. Den Justizvollzugsanstalten (JVA) selbst sind nicht zwangsläufig alle Fälle von HIV-Infektionen bei Gefangenen bekannt. Die Untersuchung ist – da für HIV-Infektionen und Aidserkrankungen keine Meldepflicht nach dem Infektionsschutzgesetz besteht – freiwillig. Es ist nicht gewährleistet, dass jeder Gefangene auf eine HIV-Infektion untersucht und die Anstaltsleitung über das Ergebnis informiert wird, sodass regelmäßige Mitteilungen der JVA an die Gerichte lückenhaft bleiben. Bei Personen, für die keine Mitteilung vorliegt, müsste weiterhin von einem Infektionsrisiko ausgegangen werden. Es führt so kein Weg daran vorbei, in jedem Fall die erforderlichen Schutzmaßnahmen, wie etwa das Tragen von Handschuhen, zu ergreifen. Die Kenntnis einer konkreten Ansteckungsgefahr, der durch **übliche Sicherheitsmaßnahmen** begegnet werden kann, ist nicht erforderlich.

Gegen eine regelmäßige Mitteilung von HIV-Infektionen spricht zudem, dass nicht von jedem HIV-Infizierten eine Ansteckungsgefahr ausgeht. Ein Infizierter, der verantwortungsbewusst mit seiner Infektion umgeht, stellt kein höheres Risiko dar als ein Nichtinfizierter. Würde **unterschiedslos über jede bekannte HIV-Infektion** berichtet, bedeutete dies, allen Gefangenen generell ein potenziell gefährdendes Verhalten und einen unverantwortungsvollen Umgang mit ihrer Infektion zu unterstellen.

Was ist zu tun?
Regelmäßige Mitteilungen an die Gerichte über alle bekannten HIV-Infektionen von Gefangenen sollten wie bisher unterbleiben.

4.3.6 „Freiwillige“ Rechnerdurchsuchung durch Interessenverband

Erneut hat die Polizei auf Anregung der Staatsanwaltschaft in einem Ermittlungsverfahren wegen Verdachts illegaler Downloads urheberrechtlich geschützter Dateien einen Interessenverband von Rechteinhabern mit der Auswertung eines Laptops beauftragt.

Im letzten Tätigkeitsbericht hatten wir über einen Fall berichtet, in dem ein Interessenverband von Rechteinhabern aus der Unterhaltungsindustrie einen Computer zur Auswertung auf Urheberrechtsverstöße erhalten hatte (30. TB, Tz. 4.3.3). Auch in einem neuen aktuellen Fall wurden dem Interessenverband nicht nur einzelne „verdächtige“ Dateien, sondern der gesamte Rechner übergeben, auf dem sich neben eventuell illegalen Musik- oder Filmdateien **zahlreiche private Dateien** der Betroffenen befanden.

Die Übermittlung im ersten Fall hatten wir beanstandet. Es fehlte hierfür die gesetzliche Grundlage. Die kreative Reaktion von Staatsanwaltschaft und Polizei auf unsere damalige Beanstandung erlebten wir bei der Prüfung des vorliegenden Falls: Die Übermittlung wurde auf eine **Einwilligung** gestützt. Der Laptop wurde von der Polizei bei einer Wohnungsdurchsuchung sichergestellt. Während der Durchsuchung hatte die Betroffene eine Erklärung unterzeichnet, in der sie sich mit der Übergabe des Laptops an und dessen Durchsuchung durch den Interessenverband einverstanden erklärte.

Eine Erklärung in einer solchen Situation ist keine wirksame Einwilligung bezüglich der Datenverarbeitung, da sie freiwillig erteilt sein muss. Es scheint ausgeschlossen, dass eine überlegte und freie Entscheidung in der Situation einer Wohnungsdurchsuchung und Sicherstellung privater Gegenstände und Daten getroffen werden kann. Von Freiwilligkeit kann hier keine Rede sein. Der Fall zeigt erneut, wie öffentliche Stellen Maßnahmen der Datenerhebung und -verarbeitung auf eine Einwilligung des Betroffenen stützen, wenn die gesetzliche Befugnis fehlt. Dies ist insbesondere in der klassischen Eingriffsverwaltung sehr heikel. Das Verhältnis zwischen Staat und Bürger ist hier nicht – wie grundsätzlich im privaten Bereich – von Vertragsfreiheit und einer Gleichrangigkeit der Parteien geprägt. Daher kommt der gesetzlichen Festlegung von behördlichen Aufgaben und Befugnissen eine besondere Bedeutung zu. Deren Voraussetzungen und Grenzen müssen – gerade bei der Erhebung und Verarbeitung von personenbezogenen Daten – durch Gesetz klar geregelt sein. Es bedarf einer strengen Prüfung, ob die Verarbeitung für die Erfüllung der gesetzlichen Aufgaben erforderlich ist. Die Grundsätze des **Gesetzesvorbehalts** und der Verhältnismäßigkeit können nicht durch eine – zumeist im Hinblick auf ihre Freiwilligkeit zweifelhafte – Einwilligung des Betroffenen unterlaufen werden.

Was ist zu tun?
Die Verarbeitung personenbezogener Daten in der Eingriffsverwaltung muss sich streng am Erforderlichkeitsprinzip orientieren. Einwilligungen sind in diesem Bereich kein probates Mittel, um fehlende gesetzliche Befugnisse zu kompensieren.

4.4 Verkehr

4.4.1 Kontrollen von Kopfstellen der Kfz-Zulassungs- und Fahrerlaubnisbehörden

Nach der Herausgabe von Hinweisen für den ordnungsgemäßen Betrieb der Kopfstellen prüften wir die Umsetzung bei vier Kreisverwaltungen. Unterstützt wurden wir dabei vom IT-Sicherheitsbeauftragten des Kraftfahrt-Bundesamtes (KBA).

Die technisch-organistorischen Vorgaben für die Schnittstelle zwischen kommunalen Behörden und KBA haben wir gemeinsam mit dem KBA herausgegeben (30. TB, Tz. 4.4.2). Unsere Prüfungen ergaben, dass die Datensicherheit der Computer, die die Kommunikation der Kfz-Zulassungsbehörden und der Fahrerlaubnisbehörden mit dem KBA ermöglichen, bei drei von vier Behörden dem geforderten Stand der Technik und den Vorgaben der Hinweise entsprach. Lediglich eine Kreisverwaltung gab diesbezüglich Anlass zur Beanstandung. Ein Problem trafen wir allerdings bei allen vier Stellen an: Die **Protokolldaten**, die zum Nachweis der Kommunikation zwischen den genannten Stellen und dem KBA erforderlich sind, wurden nicht revisionssicher, d. h. nicht unveränderbar gespeichert. Alle Stellen haben uns mitgeteilt, dass sie diesen Mangel zwischenzeitlich abgestellt haben.

Die Kontrollen bestätigten unsere Meinung, dass **gesetzliche Regelungen notwendig** sind, die genaue Anforderungen an die sichere und nachweisbare Übermittlung personenbezogener Daten zwischen den genannten Stellen festlegen. Selbstverpflichtungserklärungen der für die Verarbeitung von Kfz-Halterdaten und Fahrerlaubnisinhaberdaten zuständigen Stellen gegenüber dem KBA reichen nicht aus.

Was ist zu tun?
Die Datenschutzbeauftragten des Bundes und der Länder haben den zuständigen Fachministerien von Bund und Ländern Vorschläge für gesetzliche Regelungen unterbreitet. Es liegt nun an diesen, diese Vorschläge zügig umzusetzen. Die Datenschutzbeauftragten bieten hierfür ihre konstruktive Zusammenarbeit an.

4.4.2 Fachaufsicht über Kfz-Zulassungsbehörden weiter auf Tauchstation

Das Verkehrsministerium betrachtet sich weiterhin als nicht zuständig für die notwendigen fachaufsichtlichen Hinweise und Weisungen gegenüber den Kfz-Zulassungsbehörden und den Fahrerlaubnisbehörden. Der Schwarze Peter soll dem Innenministerium zugespielt werden.

Zur Erinnerung: Wir hatten das Verkehrsministerium des Landes gebeten, die von uns gemeinsam mit dem Kraftfahrt-Bundesamt erarbeiteten Hinweise zur Datensicherheit der Kopfstellen der Kfz-Zulassungsbehörden und der Fahrerlaubnisbehörden durch Erlass an diese Stellen weiterzugeben. Wir erhielten zunächst die für uns erstaunliche Antwort, dass dies nicht in der Zuständigkeit des Verkehrs-

ministeriums läge, weil es sich um eine kommunalaufsichtliche Angelegenheit handele. Die Antwort des Verkehrsministeriums auf unseren daraufhin verfassten Beitrag im letzten Tätigkeitsbericht (30. TB, Tz. 4.4.2) gegenüber dem Landtag offenbarte uns eine seltsame Arbeitsteilung. Sie führt aus, dass „der Datenschutz nicht der **straßenverkehrsrechtlichen Fachaufsicht** unterliegt, auch dann nicht, wenn die Datenschutzbestimmungen im Straßenverkehrsgesetz (StVG) … enthalten sind". Da keine straßenverkehrsrechtlichen Mängel dargelegt worden wären, sei das Verkehrsministerium nicht zuständig. Diese Haltung ist neu. Das Ministerium hatte bisher das ULD immer wieder zu datenschutzrechtlichen Fragestellungen konsultiert, zuletzt anlässlich der Ausgestaltung des Modellversuchs „Begleitetes Fahren ab 17".

Das Ministerium weigert sich zu erkennen, dass die Datenverarbeitung der Straßenverkehrsbehörden auf straßenverkehrsrechtlichen Vorschriften beruht. Kfz-Zulassungsvorgänge und Fahrerlaubniserteilungen sind **untrennbar verbunden** mit personenbezogener Datenverarbeitung. Der straßenverkehrsrechtliche Zusammenhang ist nicht zu leugnen. Wir gehen davon aus, dass die Zulassung von Kopfstellen in den Bund-Länder-Fachausschüssen besprochen wird. An der Entscheidung für die Einführung war das Verkehrsministerium beteiligt. Dies ist zudem unstreitig für Fragen der Verfolgung von Ordnungswidrigkeiten zuständig – auch hier geht es um Verwaltungsverfahrensfragen. Fachbezogene Datenschutzfragen sind von der für dieses Rechtsgebiet zuständigen Fachaufsichtsbehörde zu beantworten. In anderen Rechtsbereichen haben die dort zuständigen Ministerien kein Problem, sich solcher Fragen anzunehmen.

Hätte das Verkehrsministerium recht, müsste sich das **Innenministerium** zukünftig mit allen in Kommunen auftretenden Datenschutzfragen in sämtlichen Fachbereichen befassen. Es bedürfte dort somit des Vorhaltens einer zusätzlichen Fachkompetenz. Der Amtsschimmel wiehert. Das sollte nicht sein.

Was ist zu tun?
Das Verkehrsministerium muss umgehend wieder zu seiner Praxis der datenschutzrechtlichen Fachaufsicht zurückkehren.

4.4.3 Update: Anbindung Fahrerlaubnisbehörden – Kraftfahrt-Bundesamt (KBA)

Bund und Länder reagieren zögerlich auf die Forderung der Datenschützer, die mit der Online-Anbindung der Fahrerlaubnisbehörden an das KBA einhergehende neue Qualität der zentralen Verarbeitung der Fahrerlaubnisinhaberdaten rechtlich und technisch datenschutzkonform zu gestalten.

In den beiden letzten Jahren (29. TB, Tz. 4.4.2; 30. TB, Tz. 4.4.1) berichteten wir über die Zuleitung eines **Gutachtens der Konferenz der Datenschutzbeauftragten** an das Bundesministerium für Verkehr, Bau und Stadtentwicklung (BMVBS) zu rechtlichen und technischen Fragen, die mit der Online-Anbindung der Fahrerlaubnisbehörden an das KBA zu beantworten sind.

Erst auf nachhaltiges Drängen des Bundesbeauftragten war das BMVBS bereit, das Gutachten zu besprechen. Es verwies auf die **Zuständigkeit der Länder**, wenngleich die personenbezogene Datenverarbeitung der Fahrerlaubnisbehörden und der Kfz-Zulassungsbehörden bundesrechtlich geregelt ist. Als wir uns an die Verkehrsministerkonferenz wandten, wurden wir von dieser auf die Zuständigkeit des Bundes verwiesen. Erst danach konnten wir die in unserem Gutachten aufgezeigten Defizite dem zuständigen Bund-Länder-Fachausschuss vortragen. Zu unserer Überraschung war den Vertretern der Länder unser Gutachten nicht bekannt, obwohl wir den Bund seinerzeit ausdrücklich gebeten hatten, dieses an die Länder zu verteilen. Das BVMBS versuchte, sich weiterhin aus seiner Verantwortung zu stehlen, und übertrug die Initiative für Vorschläge zur Änderung gesetzlicher Regelungen an das KBA. Dies ist insofern zielführend, als das KBA wegen seiner Kenntnisse um die Datenverarbeitungsvorgänge die nötige Kompetenz vorweist. Wir erfuhren, dass das KBA bereits Vorschläge gemacht hatte, die zwar dem BMVBS bekannt waren, nicht aber dem Bundesbeauftragten und dem ULD als Leitung der Unterarbeitsgruppe der Datenschutzbeauftragten, obwohl wir immer signalisiert haben, an einer engen und konstruktiven Zusammenarbeit interessiert zu sein. Durch die zögerliche Herangehensweise des Bundes ist nach einem Jahr bezüglich der notwendigen Änderungen im Straßenverkehrsrecht immer noch nichts erreicht, um Rechtsverbindlichkeit und Sicherheit der für Jahrzehnte beim KBA gespeicherten Daten der Fahrerlaubnisinhaber zu gewährleisten.

Was ist zu tun?
Bund und Länder sollten schnellstmöglich den Dialog mit den Datenschutzbeauftragten aufnehmen und eine Abstimmung hinsichtlich des Regelungsrahmens für die Kommunikation Fahrerlaubnisbehörden – KBA anstreben.

4.5 Soziales

4.5.1 Anforderung von Kontoauszügen – Bundessozialgericht bestätigt ULD

Die Frage, ob, in welchem Umfang und für welchen Zeitraum Antragsteller verpflichtet sind, ihre Kontoauszüge bei Sozialleistungen im Amt vorzulegen, ist seit Jahren ein Dauerkonflikt. Das Bundessozialgericht bestätigte nun die vom ULD über Jahre vertretene Position.

Wer Sozialleistungen wie Arbeitslosengeld II oder Sozialhilfe beantragt, muss seine finanzielle und wirtschaftliche Situation darlegen. Der Antragsteller ist verpflichtet, alle erforderlichen Angaben zur Feststellung von Einkommen, Vermögen und Bedarf zu machen. Um die gemachten Angaben auf Vollständigkeit und Richtigkeit zu prüfen, darf die Behörde unter Berufung auf die **Mitwirkungspflicht des Antragstellers** grundsätzlich die Vorlage von Kontoauszügen fordern. Wer dem nicht nachkommt, muss damit rechnen, dass die begehrte Leistung versagt wird.

Allerdings gilt diese Form der Mitwirkungspflicht **nicht uneingeschränkt**. Schon im November 1998 hatten wir in einer Veröffentlichung im Amtsblatt unsere Auffassung zu den Grenzen der Vorlagepflicht von Kontoauszügen dargelegt

(21. TB, Tz. 4.7.4). Das Bundessozialgericht bestätigte nun in einer Entscheidung vom September 2008 die vom ULD und anderen Datenschutzbeauftragten vertretene Auslegung:

- Die Vorlage von Kontoauszügen darf verlangt werden bei der erstmaligen Beantragung von Leistungen, bei Stellung eines Folgeantrages und ansonsten, wenn konkrete Fragen zur oder Zweifel an der Hilfebedürftigkeit nicht anderweitig geklärt werden können.
- Die Aufforderung ist grundsätzlich nur für einen Zeitraum der letzten drei Monate verhältnismäßig.
- Die Schwärzung einzelner Buchungstexte – nicht der Beträge – von Sollbuchungen darf erfolgen, wenn die Informationen über den Zahlungsempfänger sensible Daten über politische, weltanschauliche oder religiöse Vorlieben offenbaren würden, etwa Beiträge für Gewerkschaften, politische Parteien, Religionsgemeinschaften.
- Das Amt ist verpflichtet, den Antragsteller auf die Möglichkeit der Schwärzung hinzuweisen.
- Die vorgelegten Kontoauszüge dürfen nur in Kopie zur Akte genommen werden, soweit diese leistungsrelevante Angaben enthalten.

Nähere Informationen dazu finden sich in den „**Gemeinsamen Hinweisen** zur datenschutzgerechten Ausgestaltung der Anforderung von Kontoauszügen bei der Beantragung von Sozialleistungen der Landesbeauftragten für den Datenschutz der Länder Berlin, Brandenburg, Hamburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und Schleswig-Holstein“ (30. TB, Tz. 4.5.2).


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

Was ist zu tun?
Die Mitarbeiterinnen und Mitarbeiter der Träger der Leistungsverwaltung nach dem SGB II müssen geschult werden, damit nur in dem aufgezeigten Umfang die Vorlage von Kontoauszügen verlangt wird, diese nicht in jedem Fall kopiert und Antragsteller auf das Recht der Schwärzung hingewiesen werden.

4.5.2 Wenn Mitarbeiter in Behördenrechnern privat recherchieren können

Die Daten aller Empfänger von Arbeitslosengeld I und II werden auf zentralen Rechnern der Bundesagentur für Arbeit (BA) gespeichert. Die Mitarbeiter in den Agenturen, ARGEn und JobCentern haben Zugriff auf sensibelste Daten, z. B. Bankverbindungen oder Gesundheitsangaben. Die BA will hieran nichts ändern – was fatale Folgen hat.

Der in der **bundesweiten Datenzugriffsmöglichkeit** liegende Rechtsverstoß ist schon lange bekannt (28. TB, Tz. 4.5.1).

- **Kurz einmal die neue Freundin checken**

Blind Date? Nicht für Mitarbeiter der ARGEn! Eine junge Frau staunte nicht schlecht, als ihr neuer Freund sie auf so manch bislang gut gehütetes Geheimnis ansprach. Dieser hatte über sie in den Datenbeständen der BA recherchiert und wusste bestens Bescheid über ihre Einkommens- und Familiensituation, Schul- und Berufsausbildung, mögliche Erkrankungen, Drogen, Vorstrafen usw. Für seine Nachforschungen brauchte dieser Mitarbeiter lediglich den Nachnamen der Betroffenen. Seine Vorgesetzten haben richtig reagiert und die fristlose Kündigung ausgesprochen.

- **Deutschland sucht den Superstar**

Während Dieter Bohlen noch sucht, wissen die Mitarbeiter der ARGEn schon mehr. Vermutlich hätten Thomas Godoj und Michael Hirte, Kandidaten dieser Fensehsendung, nicht so freizügig von ihrer Arbeitslosigkeit erzählt, wenn sie geahnt hätten, wie viele Mitarbeiterinnen und Mitarbeiter in den ARGEn ihre Daten anschauen würden. Unter der Hand wurde uns geschildert, dass weit über 10.000 Zugriffe auf ihre Datensätze zu verzeichnen waren.

- **Neues Personal? Erst mal recherchieren!**

Wovon so mancher private Arbeitgeber träumt, ist für ARGEn möglich. Bei den ARGEn, wo Zigtausende Mitarbeiter tätig sind, werden immer wieder Stellen frei. Wer sich auf eine dieser freien Stellen bewirbt, muss offenbar damit rechnen, dass nicht nur seine Bewerbungsunterlagen durchgeschaut werden. In einem Fall konnten wir nachweisen, dass der für die Personalauswahl zuständige Mitarbeiter im Datenbestand der BA recherchiert hatte. So bleibt nichts verborgen. Zu allem Überfluss wurde nach Abschluss des Auswahlverfahrens auch noch die für ihn zuständige Agentur für Arbeit unterrichtet. Die Bemerkung „So wird der Bewerber nie eine Stelle bekommen“ brachte den Bewerber in arge Verlegenheit.

- **Infos über deinen Nachbarn? Dann frage doch das Arbeitsamt!**

Zu jedem richtigen Nachbarschaftstreit gehören falsche Anschuldigungen, Häme und Beleidigungen. Gut, wenn man da auf die freundliche Unterstützung eines Arbeitsamtes oder einer ARGE zurückgreifen kann. Von Balkon zu Balkon wurde die junge Frau von ihrem Nachbarn beschimpft. „Zu faul zum Arbeiten und jetzt bekommt sie auch noch Hartz IV“, wurde da gegrölt. Dass dieser „freundliche“ Nachbar sein Wissen von einem Bekannten hatte, der zufällig bei einer ARGE arbeitet, konnte jedoch nicht nachgewiesen werden. Lapidar wurde uns von der ARGE mitgeteilt, dass lesende Zugriffe auf die Datenbestände nicht protokolliert würden; der Vorwurf konnte nicht bestätigt werden.

Was ist zu tun?
Solange die BA den ARGEn keine datenschutzgerechten Verfahren zur Verfügung stellt, müssen diese durch organisatorische Vorkehrungen sicherstellen, dass Mitarbeiter ihre Befugnisse nicht überschreiten. Vertrauen ist gut, Kontrolle ist besser. Lesende Zugriffe müssen protokolliert und regelmäßig ausgewertet werden.

4.5.3 Wenn Mitarbeiter von Hartz-IV-Behörden einfach zu viel wissen wollen

Nicht jede Frage, die anlässlich der Beantragung von Arbeitslosengeld II gestellt wird, ist zulässig und muss beantwortet werden. Zu viel behördliche Neugier führt immer wieder zu „Stilblüten".

- **Schufa-Eigenauskunft?**

In einem „unbequemen" Fall wurde der Betroffene aufgefordert, eine Schufa-Eigenauskunft im Amt vorzulegen. So sollte die Existenz weiterer Konten geklärt werden. Übersehen wurde, dass eine Schufa-Eigenauskunft auch Angaben über Handyverträge, Kundenkonten bei einem Versandhandel, eidesstattliche Versicherungen, private Insolvenzverfahren, offene Forderungen, überzogene Girokonten usw. beinhalten kann. Auf unsere Nachfrage zog die Behörde ihre Aufforderung zurück.

- **Vermieterbescheinigung mit einer Unterschrift des Vermieters**

Selbstverständlich müssen die Kosten der Unterkunft nachgewiesen werden, um einen Leistungsanspruch berechnen zu können. Gemeinsam mit dem Bundesbeauftragten und den Landesbeauftragten für Datenschutz entwickelte die Bundesagentur für Arbeit (BA) datenschutzgerechte Vordrucke. Als Nachweis für die Höhe der Mietkosten ist die Vorlage des Mietvertrages vorgesehen. Einzelne ARGEn verwenden darüber hinaus eigene Vordrucke, die zusätzlich die Unterschrift des Vermieters vorsehen. Welchem Zweck dies dienen soll, ist nicht nachzuvollziehen. Der Nachteil dieses Verfahrens liegt auf der Hand: Der Vermieter erfährt so, dass sein Mieter auf Sozialleistungen angewiesen ist. Dieses Wissen können unseriöse Vermieter ausnutzen, z. B. für Mieterhöhungen oder zur Kündigung.

- **Daten von Mitbewohnern**

Nicht jede Person wohnt allein. Ist das Geld knapp, versuchen viele, Geld zu sparen, und gründen eine Wohngemeinschaft. Liegt nicht zugleich eine „eheähnliche Gemeinschaft" vor, dann ist der Wohnpartner des Antragstellers nicht verpflichtet, Angaben zu seinen persönlichen und wirtschaftlichen Verhältnissen zu machen. Auch der Antragsteller selbst ist in diesem Fall nicht verpflichtet, derartige Angaben zu seinem Wohnpartner zu machen.

- **Fragebogen „Feststellung Kindesvater"**

Da staunten auch wir nicht schlecht. Zur „Feststellung des Kindesvaters" sollten junge Mütter äußerst detaillierte Fragen beantworten. Sie wurden aufgefordert, Auskunft über Haar- und Augenfarbe, Narben, Piercings, Tattoos und über den

Alkohol- und Drogenkonsum des möglichen Kindesvaters zu geben. Es wurde nachgefragt, wann und wo sie den mutmaßlichen Kindesvater kennengelernt hatten und ob sie in der „gesetzlichen Empfängniszeit“ mit anderen Männern Geschlechtsverkehr hatten. Die ARGE klärte nicht darüber auf, ob eine Kindesmutter überhaupt verpflichtet ist, diese Angaben zu machen, und was sie mit diesen Angaben anfangen wollte. Auf unsere Nachfrage sicherte man uns zu, den Fragebogen nicht mehr zu verwenden.

- **Daten von Kunden**

Ein Selbstständiger, der Arbeitslosengeld II beantragt, muss nachweisen, wie hoch seine Einkünfte sind. Zu diesem Zweck werden in der Regel Gewinn- und Verlustrechnungen und vergleichbare Unterlagen gefordert. Angaben über die Kunden des Selbstständigen dürfen grundsätzlich nicht verlangt werden. Dies gilt auch bei der Anforderung von Kontoauszügen des Geschäftskontos.

Was ist zu tun?
Zur Feststellung des Leistungsanspruches dürfen nur die erforderlichen Daten erhoben werden. Jeder Sachbearbeiter muss entsprechend geschult sein. Vordrucke sind vor ihrer Freigabe von dem behördlichen Datenschutzbeauftragten zu prüfen.

4.5.4 eGK – die Einführung verschiebt sich weiter

Die Berichterstattung zur Einführung der elektronischen Gesundheitskarte wiederholt sich: Das Konzept ist datenschutzfreundlich; die flächendeckende Einführung verschiebt sich weiter.

Mit diesem Tenor hatten wir bereits im letzten Jahr berichtet (30. TB, Tz. 4.6.1). Ein wesentlicher **Durchbruch** ist seitdem nicht zu verzeichnen, weder hinsichtlich der Testung in der Region Flensburg noch hinsichtlich der Einführung der elektronischen Gesundheitskarte (eGK) im Echtbetrieb. Dies heißt allerdings nicht, dass nichts geschehen wäre.

In der Region Flensburg hielten die am Test teilnehmenden Ärzte die **Probleme bei der PIN-Eingabe** durch Patienten im Zusammenhang mit der Speicherung von Notfalldaten auf der Karte (30. TB, Tz. 4.6.1) für so massiv, dass im Frühjahr beschlossen wurde, den laufenden Test hinsichtlich dieser Komponente auszusetzen. Im Laufe des Jahres wurde deutlich, dass diese Probleme auch in anderen Testregionen auftraten. Das ULD hat den Beteiligten Lösungsvorschläge angeboten. Die Umsetzung einer Problemlösung ist bisher jedoch nicht ersichtlich.

Im Mai 2008 veröffentlichte die „gematik“ (30. TB, Tz. 4.6.1) ein an die breitere Öffentlichkeit gerichtetes sogenanntes White Paper, in dem die **Sicherheit der eGK** umfassend dargestellt wird. Damit reagierte die gematik auch auf die anhaltende Kritik an dem Projekt, vor allem vonseiten der Ärzte. Diese Kritik wurde vehement auf dem 111. Ärztekongress im Mai 2008 in Ulm vorgetragen, wo das

ULD versuchte, durch einen Grundsatzbeitrag die Debatte um den Datenschutz bei der Gesundheitskarte zu versachlichen.

 https://www.datenschutzzentrum.de/medizin/gesundheitskarte

Im Bericht vom letzten Jahr, zuvor und auch jüngst haben wir immer wieder darauf hingewiesen, dass ein Großteil der **Kritik an der eGK**, soweit sie das Datenschutzkonzept betrifft, sachlich falsch ist. Gleichwohl ist es den Gegnern der eGK im Berichtszeitraum weiterhin in starkem Maße gelungen, ihre Lesart in den Medien zu transportieren, was nicht weiter verwundert: Bad News are good News.

Zu einer größeren Akzeptanz soll auch eine Umstellung in der **Reihenfolge der Testung** der einzelnen Anwendungen beitragen: Der Test des sogenannten eRezepts in der Online-Version wird erst später stattfinden. Vorgezogen werden dagegen der Versichertenstammdatendienst, mit dem die Stammdaten der Versicherten auf der Karte elektronisch aktualisiert werden können, sowie vor allem der elektronische Arztbrief. Dieser hat am ehesten das Potenzial, die Ärzte von der Sinnhaftigkeit der eGK zu überzeugen, da er direkt der ärztlichen Kommunikation dient und dabei Arbeitsabläufe erleichtern kann. Nach einem Beschluss der zuständigen Gremien vom Dezember 2008 sollen auch diese beiden Dienste im Online-Rollout der Karte umgesetzt werden. Dieser ist allerdings wohl kaum vor Ende 2009 zu erwarten.

Was ist zu tun?
Die Testung und Einführung der eGK muss weiterhin den Datenschutz in den Vordergrund stellen. Die Diskussion über die eGK muss sich an den Fakten orientieren.

4.5.5 Qualitätskontrolle des Mammografie-Screenings über das Krebsregister?

Das Verfahren des Mammografie-Screenings ist inzwischen landesweit im Einsatz und verursacht kaum datenschutzrechtliche Beschwerden. Bedenklich sind aber Tendenzen zur Ausweitung des Krebsregisters für die Qualitätskontrolle beim Mammografie-Screening.

Das ULD berichtete schon über das Vorhaben, individuelle Datenabgleiche zwischen dem Krebsregister und dem Mammografie-Screening einzurichten (30. TB, Tz. 4.6.3). Mit solchen **Datenabgleichen** soll eine umfassende Qualitätskontrolle des Mammografie-Screenings ermöglicht werden. Von Interesse sind vor allem sogenannte Intervallkarzinome, die bei einzelnen Frauen zwischen zwei Screening-Terminen auftreten. Die Intervallkarzinome sind dem Krebsregister bekannt, denn die Ärzte, die diese diagnostizieren, sind verpflichtet, sie an das Register zu melden. Nun ist vorgesehen, die medizinischen Daten aus diesen Registermeldungen dem sogenannten Referenzzentrum, welchem die Überwachung der Qualitätssicherung in der jeweiligen Region obliegt, zu übermitteln. Dies soll allerdings nicht unter dem Namen der betroffenen Frau erfolgen, sondern mit einem Pseudonym.

Nach Erhalt dieser Daten soll das Referenzzentrum von der jeweiligen Screening-Einheit, also der Stelle, die die Mammografien im Screening-Verfahren durchgeführt hat, die dort zu dem Fall vorhandenen Daten einschließlich der gefertigten Röntgenaufnahmen auf Anforderung erhalten. Das Referenzzentrum soll diese Mammografien dann untersuchen und feststellen, ob das Intervallkarzinom nicht schon bei der Mammografie hätte erkannt werden können. Zur vertieften Auswertung sollen dazu, wenn möglich, zusätzliche Behandlungsunterlagen von dem Arzt angefordert werden, der das Intervallkarzinom entdeckt und pflichtgemäß an das Krebsregister gemeldet hat. Dabei sollen auch die dort gefertigten **Röntgenaufnahmen an das Referenzzentrum** übermittelt werden. Zwar ist vorgesehen, dass die Übermittlungen an das Referenzzentrum sowie die dort stattfindende Überprüfung in pseudonymisierter Form erfolgen, d. h. ohne die Nennung des Namens der betroffenen Frau. Allerdings ist eine wirksame Pseudonymisierung zurzeit kaum realisierbar, da die Systeme, in denen die Röntgenaufnahmen verwaltet werden, dies zum großen Teil nicht unterstützen und zudem die Namen der Patientinnen in Sonografien, die regelmäßig als zweite Stufe der Diagnostik gefertigt werden, auf Bildebene eingebunden sind.

Die vorgesehene Vorgehensweise ist im Entwurf zur Änderung der sogenannten **Krebsfrüherkennungsrichtlinie** des Gemeinsamen Bundesausschusses (G-BA) niedergelegt. Der G-BA ist als oberstes Gremium in der sozialen Krankenversicherung u. a. dazu berufen, Regelungen über die Leistungsansprüche der Versicherten in der gesetzlichen Krankenversicherung zu treffen. Zum Redaktionsschluss war die Richtlinie noch nicht in Kraft getreten; offenbar fehlte noch die erforderliche Genehmigung durch das Bundesgesundheitsministerium.

An dem Richtlinienentwurf ist einiges bemerkenswert. Zum einen wird nun vollständig auf die Einwilligung der Frau in die vorgesehenen Datenflüsse verzichtet. In der bisher geltenden Fassung sollte wenigstens der Zugriff auf die bei der Screening-Einheit erzeugten medizinischen Daten von der **Einwilligung der Frau** abhängen. Zum Verzicht auf diese Anforderung findet sich nun die bemerkenswerte Begründung, es sei aus Modellprojekten bekannt, dass bis zu 40 % der Teilnehmerinnen ihre Einwilligung nicht erteilen würden. Überspitzt ließe sich dieses Argument auf den Punkt bringen: Rechte werden nur gewährt, wenn sichergestellt ist, dass kaum jemand davon Gebrauch macht.

Bemerkenswert ist auch, dass die Richtlinie einen Bereich regelt, für den zumindest zweifelhaft ist, ob er überhaupt der Regelungsbefugnis des G-BA unterfällt. Typischerweise legen die Richtlinien fest, welche Behandlungsformen im System der gesetzlichen Krankenversicherung anerkannt und finanziert werden. **Eingriffe in das Recht auf informationelle Selbstbestimmung** haben eine andere rechtliche Qualität, weswegen allgemein anerkannt ist, dass sie vom Parlament in Form eines Gesetzes geregelt werden müssen. Jedenfalls für die Weitergabe von Daten und Unterlagen von den behandelnden Ärzten geht die Richtlinie auch davon aus, dass insoweit eine zusätzliche Rechtsgrundlage nach Landesrecht erforderlich ist.

Der Richtlinienentwurf **kollidiert mit den Krebsregistergesetzen** der meisten Bundesländer, so auch mit dem von Schleswig-Holstein. Nach dem Krebsregister-

gesetz ist zwar die Weitergabe von medizinischen Daten aus dem Krebsregister im Grundsatz möglich. Voraussetzung ist allerdings die Einwilligung der betroffenen Personen.

Auch wenn die Bedeutung der Qualitätskontrolle in Screening-Verfahren nachvollziehbar ist, müssen doch die Datenschutzrechte der betroffenen Personen gewahrt bleiben. So ist nicht klar, warum die **Evaluation auf der Basis der Fälle**, in denen die Frauen ihre Einwilligung erteilen, nicht ausreichend sein soll. Bei dem bisher vorgesehenen Verfahren droht eine Aushöhlung des Patientengeheimnisses, die vermieden werden sollte.

Was ist zu tun?
Die Nutzung des Krebsregisters für andere als die bisher verfolgten epidemiologischen Zwecke sollte an die Einwilligung der betroffenen Personen geknüpft werden.

4.5.6 Unzulässige Adressbeschaffung der gesetzlichen Krankenkassen

Wirtschaftsunternehmen hätten gern möglichst viele Kunden, gesetzliche Krankenkassen hätten gern möglichst viele Versicherte. Die Werbemöglichkeiten von Kassen sind aber gegenüber „normalen“ Wirtschaftsunternehmen beschränkt.

Gesetzliche Krankenkassen sind öffentliche Stellen. Der Gesetzgeber hat ihnen lediglich zugestanden, (Adress-)Daten aus allgemein zugänglichen Quellen wie z. B. Telefonbüchern zu nutzen, um **Mitgliederwerbeaktionen** durchzuführen. Nicht alle Krankenkassen wollen sich an diese Spielregel halten.

Anfang 2008 wurde uns ein Schreiben der IKK Nord bekannt, mit dem **Arbeitgeber** aufgefordert wurden, Namen, Anschriften und Geburtsdaten der Auszubildenden mitzuteilen. Lediglich die vorgefertigte Rückantwort enthielt in – sehr – kleiner Schrift den Hinweis, dass die **Auszubildenden** dieser Datenübermittlung zustimmen müssen. Ein Schelm, wer Böses dabei denkt. Auf Nachfrage wurde uns zugesichert, dass derartige Anfragen zukünftig unterbleiben und bereits gespeicherte Daten gelöscht werden.

Wenige Monate später berichtete uns ein Petent, er habe als Privatperson Post von der IKK Nord erhalten und wundere sich, woher diese Kenntnis von seiner Anschrift hatte. Die IKK teilte uns lapidar mit, die **Adressdaten potenzieller Kassenwechsler** habe sie bei einem Adresshändler erworben. Dass die nach bestimmten Selektionskriterien aufgearbeiteten Datensätze eines Adresshändlers gerade nicht öffentlich zugänglich sind und damit nicht von den Kassen zu Werbezwecken erworben werden dürfen, wollte die IKK zunächst nicht einsehen.

Wir mussten die Adressbeschaffung und -nutzung als Verstoß gegen die Vorschriften zum Sozialdatenschutz formell beanstanden. Nachdem der behördliche Datenschutzbeauftragte beteiligt wurde, gelobte der Vorstand Besserung.

Was ist zu tun?
Auch und gerade unter dem Druck von vermeintlichen wirtschaftlichen Notwendigkeiten bei den gesetzlichen Krankenkassen müssen die Vorschriften zum Sozialdatenschutz bei der Werbung neuer Mitglieder beachtet werden. Speziell selektierte Adressdatensätze von Adresshändlern dürfen nicht erworben werden.

4.5.7 Kindeswohlgefährdung – Kinderschutz braucht Datenschutz!

Auf vielen Veranstaltungen hat sich das ULD der Diskussion mit Hebammen und Kinderärzten, Mitarbeitern der Kindertagesstätten, Amtsärzten und nicht zuletzt Jugendämtern und freien Trägern der Jugendhilfe gestellt, ob datenschutzrechtliche Vorschriften den Kinderschutz behindern.

Das Ergebnis vorweg: Die bestehenden Vorschriften sind ausreichend. Aber es bestehen **große Unsicherheiten**. Wann darf ein Kinderarzt welche Daten an welche Stelle übermitteln? Auf unserer Homepage geben wir Handlungshilfen:

https://www.datenschutzzentrum.de/vortraege/20081106-koop-kinderschutz.html

Um feststellen zu können, ob tatsächlich eine Kindeswohlgefährdung vorliegt, sollte sich der Arzt zunächst – ohne dabei den Namen seiner Patienten zu nennen – mit dem Jugendamt und gegebenenfalls anderen Stellen über seine Erkenntnisse austauschen. Wenn seine Vermutung bestätigt wird, gilt es zu handeln.

Aber Vorsicht: Hebammen und Kinderärzte müssen **die berufliche Schweigepflicht** als besonderes Berufsgeheimnis beachten. Dieses soll sicherstellen, dass – im Interesse des Funktionierens unseres Gesundheitssystems – nicht nur eine qualifizierte medizinische Behandlung angeboten wird, sondern diese von den Patienten auch angenommen wird. Nur wenn ein Patient sicher sein kann, dass seine medizinischen Informationen vertraulich behandelt werden, wird er bereit sein, dem medizinischen Helfer gegenüber alle notwendigen Angaben zu seiner Erkrankung zu machen und so den Grundstein für eine erfolgreiche Behandlung zu legen.

In bestimmten Konstellationen ist die Durchbrechung der Schweigepflicht erlaubt. Derzeit existiert in Schleswig-Holstein keine eindeutige gesetzliche Befugnis zur Offenbarung von Patientendaten in Fällen von Kindeswohlgefährdung. Fehlt eine gesetzliche Regelung und sollen Informationen gleichwohl weitergegeben werden,

so kann dies durch eine **Schweigepflichtentbindungserklärung** des Patienten bzw. seines gesetzlichen Vertreters legitimiert werden. Die Bereitschaft der Eltern, den Arzt von seiner Schweigepflicht zu entbinden, ist umso größer, je deutlicher er aufzeigen kann, welche Hilfen der Familie angeboten werden können. Der Arzt muss also über die Aufgaben, Befugnisse und Möglichkeiten der Jugendämter und freien Träger der Jugendhilfe informiert sein.

Wird die Schweigepflichtentbindungserklärung nicht erteilt, kann eine **Übermittlung gesetzlich erlaubt** sein, und zwar wenn

- eine Gefahr für Leben, Leib und Freiheit vorliegt,
- die Gefahr aktuell besteht,
- die Gefahr von dem Arzt nicht anders als durch Unterrichtung einer dritten Stelle abgewendet werden kann und
- das Interesse am Kindeswohl das Interesse an der Geheimhaltung überwiegt.

In diesem Fall kann sich der Arzt auf einen **rechtfertigenden Notstand** berufen.

Abhängig vom **Einzelfall** muss geprüft werden, welche Stelle am ehesten der Familie wirklich helfen kann. Häufig wird dies das Jugendamt sein, nur selten die Polizei. Der Arzt sollte seine Überlegungen dokumentieren.

Was ist zu tun?
Die ärztliche Schweigepflicht ist ein hohes Gut und oftmals Grundlage dafür, dass sich ein Patient seinem Arzt anvertraut. Ein Arzt darf dennoch in einem begründeten Fall einer Kindeswohlgefährdung dritte Stellen, wie z. B. das Jugendamt, unterrichten.

4.5.8 Kontrollierende Einladungen zur freiwilligen Kinderuntersuchung

Im Berichtszeitraum ist das kontrollierende Einladungswesen zu den Früherkennungsuntersuchungen für Kinder im Vorschulalter angelaufen. Das Verfahren führt zu einer umfangreichen Verarbeitung personenbezogener Daten. Ein effektiver Datenschutz ist unabdingbar.

Das Land Schleswig-Holstein hat ein sogenanntes kontrollierendes Einladungs- und Meldewesen zu den von den Krankenkassen und sonstigen Kostenträgern angebotenen Früherkennungsuntersuchungen (U4 bis U9) eingeführt (30. TB, Tz. 4.5.7). Damit soll die – ohnehin schon hohe – Teilnahmequote an den Untersuchungen weiter gesteigert werden, wohlgemerkt, ohne dass die Teilnahme an den Untersuchungen selbst verpflichtend ist. Ziel ist es, mögliche Fälle von **Vernachlässigung des Kindeswohls** rechtzeitig zu erkennen, sei es bei den Untersuchungen selbst oder, wenn die Untersuchungen nicht durchgeführt werden, über nachfolgende Maßnahmen des Jugendamtes.

Das verfolgte Ziel ist selbstverständlich von hoher Bedeutung. Allerdings darf nicht außer Acht gelassen werden, dass das gesamte Verfahren die Verarbeitung personenbezogener Daten in erheblichem Umfang mit sich bringt – und dies in einem sehr sensiblen Kontext. Daher ist es wichtig, dass durchgängig **hohe Datenschutzstandards** eingehalten werden.

Das Verfahren beginnt damit, dass das Landesfamilienbüro beim Landesamt für Soziale Dienste (LAsD) die Daten über die Kinder im entsprechenden Alter sowie deren Eltern von den Meldebehörden erhält. Auf der Basis dieser Daten verschickt es Einladungen zur Teilnahme an der nächsten fälligen Untersuchung. Wird die Untersuchung durch einen Kinderarzt durchgeführt, so hat dieser die mit der Einladung verschickte Antwortkarte an das Landesfamilienbüro zurückzusenden. Geht keine Rücksendekarte ein, verschickt das Landesfamilienbüro eine Erinnerung. Wird dann weiterhin kein Eingang der Rücksendekarte festgestellt, so gibt das Landesfamilienbüro den Fall an die zuständigen Kreise und kreisfreien Städte ab. Dieser Teil des Verfahrens ist in den zugrunde liegenden gesetzlichen Vorschriften präzise geregelt; Zweifelsfragen konnten in enger Abstimmung zwischen dem LAsD und dem ULD geklärt werden. Allerdings sind immer noch nicht alle Probleme mit der erforderlichen **Übermittlung der Meldedaten an das LAsD** behoben. Einzelne Kommunen haben wegen der dort verwendeten Software im Meldeverfahren Probleme, die geforderten Daten über Kinder mit Bezug zu den Sorgeberechtigten überhaupt zu liefern. Unabhängig davon ist ein gewisser Teil der gelieferten Daten so fehlerhaft, dass Einladungen nicht verschickt werden können. Die Probleme scheinen in der Extraktion der Meldedaten aus den Originalbeständen in den Spiegeldatenbestand, der für die Lieferungen an das LAsD genutzt wird, zu liegen.

Im Gegensatz zu den Prozessen beim LAsD ist **das weitere Verfahren** bei den Kommunen nach Empfang von Meldungen über nicht wahrgenommene Untersuchungen weniger klar. Das Gesetz schreibt nur vor, dass die Kommunen „eine Beratung über den Inhalt und Zweck der Früherkennungsuntersuchung sowie die Durchführung der ausstehenden Früherkennungsuntersuchung durch eine Ärztin oder einen Arzt“ anzubieten haben. In der Praxis wird dazu das kommunale Gesundheitsamt eingeschaltet. Dieses versendet ein weiteres Anschreiben an die Eltern und bietet eine Beratung über die Bedeutung der Früherkennungsuntersuchungen an. Melden sich die Eltern daraufhin nicht bei der Kommune, wird dort der Fall an das Jugendamt weitergereicht. Dieses versucht – zum Teil mit Beteiligung des Gesundheitsamtes – mit den Eltern Kontakt aufzunehmen, wobei einem Besuch vor Ort in der Regel die briefliche und telefonische Kontaktaufnahme vorausgeht. Nach dem Gesetz „prüft das Jugendamt, ob gewichtige Anhaltspunkte für die Gefährdung des Wohls des Kindes vorliegen“.

Wir haben von Anfang an die zusätzliche Runde über die kommunalen Gesundheitsämter kritisch beleuchtet (30. TB, Tz. 4.5.7). Es liegt nicht gerade nahe, dass Eltern, die bereits eine Einladung und eine Erinnerung ignoriert haben, in den Kreisen zum Teil weite Wege auf sich nehmen, nur um sich über die Sinnhaftigkeit der Untersuchungen belehren zu lassen. Die Einbeziehung der Gesundheitsämter führt zu einer zusätzlichen Verarbeitung von personenbezogenen Daten, die als Sammlung von **Daten über „Rabeneltern“** missverstanden werden kann. Nach

den bisher vorliegenden Berichten finden sich in der Mehrzahl der Fälle harmlose Erklärungen dafür, warum keine Rücksendekarte beim LAsD eingegangen ist. Es ist wichtig, für eine nur kurze Aufbewahrung der als unkritisch abgeschlossenen Fälle zu sorgen, wobei auch sichergestellt werden muss, dass eine Verwendung der Daten für andere Zwecke ausscheidet.

Bei den Gesprächen zwischen Eltern und Jugendamt stellt sich nicht selten heraus, dass die Untersuchung durchgeführt wurde, die Rücksendekarte aber nicht abgeschickt wurde und auch nicht mehr auffindbar ist. Selbstverständlich kann durch das Vorlegen des gelben Hefts, in dem die Untersuchungen vermerkt werden, die Durchführung der Untersuchung nachgewiesen werden. Allerdings besteht keine Pflicht für die Eltern, dem Jugendamt die Teilnahme an der Untersuchung, z. B. durch Vorlage des gelben Heftes, nachzuweisen. Schließlich gibt es nach wie vor überhaupt **keine Pflicht zur Teilnahme** an den Untersuchungen. Das Jugendamt ist gesetzlich zum Tätigwerden verpflichtet, muss sich aber darauf beschränken, durch eine Bestandsaufnahme festzustellen, ob Anzeichen für eine Kindeswohlgefährdung vorliegen. Ist dies nicht der Fall, so kann es keine weiteren Schritte unternehmen, um doch an die Information zu gelangen, ob die Untersuchungen wahrgenommen wurden oder nicht. Diese Information sollte für das Jugendamt auch nicht die erste Quelle sein, um Kindeswohlgefährdungen zu erkennen.

Eine Bestätigung der Durchführung der Untersuchung könnte auch durch den Arzt erfolgen. Weder das Jugendamt noch das Gesundheitsamt sind aber ohne Weiteres berechtigt, bei einem – z. B. von den Eltern im Gespräch erwähnten – **Kinderarzt nachzufragen**, ob die Untersuchung stattgefunden hat. Eine solche Auskunft darf der Arzt nur geben, wenn die Eltern ihn diesbezüglich ausdrücklich von der Schweigepflicht entbunden haben. Gemäß den gesetzlichen Vorschriften trifft den Arzt nur die Pflicht zur Rückmeldung bestimmter Daten an das LAsD mittels der Rücksendekarte. Nur in diesem Punkt ist seine Schweigepflicht durchbrochen; dies gilt jedoch nicht gegenüber den kommunalen Stellen.

Die **Entbindung von der Schweigepflicht** zur Bestätigung der Teilnahme an den Früherkennungsuntersuchungen durch den Kinderarzt ist in der Regel schriftlich zu erklären. Kommt es nicht zu einem direkten Kontakt zwischen Jugendamt und Eltern, kann die Entbindungserklärung aus praktischen Gründen ausnahmsweise telefonisch abgegeben werden. Das Jugendamt hat darüber einen Aktenvermerk anzufertigen. Genügt dem Arzt auf die Anfrage des Jugendamtes hin die mündliche Erklärung nicht, so kann er sich selbst bei den Eltern das tatsächliche Vorliegen der Erklärung, z. B. telefonisch, bestätigen lassen. Ist er dazu nicht bereit, so muss das Jugendamt letztlich eine von den Eltern unterschriebene Erklärung vorlegen.

Was ist zu tun?
Die Kommunen sollten das Verfahren bei Meldungen über nicht durchgeführte Früherkennungsuntersuchungen klar regeln. Die dazu empfangenen und die im weiteren Verlauf ermittelten Daten über nicht bestätigte Verdachtsfälle sind streng zweckgebunden und müssen zeitnah vernichtet werden.

4.5.9 Bestattungsgesetz des Landes

Neuregelungen im Bestattungsgesetz verbessern den Schutz von sensiblen Daten in den Todesbescheinigungen und erleichtern die Forschung. Details müssen noch in einer Verordnung geregelt werden.

In der Informationsgesellschaft wird der Bürger ein Leben lang von der Verarbeitung seiner personenbezogenen Daten begleitet – und auch darüber hinaus: Im Bestattungsgesetz des Landes finden sich nicht nur Regelungen über Anforderungen an Friedhöfe und dergleichen, sondern auch Vorschriften, die die Erhebung von Daten im Zusammenhang mit dem Tod vorgeben. Dazu gehören die in der sogenannten Todesbescheinigung anlässlich der pflichtgemäß durchzuführenden Leichenschau erhobenen Daten. Neben der für unterschiedliche Zwecke erforderlichen bloßen Bestätigung, dass eine Person verstorben ist, enthalten die **Todesbescheinigungen** in einem sogenannten vertraulichen Teil auch medizinische Daten wie z. B. über die vermutete Todesursache oder über Vorerkrankungen. Hierbei handelt es sich streng genommen nicht um personenbezogene Daten im Sinne des Landesdatenschutzgesetzes, denn von diesem gesetzlichen Begriff werden nur die Daten von lebenden Personen umfasst. Die Leichenschau muss allerdings durch einen Arzt oder eine Ärztin durchgeführt werden; es ist anerkannt, dass die solcherart erhobenen Daten unter die ärztliche Schweigepflicht fallen.

Daraus ergaben sich rechtliche Probleme mit der geltenden Fassung des Bestattungsgesetzes. So fehlte eine Vorschrift, die vergleichbar mit der entsprechenden Regelung im LDSG die Nutzung von Daten aus der Todesbescheinigung für **Forschungszwecke** erlaubt. Außerdem war der Umgang mit den Todesbescheinigungen nicht durch Rechtsnormen geregelt, obwohl dies im Hinblick auf die Sensibilität und den Schutzbedarf der dort enthaltenen Daten erforderlich ist.

In enger Zusammenarbeit mit dem fachlich zuständigen Ministerium für Soziales, Gesundheit, Familie, Jugend und Senioren konnte das ULD dazu beitragen, dass **die nötigen Vorschriften** in das Gesetz aufgenommen wurden. Der Umgang mit den Todesbescheinigungen und insbesondere die dabei zu beachtenden Maßnahmen der Datensicherheit sollen in einer Verordnung geregelt werden; eine entsprechende Verordnungsermächtigung enthält das Gesetz. Eine neue Regelung zur Nutzung der Daten aus dem vertraulichen Teil der Todesbescheinigung erleichtert zum einen künftig Forschern den Zugang zu diesen Daten für wissenschaftliche Zwecke. Es gibt nun zudem eine klare Regelung, die den Zugang von Privaten, z. B. Angehörigen, zu diesen Daten davon abhängig macht, ob ein rechtliches Interesse besteht und schutzwürdige Interessen der Verstorbenen und ihrer Angehörigen beeinträchtigt werden.

Was ist zu tun?
Wie vorgesehen, ist vom zuständigen Sozialministerium kurzfristig die vorgesehene Verordnung zum Umgang mit den Todesbescheinigungen zu erlassen. Das ULD steht für eine fachliche Beratung bereit. Die Kreise und kreisfreien Städte werden die Verfahren in ihren Gesundheitsämtern entsprechend anzupassen haben.

4.5.10 Datenerhebungsbefugnis der Heimaufsicht

Im Bereich der Pflegeheime spielt der Datenschutz der Bewohner eine wichtige Rolle und wird nicht selten missachtet. Betreiber von Heimen entdecken den Datenschutz aber manchmal, wenn eine Kontrolle durch die Heimaufsicht ansteht. Dieser müssen aber alle relevanten Dokumente ausgehändigt werden.

Wiederholt kam es zu Eingaben, mit denen eine vermeintlich zu weit gehende Datenerhebung durch die Heimaufsicht gerügt wurde. Die bei dem Kreis oder der kreisfreien Stadt angesiedelte Heimaufsichtsbehörde hat die Aufgabe, Heime, die ältere Menschen, pflegebedürftige oder behinderte Volljährige aufnehmen, daraufhin zu überprüfen, ob sie den **Anforderungen an den Betrieb** nach dem Heimgesetz genügen. Zu diesem Zweck ist es regelmäßig erforderlich, auch in die Unterlagen über einzelne oder alle Heimbewohner Einsicht zu nehmen, so namentlich in die Pflegedokumentation. Das Gesetz schreibt vor, dass alle erforderlichen mündlichen und schriftlichen Auskünfte auf Verlangen und unentgeltlich zu erteilen sind.

So forderte die Heimaufsichtsbehörde anlässlich einer Vor-Ort-Prüfung, dass einzelne Bestandteile aus der ausschließlich in elektronischer Form geführten **Pflegedokumentation ausgedruckt** würden, damit die Behörde diese zur weiteren Prüfung mitnehmen könne. Der Leiter des Heims weigerte sich. Er meinte, die gesetzliche Pflicht zur Erteilung von Auskünften umfasse nicht die Erstellung dieser Ausdrucke. Solche ausgedruckten Unterlagen seien in ihrer Aussagekraft beschränkt, da sie nur im Gesamtzusammenhang der vollständigen elektronischen Dokumentation hinreichend gewürdigt werden könnten. Sie seien daher nicht für die Aufgabenerfüllung der Behörde erforderlich.

In einem anderen Fall wurde der Heimaufsicht sogar die Aushändigung von **Bewohnerlisten** unter Berufung auf den Datenschutz verweigert.

Das ULD stellte klar, dass die Weigerung der Vorlage bzw. des Ausdrucks von Unterlagen in beiden Fällen nicht haltbar war. Auch die verwaltungsgerichtliche Rechtsprechung hat festgestellt, dass das Gesetz den Prüfungsumfang nicht in irgendeiner Hinsicht beschränkt. Den Heimaufsichtsbehörden sollen alle notwendigen Mittel an die Hand gegeben werden, um die **Einhaltung der gesetzlichen Vorgaben** zu überprüfen. Einer effizienten Kontrolle durch die Heimaufsicht wäre der Boden entzogen, wenn es die geprüfte Stelle selbst in der Hand hätte, die Geeignetheit und Erforderlichkeit einzelner Erhebungen zu bewerten und daraus folgend die Vorlage von Unterlagen zu verweigern.

Das ULD als Datenschutzkontrollbehörde kann nicht die Ermessensausübung der Fachbehörde an sich ziehen. Es findet lediglich eine **Kontrolle der Schlüssigkeit** der zur Erforderlichkeit der Datenverarbeitung vorgebrachten Argumente statt. Da sich insoweit keine Anhaltspunkte für Zweifel ergaben, hatten die Heime die angeforderten Unterlagen vorzulegen.

Was ist zu tun?
Betreiber und Leitungen von Pflegeheimen können nicht mit dem Verweis auf den Datenschutz der Heimaufsicht die Vorlage und Aushändigung von Unterlagen im Rahmen von Prüfungen verweigern.

4.5.11 ELENA-Gesetzentwurf auf den Weg gebracht

Die Bundesregierung hat im Berichtszeitraum das Einführungsgesetz zu dem Verfahren ELENA trotz der Kritik vieler Datenschutzbeauftragter und der Bundesländer beschlossen. Damit wird einer gefährlichen Vorratsdatenverarbeitung der Weg bereitet.

Obwohl die kritischen Stimmen nicht verstummt sind, hat das Bundeskabinett im Juni 2008 den Gesetzentwurf zur Einführung des „Elektronischen Einkommensnachweises“ (ELENA) beschlossen. Damit ist ein Projekt auf den Weg gebracht, dass vom ULD und vielen anderen Datenschutzbeauftragten kritisch gesehen wird, vor allem weil es für eine große Zahl von Bürgern eine **Vorratsdatenspeicherung ihrer Einkommensverhältnisse** mit sich bringen wird, ohne dass diese Daten jemals benötigt werden (30. TB, Tz. 4.5.8; 28. TB, Tz. 4.5.2).

Das nun geplante Verfahren das von Anfang an in seiner Grundstruktur unverändert geblieben ist, ermöglicht technisch den **zentralen Zugriff auf die Daten** ohne die Kenntnis der Betroffenen. Leider hat sich das Bundeskabinett nicht dazu durchringen können, den Vorschlägen der Landesbeauftragten für Datenschutz zu folgen und ein Verfahren der individuellen Verschlüsselung dieser hochsensiblen Daten vorzusehen. Die Bundesregierung weist auf die strenge Zweckbindung der Daten hin. Erfahrungen aus der Vergangenheit in anderen Zusammenhängen veranlassen aber zur Skepsis: Sind Daten einmal vorhanden, so sind diese schnell vielfältigen Begehrlichkeiten ausgesetzt, gegen die die Betroffenen keine Abwehrmöglichkeiten haben. Viele andere Stellen, allen voran die Finanzämter, dürften an diesen Informationen ein großes Interesse haben.

Der **Bundesrat** hat in seiner Stellungnahme zu dem Gesetzentwurf deutlich gemacht, dass auch er den Entwurf datenschutzrechtlich für unzureichend hält. Da das Gesetz die Zustimmung des Bundesrates benötigt, besteht also die Hoffnung, dass es nicht in der von der Bundesregierung vorgelegten Form verabschiedet wird.

Was ist zu tun?
Das Land Schleswig-Holstein sollte sich weiterhin dafür einsetzen, das Verfahren ELENA in einer datenschutzkonformen Weise zu verändern.

4.6 Schutz des Patientengeheimnisses

4.6.1 Entwurf eines Gendiagnostikgesetzes des Bundes

Der Entwurf eines Gendiagnostikgesetzes bringt einen deutlichen Fortschritt für den Schutz von besonders sensiblen Daten. Ein Manko ist aber die komplette Ausklammerung des Forschungsbereichs.

Im August 2008 beschloss das **Bundeskabinett** den Entwurf eines Gendiagnostikgesetzes. In Teilen geht dieses Regelungsvorhaben auf einen im Jahr 2006 von der Bundestagsfraktion von Bündnis90/Die Grünen vorgelegten ähnlichen Gesetzentwurf zurück. Vor der Verabschiedung des Entwurfs hatte auch das ULD die Gelegenheit wahrgenommen, eine Stellungnahme abzugeben.

Der Gesetzentwurf regelt den Umgang mit genetischen Daten, wobei das Recht auf informationelle Selbstbestimmung betont wird. Im Hinblick auf die weitreichenden Erkenntnisse, die sich aus genetischen Daten ergeben können, hat der Einzelne nicht nur das Recht auf Zugang zu seinen genetischen Daten, sondern auch das **Recht auf Nichtkenntnis**; er darf nicht zur Kenntnisnahme seiner genetischen Disposition gezwungen werden, wenn er diese ablehnt.

Wie schon von der Rechtsprechung angenommen, soll eine genetische Abstammungsanalyse nur erlaubt sein, wenn die Personen, deren Zellmaterial untersucht werden soll, ausdrücklich eingewilligt haben. **Heimliche Abstammungsuntersuchungen** bleiben verboten.

Von hoher Bedeutung sind die Regelungen über genetische Untersuchungen im **Arbeitsverhältnis** und im Zusammenhang mit einem Versicherungsvertrag. Es wird klargestellt, dass der Arbeitgeber nicht verlangen darf, dass sich der Arbeitnehmer genetischen Untersuchungen unterwirft. Bestimmte, eng umrissene Ausnahmen sind zulässig bei arbeitsmedizinischen Vorsorgeuntersuchungen. Verboten wird auch die Verwertung von Erkenntnissen aus vorhandenen Genanalysen durch den Arbeitgeber.

Auch **Versicherungsunternehmen** sollen künftig daran gehindert werden, genetische Erkenntnisse über den Versicherungsnehmer zu erheben oder zu verwerten. Bisher gilt insoweit eine Selbstverpflichtung der Versicherungsbranche; dieses Moratorium läuft allerdings 2014 aus. Eine Ausnahme von dem Verbot soll es geben, wenn eine Versicherung mit einer sehr hohen Versicherungssumme abgeschlossen wird. Allerdings ist fraglich, ob die hierfür festgesetzte Grenze von 300.000 Euro nicht zu niedrig angesetzt ist.

Der Entwurf enhält flankierende **verfahrensmäßige Sicherungen**. Eine genetische Untersuchung zu medizinischen Zwecken darf nur durch einen Arzt vorgenommen werden. Eine zentrale Bedeutung hat auch die Beratung über die genetische Untersuchung. Teilweise sind solche Beratungen im Kontext mit genetischen Untersuchungen zwingend vorgeschrieben; bei anderen genetischen Untersuchungen soll die Beratung nur angeboten werden.

Ein vom ULD in seiner Stellungnahme hervorgehobener wesentlicher Kritikpunkt betrifft das vollständige Fehlen von Regelungen über den Umgang mit genetischen Proben und Daten zu **Forschungszwecken**. Damit bleibt ein wesentliches Feld ungeregelt und der Einzelne insoweit nur unzureichend geschützt. Dies erscheint unangemessen – gerade angesichts der weiter wachsenden Bedeutung von genetischer Forschung und namentlich der Zunahme von Biobanken, die auch genetische Daten vorhalten (Tz. 8.10).

Was ist zu tun?
Das Land Schleswig-Holstein sollte weiterhin darauf hinwirken, dass noch bestehende Defizite des Gesetzentwurfs beseitigt oder fehlende Regelungen in einer späteren Gesetzgebung ergänzt werden.

4.6.2 Versagung der Einsicht in Patientenakte beim Betriebsarzt

Jeder Patient hat ein Recht, in die vom Arzt über ihn mit seinen Gesundheitsdaten geführte Akte Einsicht zu nehmen. Dies gilt auch für Akten beim Betriebsarzt. Unerheblich ist, ob zwischen Arzt und betroffener Person ein Behandlungsvertrag besteht oder der Arzt im Auftrag des Arbeitgebers tätig wird.

Ein Arbeitnehmer wurde nach der Untersuchung durch den Betriebsarzt vom Nacht- **in den Tagdienst versetzt**. Hierdurch erlitt er Einkommenseinbußen. Nicht klar war, ob der Arzt konkrete Untersuchungsergebnisse unbefugt an den Arbeitgeber weitergegeben hatte. Der Arbeitnehmer forderte deshalb von dem Arzt umfassend Auskunft über den Inhalt seiner Patientenakte. Diese wurde ihm wiederholt verwehrt.

Immer wieder verweigern Mediziner Patienten die Einsicht in die über sie geführten Unterlagen. Dabei hat sich die höchstrichterliche Rechtsprechung in den letzten Jahren klar zugunsten der Patienten positioniert. Angaben über Anamnese, Diagnose und therapeutische Maßnahmen betreffen den Patienten unmittelbar in seiner Privatsphäre. Sein **Einsichtsrecht** darf daher nur in besonderen Ausnahmefällen beschränkt werden, beispielsweise wenn die Kenntnisnahme durch den Patienten medizinisch nicht verantwortbar ist oder wenn persönliche Notizen des Arztes betroffen sind.

Der Arbeitsmediziner rechtfertigte die Einsichtsverweigerung damit, zwischen ihm und dem untersuchten Arbeitnehmer bestehe **kein Vertragsverhältnis**. Dies ist kein Grund: Der Anspruch auf Zugang zu den Inhalten der Arztakte ist rechtlich vielfach verankert und ergibt sich nicht nur aus dem Behandlungsvertrag.

Ärzte sind bereits aufgrund des **verfassungsrechtlich gewährten Rechts** auf freie Entfaltung der Persönlichkeit sowie aufgrund der Regelungen des Datenschutzgesetzes zur vollständigen schriftlichen Auskunft verpflichtet. Der Arzt wurde vom ULD aufgefordert, dem Arbeitnehmer schriftlich über den Inhalt der Patientenunterlagen Auskunft zu erteilen.

Was ist zu tun?
Ärzte müssen dem Betroffenen unabhängig vom Bestehen eines Vertragsverhältnisses Auskunft über den Inhalt der Behandlungsunterlagen gewähren. Zweckmäßigerweise werden für den Patienten Kopien der Unterlagen angefertigt. Persönliche Notizen des Arztes dürfen geschwärzt werden.

4.6.3 Einhaltung von Sicherheitsstufen bei der Vernichtung von konventionellen Datenträgern

Ein Schredder mit Crosscut oder Streifenschnitt? Sicherheitsstufe 2, 3 oder 4? Wie sind konventionelle Datenträger mit personenbezogenen Daten, die einem besonderen Berufsgeheimnis wie der ärztlichen Schweigepflicht unterliegen, zu vernichten?

Ausführliche **Antworten** hierzu finden sich in unserem Beitrag „Datenschutzgerechte Entsorgung von Patientenunterlagen“:


www.datenschutzzentrum.de/material/themen/gesund/entsorg.htm

Vorweg folgende Anmerkung: Der beste Schredder nützt wenig, wenn die zu vernichtenden Unterlagen über Wochen hinweg in einem Pappkarton irgendwo für jedermann frei zugänglich gesammelt werden. Auch diese Unterlagen sind bis zu ihrer endgültigen Vernichtung **sicher aufzubewahren**.

Wird ein **Fremdunternehmen** mit der Vernichtung beauftragt, muss sichergestellt werden, dass die Mitarbeiter dieses Dienstleisters keine Kenntnis von den Daten nehmen (können). Dies kann bedeuten, dass ein Mitarbeiter der Arztpraxis die Unterlagen von ihrer Übergabe bis zu ihrer endgültigen Vernichtung begleitet.

Wer die Vernichtung selbst vornehmen möchte, muss darauf achten, dass die nach der Vernichtung überbleibenden Materialteilchen **keine lesbaren Informationen** mehr enthalten. Entscheidend ist hierbei die Größe der Materialteilchen. Wer sichergehen will, achtet darauf, dass der Schredder eine Vernichtung nach Sicherheitsstufe 4 garantiert.

Was ist zu tun?
Bei der Vernichtung von konventionellen Datenträgern mit personenbezogenen Daten, die einem besonderen Berufsgeheimnis wie z. B. der ärztlichen Schweigepflicht unterliegen, muss während des gesamten Prozesses darauf geachtet werden, dass Unbefugte keine Kenntnis von den Daten nehmen können.

4.7 Steuerverwaltung

4.7.1 Einführung der Steueridentifikationsnummer

Finanzbehörden dürfen die Steueridentifikationsnummer (Steuer-ID) für ihre gesetzlich zugewiesenen Zwecke verarbeiten. Anderen Stellen kann die Verarbeitung der Steuer-ID durch eine spezifische gesetzliche Vorschrift erlaubt werden. Der Gesetzgeber sollte von dieser Möglichkeit jedoch nur in engen Grenzen Gebrauch machen.

Mit der Zuteilung der Steuer-ID hat jede Bundesbürgerin und jeder Bundesbürger vom Bundeszentralamt für Steuern ein **eindeutiges Identifikationsmerkmal** erhalten, welches bis 20 Jahre nach dem Tod bestehen bleibt. Unter dieser Nummer speichert das Bundeszentralamt zu jedem Steuerpflichtigen folgende Daten, sofern diese vorliegen: Titel, Familienname, Ehename, Lebenspartnerschaftsname, Geburtsname, Vorname, Geschlecht, vollständige Adresse, Geburtstag und -ort sowie Geburtsstaat. 5.300 Meldebehörden haben hierzu dem Bundeszentralamt für Steuern entsprechende Datensätze übermittelt.

Die Finanzbehörden dürfen die Steuer-ID erheben und verwenden, soweit dies für die Wahrnehmung ihrer gesetzlichen Aufgaben notwendig ist oder ein Gesetz die Verarbeitung ausdrücklich erlaubt oder anordnet. Stellen außerhalb der Finanzverwaltung dürfen die Nummer hingegen nur dann verarbeiten, wenn dies im Rahmen einer Datenübermittlung an die Finanzbehörden erforderlich ist oder eine **gesetzliche Vorschrift** die Datenverarbeitung rechtfertigt.

Problematisch ist, dass der Gesetzgeber zunehmend dazu übergehen möchte, **Stellen außerhalb der Finanzverwaltung** eine Verarbeitung der Steuer-ID zu erlauben. Im Bereich der Rentenbezugsmitteilungen an die Deutsche Rentenversicherung Bund haben u. a. die Träger der gesetzlichen Rentenversicherung, die berufsständischen Versorgungseinrichtungen, die Pensionskassen und die Versicherungsunternehmen die Steuer-ID von Leistungsempfängern mitzuteilen. Teilt der Steuerpflichtige der jeweiligen Stelle seine Nummer nicht mit, so übermittelt das Bundeszentralamt für Steuern der anfragenden Stelle die begehrte Information. Hieran anknüpfend möchte der Gesetzgeber in seinem Entwurf zum sogenannten Steuerbürokratieabbaugesetz im Bereich des Bezugs von Altersvorsorgebeiträgen als Sonderausgaben, dass Anbieter wie Lebensversicherungsunternehmen, Kreditinstitute, Bausparkassen und Kapitalanlagegesellschaften mit der Steuer-ID in ähnlicher Weise verfahren dürfen.

So wächst die Gefahr, dass die Steuer-ID als **Personenkennzeichen** im Bereich außerhalb der Finanzverwaltung verwendet wird. Zwar droht Unternehmern, die die Steuer-ID in „leichtfertiger“ Weise für gesetzlich nicht zulässige Zwecke nutzen, eine Geldbuße von bis zu 10.000 Euro. Allerdings genügt die Sanktionierung des Datenmissbrauchs als Ordnungswidrigkeit nicht, zumal eine „leichtfertige“ Verwendung der Nummer oft nicht nachweisbar sein wird. Stattdessen sollte auf die Verbreitung der Nummer an Stellen außerhalb der Finanzverwaltung verzichtet werden.

Was ist zu tun?
Der Gesetzgeber ist aufgefordert, die Verarbeitung der Steueridentifikationsnummer nicht weiter auf Stellen außerhalb der Finanzverwaltung auszudehnen.

4.7.2 Änderung des Kirchensteuergesetzes

Der Schleswig-Holsteinische Landtag befasste sich mit einem Gesetz zur Änderung des Kirchensteuergesetzes. Nicht alle Regelungen des Entwurfs hielten einer datenschutzrechtlichen Würdigung stand.

Kirchensteuerpflichtige sollten nach dem Entwurf die Möglichkeit haben, ihre Kirchensteuer auch von inländischen Kreditinstituten, Finanzdienstleistungsinstituten, Wertpapierhandelsunternehmen und Wertpapierhandelsbanken berechnen und an die Finanzämter weiterleiten zu lassen. Hierzu soll der Kirchensteuerpflichtige beim jeweiligen Institut einen Antrag stellen, in welchem er seine **Religionszugehörigkeit** zu benennen hat. Der Entwurf zum Kirchensteuergesetz enthielt die Regelung, dass die erhobenen Daten nur für den Kirchensteuerabzug verwendet werden dürfen und eine Verarbeitung für andere Zwecke nur mit Einwilligung des Steuerpflichtigen oder bei entsprechender gesetzlicher Regelung zulässig ist.

Mit einem bloßen Antrag wird der Kirchensteuerpflichtige allerdings nicht darüber informiert, dass ihm alternativ ein zweiter Weg offensteht: Es bleibt weiterhin möglich, die Kirchensteuer bei der Einkommensteuerveranlagung zu berücksichtigen. Damit besteht für den Kirchensteuerpflichtigen die Wahl, ob er Informationen zu seiner Religionszugehörigkeit z. B. einem Finanzdienstleistungsinstitut mitteilt oder nicht. Bei der Religionszugehörigkeit handelt es sich um besondere sensible personenbezogene Daten, deren Verarbeitung grundsätzlich einer besonderen Einwilligung des betroffenen Bürgers bedarf. Diese Einwilligung muss auf einer **freiwilligen Entscheidung** basieren, was voraussetzt, dass der Bürger seine Wahlmöglichkeit kennt. Dies kam im Entwurf zur Änderung des Kirchensteuergesetzes nicht klar zum Ausdruck.

Was ist zu tun?
Die Antragsformulare sind so zu gestalten, dass die betroffenen Bürger auf die bestehende Wahlmöglichkeit hingewiesen werden.

4.7.3 Zusendung falscher Steuerunterlagen

Die Finanzämter müssen bei der Versendung von Steuerunterlagen das Steuergeheimnis wahren. Die Unterlagen dürfen nicht in falsche Hände geraten.

Wir erhielen Kenntnis von drei Vorfällen, in denen Steuerpflichtige vom Finanzamt Steuerunterlagen **fremder Personen zugesandt** bekamen. Es handelte sich um Steuerbelege, die bei der Steuererklärung eingereicht und nach Prüfung an die

Steuerpflichtigen zurückgesandt werden sollten. Bei der Bearbeitung von Steuerfällen müssen die Mitarbeiterinnen und Mitarbeiter in den Finanzämtern technisch-organisatorische Maßnahmen zur Vermeidung derartiger Versehen ergreifen. Diese genügten nach unseren Feststellungen im Grundsatz. Bei der fehlerhaften Befüllung der Postumschläge waren in den drei Fällen drei verschiedene Personen tätig, die zudem in unterschiedlichen Bereichen ihre Aufgaben erfüllten. Es handelte sich jeweils um ein Versehen im Einzelfall. Da sich die Vorfälle in kurzem zeitlichen Abstand ereigneten und so gehäuft Verwechslungen stattfanden, hat das ULD eine Beanstandung ausgesprochen.

Was ist zu tun?
Die Mitarbeiterinnen und Mitarbeiter in den Finanzämtern sind verpflichtet, bei der Bearbeitung von Steuerfällen mit den Steuerunterlagen sorgsam umzugehen und Verwechslungen zu vermeiden.

4.7.4 Anforderungen an die Führung eines Fahrtenbuches

Zur Führung eines ordnungsgemäßen Fahrtenbuches genügt es, dass sich die Angaben zu Reiseziel, Reisezweck und beruflicher Veranlassung aus neben dem Fahrtenbuch existierenden Aufzeichnungen ergeben.

Eine Bürgerin bat das ULD um Prüfung der Anforderungen eines Finanzamtes an die Führung eines Fahrtenbuches. Sie ist als Sozialpädagogin tätig und sucht im Rahmen ihrer beruflichen Tätigkeit die betreuten Personen in deren privater Wohnung auf. Um die angefallenen Fahrtkosten steuermindernd geltend zu machen, ist ein Fahrtenbuch zu führen, in dem Reisezweck und gefahrene Reiseroute einzutragen sind. Das Finanzamt forderte bei der Prüfung des Fahrtenbuches darüber hinaus Angaben zur jeweils aufgesuchten Privatanschrift und die Namen der aufgesuchten Personen. Die Bürgerin sah sich aufgrund ihrer **beruflichen Schweigepflicht** gehindert, dem Finanzamt die gewünschten Daten mitzuteilen.

Die Bedingungen zum ordnungsgemäßen Führen eines Fahrtenbuches ergeben sich nicht aus dem Gesetz. Gerichtlich ist jedoch geklärt, dass ein Fahrtenbuch zeitnah und in gebundener Form geführt werden muss und die Fahrten in einem fortlaufenden zeitlichen Zusammenhang wiederzugeben sind. Weiterhin wird gefordert, dass für jede Dienstfahrt Reiseziel, -zweck, Geschäftspartner sowie Datum und Kilometerstand zu Beginn und Ende der jeweiligen Fahrt anzugeben sind. Diese Verpflichtung gilt auch für Berufsgeheimnisträger. Eine Verpflichtung zur Angabe der **Namen aufgesuchter Personen** wird gerade vor dem Hintergrund als zulässig angesehen, weil die zuständigen Mitarbeiter in den Finanzämtern dem Steuergeheimnis unterliegen. Vorsätzliche Verstöße gegen das Steuergeheimnis werden mit Strafe bedroht. Die bloße Angabe des Reisezwecks wäre für die Führung eines ordnungsgemäßen Fahrtenbuches nur dann ausreichend, wenn sich die übrigen obligatorischen Angaben aus weiteren beigelegten Aufzeichnungen ergeben. Die Forderung des Finanzamtes musste daher vom ULD nicht beanstandet werden.

Was ist zu tun?
Zur Führung eines ordnungsgemäßen Fahrtenbuches für steuerliche Prüfungszwecke dürfen bestimmte Mindestangaben verlangt werden, auch von Berufsgeheimnisträgern. Diese müssen und dürfen aber keine darüber hinausgehenden Angaben offenbaren.

4.7.5 Rolf Uwe Frank Maier-Schulz – zur Erforderlichkeit des ganzen Namens

Manches Finanzamt tut sich damit schwer, nicht benötigte Daten zu löschen und nicht zu verwenden.

Ein neu zuständiges Finanzamt verwendete im Adressfeld von übersandten Steuerbescheiden den vollen Namen der Person, d. h. alle drei Vornamen und den Nachnamen. Das bisherige Finanzamt hatte hingegen beim Schriftwechsel nur den von der Person angegebenen ersten Vornamen benutzt. Eine Einwilligung für die Verwendung aller Vornamen wurde gegenüber dem zuständigen Finanzamt nicht erklärt. Woher stammten die Angaben zu den bisher nicht offenbarten Vornamen, und durfte das Finanzamt alle verwenden? Nach dem Melderecht dürfen die Meldebehörden den Finanzämtern alle Vornamen und den Nachnamen übermitteln, soweit dies für die Aufgabenerfüllung der Finanzbehörden erforderlich ist. Dies ist der Fall bei der Angabe der weiteren Namen. Es gehört zu den Aufgaben der Finanzämter, intern eine zweifelsfreie Zuordnung von Namen zu Steuernummern vorzunehmen. Im Hinblick auf die Adressierung von Post muss hingegen geprüft werden, ob diese für eine ordnungsgemäße Zustellung der Steuerbescheide nötig sind. Vorliegend war dies nicht der Fall; es konnte davon ausgegangen werden, dass bereits ein Vorname in Verbindung mit dem Nachnamen eine **hinreichende Unterscheidungskraft** aufweist. Die Verarbeitung aller Vornamen im Rahmen der Adressierung ist grundsätzlich nicht zulässig.

Was ist zu tun?
Die Finanzbehörden müssen auch bei der Adressierung von Schreiben an die Steuerpflichtigen prüfen, ob die Angabe aller Vornamen erforderlich ist.

4.7.6 Kontoverbindungsdaten beim Finanzamt

Auch für gespeicherte Kontoverbindungsdaten gelten die Vorschriften zur Löschung personenbezogener Daten.

Ein Bürger hatte gegenüber seinem Finanzamt eine erteilte **Einzugsermächtigung** für die Zahlung von Kraftfahrzeugsteuer widerrufen. Zahlungen wurden von ihm fortan in Eigenregie überwiesen. Daraufhin begehrte er gegenüber dem Finanzamt die Löschung seiner Kontoverbindungsdaten. Im Rahmen der vorzeitigen Abmeldung eines anderen Fahrzeuges errechnete das Finanzamt wenig später eine Gutschrift und teilte dem Steuerpflichtigen mit, den entsprechenden Betrag „auf das bekannte Konto“ zu überweisen.

Kontoverbindungsdaten wie alle personenbezogenen Daten sind zu löschen, wenn die Speicherung unzulässig ist oder die verarbeitende Stelle die Daten nicht mehr für ihre Aufgaben benötigt. Vorliegend handelte es sich um zwei verschiedene Fahrzeuge, für welche Kraftfahrzeugsteuer gezahlt werden musste. Für jeden Vorgang bzw. für jedes Fahrzeug muss **separat geprüft** werden, ob die weitere Speicherung der Kontoverbindungsdaten erforderlich ist. Für die Überweisung von Steuern durch den Steuerpflichtigen ist die Speicherung von Kontoverbindungsdaten, im Gegensatz zur Teilnahme an einem Lastschrifteinzugsverfahren, nicht notwendig. Daher musste eine Löschung dieser Daten erfolgen, wobei kein separater Antrag des Steuerpflichtigen auf Löschung gestellt werden musste.

Was ist zu tun?
Die Finanzbehörden müssen für jeden Vorgang prüfen, ob die weitere Speicherung von Kontoverbindungsdaten erforderlich ist. Ein Rückgriff auf Daten aus anderen Vorgängen ist nicht zulässig.

5 Datenschutz in der Wirtschaft

Ein turbulentes Jahr für den Datenschutz im nicht öffentlichen Bereich liegt hinter uns mit **Skandalen** wegen Arbeitnehmerüberwachung (Tz. 5.3), Nutzung von Telekommunikationsdaten und illegalem Datenhandel (Tz. 5.4), mit öffentlicher Aufmerksamkeit und verstärktem gesetzgeberischem Tätigwerden (Tz. 2.2 und Tz. 5.1).

5.1 BDSG-Novellen

Zwei **Änderungsanträge** für das Bundesdatenschutzgesetz (BDSG) befinden sich im Gesetzgebungsverfahren. Der erste betrifft die Schaffung neuer Regelungen im Bereich des Auskunfteiwesens und des Scorings. Der zweite Antrag ist initiiert durch die Vorgänge im Zusammenhang mit dem illegalen Datenhandel und bezieht sich auf die Datenverarbeitung zu Werbezwecken und die Einführung eines Auditgesetzes.

5.1.1 Gesetzentwurf zum Auskunfteibereich und zum Scoring

Mit einigem Vorlauf beschloss die Bundesregierung Ende Juli 2008 einen Entwurf zur Änderung des BDSG. Er geht – im Grundsatz zutreffend – davon aus, dass die bisherigen Regelungen nicht mehr den Anforderungen einer anonymer werdenden Geschäftswelt und der gesteigerten Bedeutung von Auskunfteien genügen.

Das BDSG wird zwar materiellrechtlich weitgehend den Erwartungen von Verbraucherinnen und Verbrauchern beim Einsatz neuer Technologien wie Scoring oder Online-Warnverfahren in der Wirtschaft gerecht. Es besteht aber in diesem Bereich ein hohes Transparenzdefizit, das u. a. auf ein großes Vollzugsdefizit zurückzuführen ist. Die vom Entwurf angenommene Rechtsunsicherheit besteht nur in wenigen Punkten. Die Bewertungen durch die Datenschutzaufsichtsbehörden erfolgen weitgehend einheitlich, nach gemeinsamen Standards und in enger Abstimmung. Unterschiedliche Bewertungen können der Fortentwicklung des Rechtes dienen. Richtig ist, dass die Unternehmen im Auskunfteigeschäft ihre gesetzlichen Pflichten oft leugnen und praktisch nicht akzeptieren. Insofern sind gesetzliche **Klarstellungen und Verbesserungen** zu begrüßen.

Erstmalig soll die Erstellung und Nutzung von Wahrscheinlichkeitswerten – **das Scoring** – im BDSG geregelt werden. Die Vorschläge bleiben allerdings in mancher Hinsicht hinter der bestehenden Rechtslage zurück. Anschriftendaten sollen fast unbeschränkt für ein Wohnort-Scoring genutzt werden dürfen, was eine hohe Diskriminierungsgefahr birgt. Detailliert werden die Auskunftsrechte der Betroffenen beim Scoring geregelt. Da die Praxis diesbezüglich bisher die bestehende Rechtslage ignorierte und die Unternehmen die Umsetzung verweigerten, sind die geplanten Transparenzregelungen zu begrüßen. Highlights sind der Anspruch auf **eine kostenlose Selbstauskunft** pro Jahr und die seit Langem von

Datenschützern geforderte Bußgeldsanktionierung der Nichterteilung von Auskünften gegenüber den Betroffenen.

Problematisch sind Regelungen zur **Einmeldung von untitulierten Forderungen** bei Auskunfteien. Schon nach zwei erfolglosen Mahnungen und unbestrittener Forderung soll dies bei einer Auskunftei als Negativmerkmal eingemeldet werden dürfen. Im Telekommunikations- und im Medienbereich erleben wir zunehmend, dass Verträge fingiert werden, d. h., dass der Abschluss eines Vertrages nach einem Telefonanruf eines Callcenters, dem Aufruf einer Webseite oder der Nutzung eines sonstigen Telemediendienstes vom Unternehmen behauptet wird, obwohl keine Willenserklärung durch den Verbraucher abgegeben wurde oder der Vertrag aus rechtlichen Gründen nicht zustande gekommen ist. Sich aus solchen fingierten Verträgen vermeintlich ergebende Zahlungspflichten können mit der geplanten Regelung künftig an Auskunfteien einfacher eingemeldet werden. Die Betroffenen würden so gezwungen, auf einen behaupteten, aber tatsächlich nicht berechtigten Zahlungsanspruch zu reagieren. Positiv ist, dass die Betroffenen rechtzeitig vor der Einmeldung unterrichtet werden müssen. Einmeldungen erfolgen heute oft, ohne dass der Betroffene Kenntnis davon hat.

Es wäre ein wichtiges Zeichen, wenn der Bundesgesetzgeber speziell die – vielfach versprochenen – transparenzverbessernden Vorgaben endlich in konkrete gesetzliche Regelungen umsetzen würde.

5.1.2 Gesetzentwurf zur Datenverarbeitung zu Werbezwecken

Das Bundesministerium des Innern kündigte beim Datenschutzgipfel Anfang September 2008 als Reaktion auf das Bekanntwerden des illegalen Handels mit sensiblen Personendaten, insbesondere Kontodaten, umfassende Verbesserungen an.

Im Zentrum seines Vorschlags steht das Erfordernis der Einwilligung bei der Datennutzung für fremde Werbezwecke. Nach einer kurzen Zeit des Schweigens liefen Lobbyisten, vor allem aus der Werbebranche, gegen die geplante Änderung Sturm. Bei dem **Wechsel zum Permission Marketing** wurde der Untergang des Direktmarketings prophezeit. Dieser Wechsel ist nicht nur verfassungsrechtlich möglich und aus Daten- und Verbraucherschutzsicht wünschenswert, er liegt auch im Interesse der Gesamtwirtschaft. Will die Wirtschaft wirklich den Dialog mit den Verbrauchern, so müssen diese gehört und es darf nicht über deren Köpfe hinweg entschieden werden.

Eine offene Bund-Länder-Arbeitsgruppe unter der Leitung Brandenburgs machte aus Sicht der Länder Vorschläge für die Änderung des BDSG. Der im Dezember 2008 vom Kabinett beschlossene Gesetzentwurf blieb leider hinter den formulierten Erwartungen zurück. Zentrale Forderungen der Bund-Länder-Gruppe, die insbesondere die **Stärkung der Aufsichtsbehörden und deren Kontrollinstrumente** betrafen, wurden nicht übernommen. Zu begrüßen ist die Einführung eines Kündigungsschutzes für den betrieblichen Datenschutzbeauftragten.

Bei den materiellen Regelungen hat die Angstkampagne der Wirtschaft Spuren hinterlassen: Man hat sich nicht durchgerungen, die Datenverarbeitung zu Werbezwecken umfassend von einem „Opt-In“, also von einer vorab erteilten Zustimmung des Betroffenen abhängig zu machen und das sogenannte **Listenprivileg** zu streichen. Der Entwurf enthält zahlreiche Ausnahmen, nicht nur bei der Datenverwendung zu Werbezwecken für „eigene“ Angebote. Erlaubt wird weiter im Grunde die Übermittlung listenmäßig zusammengefasster Daten, womit die Gefahr missbräuchlicher Weiterverwendung von Daten bei der empfangenden Stelle weiterhin besteht. Erfreulich sind konkretisierende Vorgaben für die Erteilung der Einwilligung, nämlich dass die Zustimmung bewusst erfolgt und zweifelsfrei zum Ausdruck gebracht wird.

Andere Vorschläge, etwa die Pflicht zur **Herkunfts- und Zweckkennzeichnung von Daten**, z. B. über Metadaten bzw. sogenannte „sticky Policies“ (30. TB, Tz. 8.2), blieben vollkommen unberücksichtigt. Positiv erwähnenswert ist allerdings die Informationspflicht bei Datenschutzverstößen.

Was ist zu tun?
Die beiden BDSG-Entwürfe sind noch in der laufenden Legislaturperiode zu verabschieden. So wird den Verbraucherinnen und Verbrauchern signalisiert, dass der Gesetzgeber deren Recht auf informationelle Selbstbestimmung zu schützen bereit ist.

5.2 Geodaten – Regeln für die wirtschaftliche Nutzung

Das ULD hat sein Engagement zum Schutz Betroffener bei der Verwendung von georeferenzierten Informationen fortgeführt. Geodaten spielen eine zunehmende Rolle bei der Planung von raumbedeutsamen Projekten, der Berechnung von natürlichen Risiken oder der Einschätzung von Auswirkungen menschlichen Handelns auf die Umwelt.

Viele Wirtschaftsbranchen haben ein vitales Interesse an der Verwertung von Geoinformationen. Durch immer weiter verfeinerte Verschneidungs- und Analysetechniken verstärken sich die **Gefahren für die Persönlichkeitsrechte** der Betroffenen. Hinzu kommt, dass die Erhebung der Daten in der Regel ohne Mitwirkung und ohne Wissen der Betroffenen erfolgt. Der Inhalt der Daten ist durch diejenigen, die sie betreffen, häufig nicht veränder- oder beeinflussbar.

Klärungsbedürftig ist zunächst, unter welchen Bedingungen georeferenzierte Informationen Personenbezug haben und wie stark Geoinformationen die Persönlichkeitsrechte Einzelner beeinträchtigen können. In erster Linie sind Geoinformationen inhaltliche **Aussagen zu georeferenzierten Objekten** oder Landflächen. Diese objektbezogenen Informationen können Aussagen über die persönlichen oder wirtschaftlichen Verhältnisse Einzelner beinhalten, z. B. des Eigentümers eines Grundstücks oder Gebäudes.

Das ULD erstellte für die Kommission für Geoinformationswirtschaft des Bundesministeriums für Wirtschaft und Technologie (GIW-Kommission) eine sogenannte „**Ampelstudie**“. Wir entwickelten die dogmatischen Grundlagen für eine Kategorisierung von Geodaten und bewerteten hiernach eine von der Kommission vorgelegte Liste von Datenarten. Zudem wurden die verschiedenen Zugangsmöglichkeiten zu den Daten systematisiert.

Geoinformationen besitzen nach den Ergebnissen des ULD Personenbezug, wenn der Inhalt einer Information auch eine **Aussage über eine Person** trifft. Nicht jede Information, die mit einer Person technisch verknüpft werden kann, fällt damit in den Anwendungsbereich des Datenschutzrechts. Personenbezug besitzen Geoinformationen erst, wenn sie auf die Rechte und Interessen einer natürlichen Person einwirken (Ergebniskontext), Betroffene bewerten oder ihr Verhalten bzw. ihre Stellung innerhalb einer gegebenen Gruppe beeinflussen (Zweckkontext) oder direkt eine inhaltliche Aussage über die Persönlichkeit einer Person enthalten (Inhaltskontext).

Das ULD klassifizierte die vorgegebenen Geodatensätze hinsichtlich der Gefährdung für die Persönlichkeitsrechte. Dies kann nicht losgelöst von dem jeweiligen Verarbeitungs- und Nutzungszusammenhang erfolgen. Das ULD entwickelte daher Kriterien zur Bewertung der **Sensibilität von Informationen**, wobei die Gefährdung weiterer Grundrechte sowie Nutzungsinteressen der Betroffenen, des Staates und der Wirtschaft sowie die Verfügbarkeit der Geoinformationen einfließen.

Die für die wirtschaftliche Nutzung von Geodaten erforderliche punkt- oder flächenbezogene **Verschneidung von Informationen** kann zu einer erhöhten Gefährdung der Persönlichkeitsrechte führen und bis zu einer umfassenden Profilbildung zu einzelnen Personen gehen. Eine derartige Datenakkumulation zu Einzelprofilen ist unzulässig.

Das **Ampelsystem** der Studie basiert auf den Gefährdungseinschätzungen und den vorhandenen rechtlichen Normen. „Grün“ eingestufte Daten besitzen keinen Personenbezug bzw. keine relevante Gefährdung für die Persönlichkeit des Einzelnen. Informationen der Kategorie „Gelb“ haben Personenbezug mit einem im Einzelnen variierenden Gefährdungspotenzial. Datenarten mit „Rot“ sind personenbezogen und besonders schutzwürdig. Die wirtschaftliche Nutzung dieser Daten ist in der Regel ausgeschlossen und unterliegt besonderen rechtlichen Anforderungen. Die Studie ist im Internet abrufbar unter:

http://www.geobusiness.org/

Die Erkentnisse der Studie wurden von uns sowohl in dem von uns geleiteten „Unterarbeitskreis Geodaten“ der Datenschutzbehörden als auch im „Arbeitskreis Geodateninfrastruktur des Landes Schleswig-Holstein“ eingebracht. Wir begleiteten die **Umsetzung der INSPIRE-Richtlinie** im Land Schleswig-Holstein und auf Bundesebene und wirkten an der Sensibilisierung beim Thema Geodaten und Datenschutz mit (30. TB, Tz. 8.14).

Ein nächster Schritt wird darin bestehen, **konkrete Praxisanwendungen** auf deren datenschutzrechtliche Zulässigkeit hin zu untersuchen und dabei z. B. die Grenzen der Verschneidung von Geoinformationen abzustecken, um diese ohne Bedrohung für die Persönlichkeitsrechte der Betroffenen zu ermöglichen. Dabei sind Methoden und Technologien zu entwickeln, über welche die wirtschaftlichen Potenziale von Geodaten genutzt werden können, ohne die Persönlichkeitsrechte der Betroffenen zu gefährden. Die Anonymisierung und Aggregierung von Daten sind insofern von hoher Relevanz. Mindestanforderung an eine datenschutzkonforme Nutzung ist es, die Transparenz für die Betroffenen und deren Recht auf effektiven Widerspruch zu sichern.


http://www.datenschutzzentrum.de/geodaten/

Was ist zu tun?
Die nachhaltige wirtschaftliche Nutzung von Geodaten und deren gesellschaftliche Akzeptanz kann nur durch die Schaffung von Rechtssicherheit für Betroffene und Datennutzer sichergestellt werden.

5.3 Lebensmitteldiscounter – der nichts wissen wollte und doch alles wusste

Im März 2008 brach ein Sturm der Entrüstung los: Ein Detektiv hatte Berichte über seine Tätigkeit für einen großen deutschen Lebensmitteldiscounter an die Presse weitergegeben. Im Einzelhandel wurden offensichtlich systematisch Mitarbeiter bespitzelt.

Den Überwachungsberichten waren detaillierte Protokolle über das Verhalten der Mitarbeiter des Discounters sowie Informationen aus deren Privatleben zu entnehmen. Die Mitarbeiter sowie die Kunden waren mit Miniaturkameras beobachtet worden. Bei unseren **aufsichtsbehördlichen Ermittlungen** zeigte sich immer ein ähnliches Muster der Detektiveinsätze. Die rechtlich selbstständigen Regionalgesellschaften des Discounters beauftragten eine oder mehrere Sicherheitsfirmen und wählten zwischen zwei verschiedenen Einsatzarten:

Bei der sogenannten **Ladendiebstahlskontrolle** wurden für einen Zeitraum von ca. einer Woche Miniaturkameras in der Filiale installiert. Die Bilder wurden in Echtzeit auf im Aufenthaltsraum aufgestellte Monitore übertragen, vor denen der Mitarbeiter der beauftragten Sicherheitsfirma saß und die Bilder kontrollierte. Die Beschäftigten der Filiale bekamen die Installation der Kameras mit; auch die Anwesenheit des Detektivs war für sie erkennbar. Was sie nicht wussten: Es ging nicht nur darum, Ladendiebe zu fassen. Im Wesentlichen wurden zur Aufklärung von Inventurdifferenzen auch die einzelnen Mitarbeiter unter die Lupe genommen. Die eingesetzten Detektive kontrollierten

nicht nur die Monitore, sondern führten akribisch darüber Protokoll, was ihrer Ansicht nach „verdächtig“ war. Sie hielten die Verhaltensweisen der einzelnen Mitarbeiter fest, zeichneten die Informationen auf, die sie aus eigenen Gesprächen mit den Mitarbeitern auch über deren Privatleben erhalten hatten, belauschten die Gespräche der Mitarbeiter untereinander bzw. die Gespräche, die sie z. B. in ihren Pausen privat mit dem Handy führten, und protokollierten die so gewonnenen Erkenntnisse. Von den Detektiven wurden über Eigenschaften und Gefühlszustände der Mitarbeiter zum Teil die absurdesten Einschätzungen festgehalten. Das Verhalten eines Mitarbeiters wurde vom eingesetzten Detektiv als verdächtig gekennzeichnet, weil der Mitarbeiter bei seinem Privattelefonat mit dem eigenen Handy den Raum verließ und „auffällig leise“ sprach. In den Berichten werden ganze Gespräche und Aussagen von Mitarbeitern wörtlich zitiert. Sie enthalten zum Teil intimste Informationen aus dem Privatleben der Beschäftigten, die diese im Gespräch mit dem Detektiv vertrauensvoll offenbart hatten oder die von anderen Mitarbeitern über Kollegen preisgegeben wurden. Zum Abschluss des Einsatzes wurden all diese Informationen in einem Einsatzbericht festgehalten, der dem Auftraggeber übergeben wurde.

In der zweiten Variante, dem sogenannten **Observationseinsatz**, wurden am Wochenende Miniaturkameras installiert. Diese zeichneten das Geschehen über einen Zeitraum von einer Woche auf, ohne dass die Mitarbeiter oder die Filialleitung informiert waren. Die Aufnahmen wurden von Mitarbeitern der Sicherheitsfirma nach „verdächtigen“ Szenen ausgewertet. Die zusammengestellten Videosequenzen wurden zum Abschluss des Einsatzes der Auftrag gebenden Regionalgesellschaft übergeben. Bei diesen Observierungseinsätzen ging es ausschließlich darum, die Mitarbeiter zu beobachten. Zumeist konzentrierte sich die Aktion auf einzelne Mitarbeiter einer Filiale, die sich nach Ansicht der Regionalgesellschaft zuvor „auffällig“ verhalten hatten. Aufgezeichnet wurde allerdings das Verhalten aller Mitarbeiter der betroffenen Filialen.

In **schleswig-holsteinischen Filialen** wurden insgesamt 11 Einsätze festgestellt, von denen zwei als Observierungs- und neun als Ladendiebstahlskontrolleinsätze durchgeführt wurden. Das ULD verhängte ein Bußgeld gegen die in Schleswig-Holstein ansässige Regionalgesellschaft. Diese bemühte sich festzustellen, dass die Ergebnisse der Überwachung sowie die Videosequenzen, soweit sie keine Hinweise auf Eigentumsdelikte enthielten, unbeachtet geblieben seien. Dennoch hatte sie die Ergebnisse der Überwachungen und die Videosequenzen entgegengenommen und vorgehalten, ohne die Berichte und Videos zurückzuweisen bzw. zu löschen.

Das Interesse eines Unternehmens, ungewöhnlich hohe Inventurverluste aufzuklären und die Ursachen zu ermitteln, ist anzuerkennen. Dies rechtfertigt jedoch nicht die Einholung von Erkenntnissen durch Vollüberwachungsmaßnahmen und derart invasive Eingriffe in die Persönlichkeitsrechte und **Privatsphäre der Beschäftigten**. Die oft sehr subjektiven Einschätzungen der Detektive waren nicht durch nach außen wirkende objektive Merkmale messbar bzw. einer objektiven Überprüfbarkeit zugänglich. Die Informationen waren in großem Umfang ungeeignet, um valide Erkenntnisse im Hinblick auf potenzielle Eigentumsdelikte von Mitarbeitern zu erlangen. Unabhängig von Seriosität, Zuverlässigkeit und Validität

vermögen derartige Informationen, sind sie einmal ausgesprochen oder sogar schriftlich fixiert, den Betroffenen einen Makel anzuhaften. Selbst wenn diese Darstellungen unbeachtet geblieben sind, so wurden sie doch zur Kenntnis genommen. Bei zukünftigen Unregelmäßigkeiten werden diese dann leicht zulasten der Betroffenen herangezogen. Diese können gegen den haften bleibenden Eindruck, „nicht ganz koscher zu sein“, keine wirksamen Maßnahmen ergreifen. Die Betroffenen wurden erst informiert, als die Vorgänge schon öffentlich geworden waren und die Aufsichtsbehörden ihre Verfahren eingeleitet hatten.

Die Aufsichtsbehörden der Länder arbeiteten bei ihren Ermittlungen eng zusammen. Sie ahndeten zudem die Nichtbestellung betrieblicher Datenschutzbeauftragten. Auch gegen in anderen Bundesländern ansässige Regionalgesellschaften wurden **Bußgelder** verhängt. Insgesamt betrug die Bußgeldsumme eine für Datenschutzverstöße in Deutschland bis dahin noch nicht erreichte Rekordhöhe von 1,462 Mio. Euro. Die baden-württembergische Datenschutzaufsicht, das dortige Innenministerium, koordinierte das gemeinsame Vorgehen der Aufsichtsbehörden und erstellte einen Gesamtbericht, der im Internet abrufbar ist.

https://www.datenschutzzentrum.de/presse/20080911-lidl-bussgeldverfahren.html

Arbeitgeber trifft die Pflicht zu prüfen, ob und inwieweit sie Informationen über Mitarbeiterinnen und Mitarbeiter erheben und speichern dürfen. Insbesondere Privates, Informationen vom Hörensagen sowie Dritteinschätzungen über Gefühlszustände und spezifische Eigenschaften der Mitarbeiter sind für Arbeitgeber tabu. **Vollprotokollierungen des Mitarbeiterverhaltens** am Arbeitsplatz greifen unverhältnismäßig in die Persönlichkeitsrechte von Arbeitnehmern ein. Die Nutzung derart gewonnener Informationen zur Leistungs- und Verhaltenskontrolle ist unzulässig. Sollen im Betrieb Ermittlungen zur Verhinderung von Inventurverlusten vorgenommen werden, so müssen klare Festlegungen, z. B. in Form einer mit dem Betriebsrat geschlossenen Betriebsvereinbarung, erfolgen; die Maßnahmen müssen für die Mitarbeiter transparent sein und dürfen die Grenzen des Verhältnismäßigen nicht überschreiten. Sollen im Ausnahmefall von Dritten Informationen eingeholt werden, so ist der Mitarbeiter zu benachrichtigen; es müssen Beschwerde- oder Eskalationsverfahren vorgesehen sein, die es dem Mitarbeiter ermöglichen, eine Gegendarstellung abzugeben. Heimliche Videoüberwachung in öffentlichen Räumen ist schon vom Bundesdatenschutzgesetz verboten. Technische Beobachtungen müssen ausnahmslos gekennzeichnet werden. Videoüberwachung ist nur in Ausnahmefällen zulässig; die Dauerüberwachung eines Arbeitsplatzes ist in jedem Fall unzulässig. Den Mitarbeitern müssen zudem unbeobachtete Rückzugsräume gewährt werden.

Was ist zu tun?
Arbeitgeber müssen sich an die engen Grenzen zulässiger Mitarbeiterkontrolle halten. Der Discounter muss ein Datenschutzmanagement einführen, das dies nachhaltig gewährleistet.

5.4 Bei Anruf Betrug – illegaler Handel mit Adress-, Telefon- und Bankdaten

Was früher fast unmöglich schien, erweist sich heute als bedrohlich. Tausende Bürgerinnen und Bürger erhalten unerwünschte Anrufe von Callcentern, die ihnen Verträge, z. B. Lotterieteilnahme, anbieten. Obwohl die Betroffenen die telefonischen Angebote zumeist ablehnen, werden kurze Zeit später Geldbeträge von ihren Bankkonten abgebucht. Das Vorgehen erfolgt mit auf illegale Weise beschafften Bankdaten.

- **Sachverhalt**

Im Sommer 2008 übergab die Verbraucherzentrale Schleswig-Holstein dem ULD eine ihr zugespielte CD aus einem Lübecker Callcenter. Auf der CD befanden sich mehr als 17.000 Datensätze mit Angaben zu Namen, Adresse, Geburtsdatum, Telefonnummer und Kontoverbindung. Die Struktur der Datensätze wies auf eine Herkunft aus dem Bereich einer **Klassenlotterie** hin. Weitere CDs folgten mit zusätzlichen Angaben wie E-Mail-Adressen und Verbraucherangaben. Einzelne Datenbestände bezogen sich gezielt auf ältere Menschen. Zurzeit verfügt das ULD über fast **acht Millionen** illegale Datensätze, die entweder aus der Übergabe durch die Verbraucherzentrale, von anonym zugespielten CD-ROMs oder einem Lockvogelankauf des Verbraucherzentrale Bundesverbands (vzbv) stammen. Die Datensätze werden zur Ermittlung der Quellen und für die Beauskunftung an Betroffene genutzt (Tz. 6.5).

Die Kundendaten einschließlich der Bankverbindungen wurden auf unterschiedliche Weise erlangt. Die meisten Datensätze stammen offensichtlich aus **Glücksspielunternehmen**. Diese Unternehmen geben zum Teil an, die Daten nicht verkauft zu haben. Folgende Szenarien kommen in Betracht: Entweder haben unzuverlässige Mitarbeiter Firmendatenbestände kopiert und an Adresshändler weiterverkauft, oder Callcenter haben die Daten nach Abschluss ihrer Aufträge nicht gelöscht, sondern gesammelt und für eigene Zwecke verwendet. In Einzelfällen wurden im Rahmen von telefonischen Kaltakquisen Eigenangaben von Betroffenen durch Callcenter erfasst. Andere Datenbestände stammen aus der Inanspruchnahme von Internetdiensten, aus dem Zeitschriftenvertrieb, aus Spendensammlungen, von Preisausschreiben oder aus Kundendatenbeständen anderer Unternehmen.

Die illegal erhobenen Daten wurden in vielen Fällen an Adressdatenhändler weitergegeben, die diese dann auf dem Schwarzmarkt weiterverkauften. Viele Callcenter nutzten die ihnen anvertrauten oder die gekauften Daten einschließlich Kontoverbindung und Telefonnummer für die weitere **Telefonakquise** oder für das **Fingieren von Verträgen**, insbesondere in den Branchen Lotterie, Telekommunikation, Zeitschriftenvertrieb, Online-Angebote oder Spendenanwerbung. Anschließend wurden die Daten an die Unternehmen weitergegeben, für die tatsächlich oder vermeintlich Verträge abgeschlossen wurden. Diese wiederum zahlten hierfür Provisionen und buchten von den Konten der – oft vermeintlich – gewonnenen Kunden Beträge ab. Die **Kontoabbuchungen** wurden von den Kreditinstituten regelmäßig ungeprüft akzeptiert, selbst dann, wenn es sich um

Massenabbuchungen handelte und aufgrund von Widersprüchen von Kunden und dadurch notwendigen Rückbuchungen der Verdacht bestand, dass real keine Abbuchungsermächtigungen der Kunden vorlagen. Die Rückbuchungen werden von den Banken innerhalb einer Frist von sechs Wochen ohne weitere Hinterfragung durchgeführt. Erfolgen Widersprüche später, wird die Rückbuchung zu einem langwierigen Prozess.

- **Datenschutzrechtliche Bewertung**

Nach den derzeitigen Regelungen des Bundesdatenschutzgesetzes ist die Nutzung personenbezogener Daten für **Werbezwecke** in der Regel zulässig, wenn sie sich auf Name, Adresse, Geburtsjahr, Branche und Gruppenzugehörigkeit beschränkt. Man spricht vom „Listenprivileg". Bankverbindung und Telefonnummer gehören nicht zu diesem gesetzlich definierten Datenkatalog. Deren Nutzung für Werbezwecke ist unzulässig, es sei denn, der Betroffene hat ausdrücklich und wirksam hierin eingewilligt. Dem ULD ist bisher kein einziger Fall bekannt, bei dem ein Betroffener eine derartige Einwilligung erteilt hätte.

Die Tätigkeit von Callcentern erfolgt in vielen Fällen als **Datenverarbeitung im Auftrag**. Auftragnehmer haben nach Durchführung eines Auftrags, z. B. der Kundenbetreuung, die vom Auftraggeber zur Verfügung gestellten Daten zu löschen oder sie an diesen wieder zurückzugeben. Eine Nutzung dieser Daten zu anderen und eigenen Zwecken ist unzulässig. Der Auftraggeber hat den Auftragnehmer sorgfältig auszuwählen und die Einhaltung bestimmter vertraglicher Vorgaben zu überwachen. Zudem muss der Auftraggeber sorgfältig prüfen, welche Daten für die Auftragserfüllung tatsächlich erforderlich sind, und darf auch nur diese weitergeben. In vielen Fällen spielt die Kontoverbindung keine Rolle und darf folglich nicht dem Zugriff der Dienstleister ausgesetzt werden. Sowohl Auftragnehmer als auch Auftraggeber missachteten in den Datenmissbrauchsfällen ihre datenschutzrechtlichen Pflichten.

Die materiell unzulässige Verarbeitung von Kontodaten ist eine Ordnungswidrigkeit, die mit einem Bußgeld von bis zu 250.000 Euro geahndet werden kann. Erfolgen derartige Handlungen vorsätzlich gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder zu schädigen, so liegt eine **Straftat** vor, die mit einer Freiheitsstrafe bis zu zwei Jahren bestraft werden kann. In den Fällen der Nutzung von Kontodaten zur unberechtigten Abbuchung vom Konto kann in der Regel von einer Bereicherungsabsicht ausgegangen werden.

- **Was hat das ULD gemacht?**

In den ersten Wochen des Datenskandals wurde das ULD mit **Anfragen besorgter Bürger** – per Brief, Fax, E-Mail oder telefonisch – regelrecht zugeschüttet. Wir haben allen Anfragenden geantwortet und Auskunft erteilt. Den anfragenden Betroffenen wurde mitgeteilt, ob sie in dem Bestand mit zunächst 17.000 und dann fast acht Millionen Datensätzen enthalten sind oder nicht. Die Betroffenen konnten so entscheiden, ob sie sich ein neues Konto oder eine neue Telefonnummer einrichten wollten. Das ULD empfahl zudem, eine besondere Sorgfalt bei der

Kontrolle der Kontoauszüge walten zu lassen. In Einzelfällen stellte das ULD Banken, deren Kunden vom illegalen Datenhandel betroffen waren, auf deren Angebot hin die sich hierauf beziehenden Datensätze zur Verfügung, um die Kunden im Auftrag des ULD über die unzulässige Datenspeicherung zu informieren.

Den Anfragenden wurden **Ratschläge** erteilt, z. B. wie man sich künftig vor unerlaubten Abbuchungen schützen kann, wie man die unzulässig abgebuchten Beträge zurückerhält oder dass man regelmäßig seine Kontoauszüge überprüfen sollte. Diese sind als häufig gestellte Fragen (FAQ) und Antworten im Internet abrufbar.


https://www.datenschutzzentrum.de/kontodaten/faq-kontodaten.html

Das ULD hat umgehend nach Erhalt der Daten diese an die zuständigen Staatsanwaltschaften weitergeleitet und entsprechende **Strafanträge** gestellt. Eine Rückmeldung von den Staatsanwaltschaften hat das ULD bisher nicht erhalten.

- **Forderungen an die Politik und andere Institutionen**

Alle Beteiligten – also vorrangig die Politik, die Auftrag gebenden Unternehmen, die Callcenter und die Kreditinstitute – sind aufgefordert, alles zu unternehmen, damit der illegale Datenhandel nicht weitergeführt wird. Aus den aktuellen Erfahrungen zieht das ULD folgende **Schlussfolgerungen**:

- Das Bundesdatenschutzgesetz muss überarbeitet werden. Die Weitergabe von personenbezogenen Daten für Werbezwecke sollte von der informierten **Einwilligung** des Betroffenen abhängig gemacht werden (Permission Marketing) (Tz. 2.2). Die bisherige Privilegierung der Werbenutzung ist verfassungsrechtlich fragwürdig und rechtspolitisch anachronistisch. Zudem sollte geprüft werden, ob der Sanktionsrahmen im Bereich des Ordnungswidrigkeitenrechts und des Strafrechts im Bundesdatenschutzgesetz vor dem Hintergrund der Datenschutzskandale noch ausreicht.
- Es ist sorgfältig zu prüfen, ob und unter welchen Bedingungen – nach US-amerikanischem Vorbild – die Unternehmen verpflichtet werden, die Betroffenen bei Datenpannen zu **informieren**. Dabei muss allerdings verhindert werden, dass Menschen unnötig beunruhigt werden.
- Unternehmen sollte untersagt werden, die Zustimmung zur Datennutzung für Werbezwecke zur Bedingung für den Vertragsabschluss zu machen. Dieses – aus dem Telemedienrecht bisher bekannte – sogenannte **Koppelungsverbot** sollte für alle Branchen gelten.
- Die Möglichkeiten, den durch Datenmissbrauch entstandenen Gewinn von den Unternehmen wieder einzuziehen (**Gewinnabschöpfung**), müssen geprüft werden. Praktische Voraussetzung hierfür ist allerdings eine erhebliche personelle Aufstockung für die behördlichen Ermittlungen.

- Unternehmen, die Drittfirmen wie z. B. Callcenter als Auftragnehmer oder Dienstleister einschalten, müssen diese besser **kontrollieren**. Die Auftragnehmer müssen sich strikt an die Weisungen des Auftraggebers halten und dürfen die Daten nicht für eigene Zwecke nutzen. Zudem dürfen nur solche Daten weitergegeben bzw. übermittelt werden, die auch tatsächlich erforderlich sind, um die Aufgabe zu erfüllen.
- Die **Kreditinstitute** sollten verpflichtet werden, Fälle von Massenabbuchungen und häufigen Rückbuchungen zu überprüfen. Wenn der Verdacht besteht, dass keine Einzugsermächtigungen vorliegen, dürfen die Abbuchungsaufträge nicht ungeprüft ausgeführt werden.
- Mit **Warndateien** über solche Unternehmen, bei denen der begründete Verdacht auf Datenschutz- bzw. Verbraucherschutzverstöße besteht, könnten die schwarzen Schafe vom Rest der Branche getrennt werden. Hierfür gibt es im Bundesdatenschutzgesetz schon heute hinreichende Rechtsgrundlagen.
- An einer erheblichen Verbesserung der **personellen Ausstattung** der Datenschutzaufsichtsbehörden geht kein Weg vorbei. Eine einstellige Zahl von Mitarbeitern ist regelmäßig für mehrere Hunderttausend Firmen zuständig; Vollzugsdefizite sind so zwangsläufig.

Der **Landtag Schleswig-Holstein** hat die Erfahrungen mit dem illegalen Datenhandel zum Anlass genommen, durchgängig zu begrüßende Forderungen an den Bundesgesetzgeber zu formulieren (LT-Drucksache 16/2421). Weitere Einzelheiten zum Thema sind im Internet abrufbar unter:

https://www.datenschutzzentrum.de/kontodaten

Was ist zu tun?
Alle Beteiligten und Betroffenen sind gefordert. Statt mit den Fingern immer auf die anderen zu zeigen, muss jede und jeder prüfen, was sie bzw. er selbst zur Vermeidung von Datenmissbrauch tun kann, und dies dann auch umsetzen.

5.5 Neues aus der Versicherungswirtschaft: Licht und Schatten

5.5.1 Auf dem Weg zu branchenweiten Verhaltensregeln?

Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) erstellt derzeit Verhaltensregeln, die die zulässigen Datenverarbeitungen der Mitgliedsunternehmen konkretisieren und selbstverpflichtend festlegen sollen.

Bisher wurde versucht, die Datenverarbeitung bei Versicherungsunternehmen über umfängliche Einwilligungserklärungen der Versicherungsnehmer zu legitimieren. Die Krux an der Sache: Wer die Zustimmungsklauseln nicht unterzeichnet, erhält keinen Versicherungsvertrag. Dies gilt für die gesamte Branche. Die Klauseln sind weitestgehend angeglichen. Die Versicherungsnehmer sind gezwungen, den Datenverarbeitungen zuzustimmen, weil sie sonst keinen Versicherungsschutz erhalten.

Von einer **„freiwilligen" Einwilligung** kann daher nicht die Rede sein. Dies gilt ebenso für die Erklärungen zur Entbindung von der Schweigepflicht, die in bestimmten Versicherungssparten für die Anfrage bei Ärzten oder anderen beruflichen Geheimnisträgern eingeholt wird. Für diese hat das Bundesverfassungsgericht im Jahr 2006 festgestellt, dass die Freiwilligkeit bei der Abgabe einer solchen Erklärung nur gewahrt werden kann, wenn dem Versicherungsnehmer die Möglichkeit gegeben wird, in jedem einzelnen Fall zu entscheiden, ob er einen Arzt oder eine andere Stelle von der Schweigepflicht entbinden möchte. Klar ist aber auch: Für die Abwicklung eines Versicherungsverhältnisses müssen personenbezogene Daten verarbeitet werden. Die Legitimation hierfür kann sich allerdings bereits aus dem Bundesdatenschutzgesetz ergeben, soweit ausschließlich die für die Abwicklung erforderlichen Daten verarbeitet werden. Einer Einwilligung des Betroffenen bedarf es dann nicht; diese ist auch nicht angezeigt: Mit der Einwilligung wird dem Betroffenen fälschlicherweise suggeriert, er könne über die Datenverarbeitung selbst bestimmen. Diese ist vielmehr zwingende Grundlage für die Abwicklung und Durchführung des Vertrags. Einwilligungen dürfen grundsätzlich nur dort eingesetzt werden, wo für die Betroffenen eine echte Entscheidungsmöglichkeit gegeben ist. Alle anderen Datenverarbeitungen müssen an den gesetzlichen Verarbeitungsmöglichkeiten gemessen und den dort vorgeschriebenen beschränkten Möglichkeiten angepasst werden.

Erstellung von Verhaltensregeln nach § 38a Bundesdatenschutzgesetz (BDSG)

§ 38a Bundesdatenschutzgesetz (BDSG) sieht die Möglichkeit vor, dass Berufsverbände oder andere Vereinigungen, die bestimmte Branchen vertreten, sich selbst einen Verhaltenskodex auferlegen. Diese sogenannten Verhaltensregeln ersetzen die Vorschriften des Bundesdatenschutzgesetzes nicht. Sie dienen dazu, die sehr abstrakt gehaltenen Regelungen des BDSG im Hinblick auf die branchentypischen Datenverarbeitungen zu konkretisieren. Sie bringen für die Mitgliedsunternehmen der Verbände Vorteile: Die Aufsichtsbehörde prüft die Verhaltensregeln und schafft damit Rechtssicherheit im Hinblick auf branchentypische Datenflüsse. Für die Betroffenen erhöht sich durch sie die Transparenz über die Art der Verwendung ihrer Daten. Die Branche legt die Datenverarbeitung seiner Unternehmen in den Verhaltensregeln offen und verpflichtet sich hierauf verbindlich. So wird auch die Überprüfbarkeit der Datenverarbeitung verbessert. Die Betroffenen können auf die Festlegungen bauen, weil die Aufsichtsbehörde diese überprüft hat. Trotz dieser Vorteile wurde vom § 38a BDSG bisher praktisch kein Gebrauch gemacht. Genehmigte Verhaltensregeln gab es in Deutschland bisher nicht.

Mit der Erstellung der **Verhaltensregeln** versucht jetzt erstmalig die Versicherungsbranche ihre Verarbeitungsprozesse konkret festzulegen und auf ihre Vereinbarkeit mit dem Datenschutzrecht überprüfen zu lassen. Mit dieser Unterwerfung verpflichten sich die Versicherungsunternehmen, nach den festgelegten Regeln zu verfahren. Datenschutzeinwilligungen dürfen daneben nur eingeholt werden, wenn besonders sensible Daten, z. B. Gesundheitsdaten, verarbeitet werden, oder eine echte, freiwillige Entscheidungsmöglichkeit für den Versicherungsnehmer besteht, z. B. im Bereich der Werbung. Dort kann der Versicherungsnehmer die Einwilligung verweigern, ohne dass dies das Versicherungsverhältnis berührt.

Seit nunmehr anderthalb Jahren verhandelt das ULD, das den Vorsitz der Arbeitsgruppe (AG) Versicherungswirtschaft – der Zusammenschluss der Datenschutzaufsichtsbehörden zum Thema Versicherungen – innehat, mit Vertretern des GDV, der Mitgliedsunternehmen sowie mit Vertretern der Verbraucherschützer (Verbraucherzentrale Bundesverband – vzbv) über die Erstellung der Verhaltensregeln und die Formulierung von Mustereinwilligungserklärungen. Nach endgültiger Einigung zwischen Aufsichtsbehörden und GDV sollen die Verhaltensregeln gemäß dem Bundesdatenschutzgesetz zertifiziert werden. Die Entwürfe der Verhaltensregeln sowie der Mustererklärungen zur datenschutzrechtlichen Einwilligung und zur Schweigepflichtentbindung sollen dem Düsseldorfer Kreis, d. h. dem Zusammenschluss der obersten Datenschutzaufsichtsbehörden in Deutschland, im April 2009 vorgelegt werden. Das ULD ist der Überzeugung, dass die Verhaltensregeln eine Verbesserung im Hinblick auf **Rechtmäßigkeit, Transparenz und Kontrolle** des bisherigen Wildwuchses der Datenverarbeitung in der Versicherungswirtschaft bringen können.

Was ist zu tun?
Aufsichtsbehörden und Versicherungsunternehmen müssen zu den erarbeiteten Formulierungsvorschlägen Stellung nehmen. Konkretisieren die Vorschläge das BDSG und liefern einen Datenschutzmehrwert, so sind die Verhaltensregeln zu zertifizieren – und von Unternehmen zu beachten.

5.5.2 Hinweis- und Informationssystem – Kein Land in Sicht!

Der Versicherungswirtschaft gelang es nicht, ihr Hinweis- und Informationssystem (HIS) bis zum Jahresbeginn 2009 datenschutzkonform umzugestalten. Begründet wird eine Verzögerung dieses Vorhabens um weitere zwei Jahre mit dem unerwartet hohen Entwicklungsaufwand.

Die Versicherungswirtschaft konnte davon überzeugt werden, dass ihr bisher zum Zweck der **Risikobewertung und Betrugsprävention** betriebenes System HIS den Anforderungen des Datenschutzes nicht genügt (30. TB, Tz. 5.1). Eine Beschreibung des bestehenden Systems findet sich im Internet unter:


https://www.datenschutzzentrum.de/wirtschaft/20070703-his.htm

Im November 2007 wurde den Aufsichtsbehörden vom Gesamtverband der Deutschen Versicherungswirtschaft (GDV) ein **Konzept zur Umgestaltung** des Systems vorgestellt, das eine datenschutzkonforme Umsetzung möglich macht. Das Konzept sieht wesentliche Verbesserungen vor. HIS soll zukünftig als zentrale Auskunftei beim GDV betrieben werden. Wie bisher erfolgt eine Trennung der Auskunftserteilung nach Sparten. Wegen der teilweise unterschiedlichen Zielsetzungen wird zwischen Antrags- und Leistungsprüfung differenziert. Die Kommunikation soll über das neue HIS ausschließlich elektronisch erfolgen, sodass Einmeldungen und Abrufe protokolliert und – was bisher nicht möglich ist – so einer Datenschutzkontrolle unterzogen werden können. Die über HIS vermittelten Daten dürfen weiterhin nicht als alleinige Entscheidungsgrundlage herangezogen

werden, sondern sollen lediglich Hinweise zur weiteren Prüfung geben. Nach dem neuen System soll die datenschutzrechtlich geforderte Transparenz – die gesetzlich vorgesehenen Benachrichtigungen und Auskunftserteilungen sind bisher noch nicht effektiv realisiert – umgesetzt werden.

Allerdings wurde dieses Konzept nicht – wie von den Aufsichtsbehörden gefordert – bis zum Jahresbeginn 2009 umgesetzt. Die Umgestaltung von einem dezentralen Auskunfteisystem, bei dem die einzelnen Mitgliedsunternehmen miteinander in Kontakt treten und unkontrolliert Informationen austauschen, zu einer zentralen, vom GDV betriebenen Auskunftei gestaltet sich insbesondere technisch schwieriger als vom GDV gedacht. Die **Online-Anbindung an die Unternehmen**, mit der die Verschickung von CD-ROMs abgelöst werden soll, verursacht offensichtlich einen hohen Aufwand.

Die Verzögerung ändert nichts an den rechtlichen Pflichten nach dem BDSG. Daher sind kurzfristig Maßnahmen zur Verbesserung der datenschutzrechtlichen Position der Betroffenen nötig, vor allem hinsichtlich **mehr Transparenz**. Der GDV hat zugesagt, vom zweiten Quartal 2009 an eine zentrale Auskunftserteilung an die Betroffenen zu gewährleisten. Darüber hinaus sollen die Betroffenen bei Neueinmeldungen durch die Mitgliedsunternehmen benachrichtigt werden.

Zwischen Aufsichtsbehörden und Versicherungswirtschaft besteht noch großer Klärungsbedarf im Hinblick auf die **Kriterien für HIS-Meldungen**. Wann darf an andere Versicherungsunternehmen ein Warnhinweis bezüglich Versicherungsmissbrauch und -betrug sowie bezüglich erhöhter Risiken im Antragsfall gegeben werden? Dies kann nur für Daten gelten, denen Aussagekraft im Hinblick auf diese angestrebten Zwecke zukommt. Eine Arbeitsgruppe mit Vertretern der Aufsichtsbehörden und der Versicherungswirtschaft soll die einzelnen Merkmale auf ihre Einmeldefähigkeit hin überprüfen.

Ergeben sich für Versicherte Unstimmigkeiten bei der Antragstellung oder im Leistungsfall, so ist ihnen zu empfehlen, eine Selbstauskunft über die gespeicherten Daten beim GDV einzuholen. Anhand dieser Informationen können sie – eventuell unter Mithilfe der zuständigen Datenschutzaufsichtsbehörde – überprüfen, ob eine **Einmeldung im Einzelfall** zu Unrecht erfolgte.

Was ist zu tun?
Antragsteller und Versicherungsnehmer sind über den Einsatz von HIS zu informieren und bei Einmeldung in das System zu benachrichtigen. Der GDV steht mehr denn je in der Pflicht, ein datenschutzkonformes HIS zu gestalten und schon jetzt jede mögliche Maßnahme zu ergreifen, die zur Verbesserung der Transparenz und der datenschutzrechtlichen Position der Betroffenen dient.

5.5.3 Finanzdienstleistungsaufsicht kontra Datenschutz

Versicherungsunternehmen sind immer wieder verunsichert, weil sie sich scheinbar widersprechenden Anforderungen der Finanzaufsicht und der Datenschutzaufsicht ausgesetzt sehen. In einem Gespräch zwischen den zuständigen Behörden konnte geklärt werden, dass beide Aufsichtsstränge unabhängig voneinander wahrgenommen werden.

Für die AG Versicherungswirtschaft wandte sich das ULD an die Bundesanstalt für Finanzdienstleistungsaufsicht (BAFin), um widersprechende aufsichtsrechtliche Vorgaben zu vermeiden. Immer wieder kommt es zu scheinbar widersprüchlichen Bewertungen zwischen der BAFin und den Datenschutzbehörden. So betrachteten Versicherungsunternehmen die Genehmigung von **Funktionsübertragungen** nach dem Versicherungsaufsichtsgesetz auf eine andere juristische Person als eine Befugnis zur Übermittlung von Versichertendaten zwischen Funktionsgeber und Funktionsnehmer. Eine datenschutzrechtliche Prüfung wurde aber von der BAFin nicht vorgenommen. Dennoch vertrat die BAFin die Ansicht, derartige Übermittlungen seien zulässig. Die Datenschutzaufsichtsbehörden sahen hierfür aber keine Rechtsgrundlage.

Vergleichbare Konflikte treten auf, wenn die BAFin im Interesse einer möglichst umfassenden Grundlage für ihre Aufsicht die Aufbewahrung von Unterlagen fordert, die aus Datenschutzgründen gelöscht werden müssen. Manches Versicherungsunternehmen meinte aufgrund von Vorgaben der BAFin Versicherungsvermittler bei Auskunfteien ohne datenschutzrechtliche Legitimation auf ihre Bonität hin überprüfen zu dürfen. Unter dem Stichwort „Solvency II“ fordert die BAFin Risikoüberprüfungen der Versicherer, die aber keinesfalls die Durchführung von Scoring-Verfahren bei Versicherten rechtfertigen können.

Um eine Verunsicherung der Versicherungsunternehmen zu vermeiden, suchte die AG Versicherungswirtschaft das Gespräch mit der BAFin. Dabei wurde klargestellt, dass deren Aufsichtstätigkeit sich auf Missbrauchsfälle bei wirtschaftlichen Fragen konzentriert. In keinem Fall ist damit eine **datenschutzrechtliche Bewertung** verbunden, selbst wenn die Vorgaben und Entscheidungen der BAFin Auswirkungen auf die Verarbeitung personenbezogener Daten haben.

Was ist zu tun?
Finanzdienstleister unterliegen sowohl einer fachspezifischen Gewerbeaufsicht als auch einer Datenschutzaufsicht. Diese stehen unabhängig nebeneinander und ergänzen sich. Daher muss bei personenbezogener Datenverarbeitung unabhängig vom Votum der BAFin eine datenschutzrechtliche Zulässigkeitsprüfung vorgenommen werden.

5.6 Dubioses Geschäft mit Zeitschriftenabos

Das Geschäft mit Zeitschriftenabonnements floriert. Ein in Schleswig-Holstein ansässiger Verlagsdienstleister wickelt zwischen dem Leser und dem jeweiligen Vertragspartner Lieferung und Rechnungslegung ab, ohne dass die Verantwortlichkeiten in dieser Dreiecksbeziehung durchschaubar waren.

Der Verlagsdienstleister betreut nach eigenen Angaben mehrere Millionen Verträge. Betroffene Bürgerinnen und Bürger wunderten sich, die Rechnung vom Dienstleister zu erhalten, obwohl sie doch ein Zeitschriftenabonnement bei einer anderen Stelle bestellt hatten. Ihre **Auskunfts- und Löschungsanträge** blieben unbeantwortet. Vielfach existierten gar keine Verträge, da die Betroffenen kein Abonnement bestellt hatten. Trotzdem erhielten sie eine Rechnung vom Dienstleister als Absender. Sie wollten wissen, woher dieser ihre Daten hatte.

Wir stellten fest, dass der Dienstleister im Wege der **Auftragsdatenverarbeitung** tätig wird. Er übernimmt die reine Abwicklung der Verträge auf Weisung des Auftraggebers, wobei die Belieferungsrechte vollständig beim Auftraggeber verbleiben. Datenschutzrechtlich führt dies dazu, dass der jeweilige Auftraggeber verantwortliche Stelle bleibt und damit auch für die Auskunftserteilung zuständig ist. Die Datenverarbeitung ist natürlich nur zulässig, wenn tatsächlich ein Vertrag besteht. Die Schreiben der Betroffenen gingen immer beim Dienstleister als Absender der Rechnung ein, wurden aber nicht weitergeleitet und so auch nicht bearbeitet.

Das ULD forderte eine **Umgestaltung der Vertragsformulare**, der Rechnungen usw., sodass deutlich ist, wer Vertragspartner des Abonnements ist. Zudem ist kenntlich zu machen, dass der Dienstleister als Auftragsverarbeiter

Auftragsdatenverarbeitung nach § 11 Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz privilegiert den Dienstleister, der eine Datenverarbeitung streng nach Weisung seines Auftraggebers durchführt, ohne eigene Entscheidungsmacht über die Daten zu haben. Diese Konstellation nennt das BDSG Auftragsdatenverarbeitung in Abgrenzung zur sogenannten Funktionsübertragung.

Im Falle der Auftragsdatenverarbeitung wird der Dienstleister so behandelt, als gehöre er zur Daten verarbeitenden Stelle. Er ist mithin kein „Dritter" im Sinne des Gesetzes, sodass die Weitergabe der Daten vom Auftraggeber an den Dienstleister nicht den strengen Anforderungen des § 4 Absatz 1 BDSG unterliegt. Es muss weder die Einwilligung des Betroffenen noch eine gesetzliche Rechtsgrundlage gegeben sein, die die Weitergabe legitimiert. Der Auftraggeber muss den Dienstleister allerdings sorgfältig auswählen, ihn vertraglich gem. § 11 BDSG verpflichten, nur nach seinen Weisungen zu handeln und die übergebenen Daten nicht zu eigenen Zwecken zu verwenden sowie die erforderlichen technisch-organisatorischen Maßnahmen für die Verarbeitung zu ergreifen. Der Auftraggeber muss sich zudem der Einhaltung des Vertrages vor Ort versichern. Im Gegensatz dazu findet eine Funktionsübertragung statt, wenn ein gesamter Geschäftsprozess ausgelagert wird und der Dienstleister bei der Datenverarbeitung eigene Entscheidungen trifft.

die Abrechnung übernommen hat. Für die Betroffenen ist nunmehr transparent, wer zu welchem Zweck personenbezogene Daten verarbeitet. Die Auskunfts- und Löschungsbegehren können weiterhin an den Dienstleister gerichtet werden, da dieser durch Beauftragung des Auftraggebers die Erfüllung dieser Datenschutzrechte übernommen hat.

Problematisch bleiben die **fingierten Verträge**. Der Dienstleister kann über das Bestehen oder Nichtbestehen der Belieferungsrechte nicht entscheiden, da er nur die Weisungen des Auftraggebers ausführt. Der Dienstleister muss die Beschwerden an den Auftraggeber weitergeben. Im Fall von Datenschutzbeschwerden muss sich der Betroffene an die für den jeweiligen Auftraggeber zuständige Aufsicht wenden.

Was ist zu tun?
Die Verarbeitung personenbezogener Daten ist für die Betroffenen transparent zu gestalten. Nur so können datenschutzrechtliche Anfragen ordnungsgemäß beantwortet werden.

5.7 Videoüberwachung – Best of

5.7.1 Webcam zum Kaffee – eine beliebte Mischung

Der Einsatz von Videoüberwachung im Freizeitbereich nimmt weiter zu. Gefilmt wird nicht mehr nur „zum Dienstgebrauch"; die Aufnahmen landen häufig im Internet oder werden für dieses gemacht.

In einem schon länger anhängigen Verfahren geht es um die übermäßige Videoüberwachung von **Kunden und Beschäftigten** eines über die Grenzen Schleswig-Holsteins hinaus tätigen Caféhausbetreibers (30. TB, Tz. 5.8.1). Jugendliche und Studierende gehören zur vorrangigen Zielgruppe des Unternehmens, das ausdrücklich mit der „Loungeatmosphäre" und der Möglichkeit wirbt, sich dort mit Freunden zu treffen und zu entspannen. Nahmen die Angesprochenen dieses Angebot wahr, konnten sie sicher sein, dass der Betreiber auch elektronisch ein Auge darauf warf, dass er sein Werbeversprechen einhält. Überwacht wurden nicht nur die Freizeitbereiche, sondern auch die Räume, in denen sich die Beschäftigten des Unternehmens aufhielten und arbeiteten. Niemand blieb unbeobachtet. Erschwerend kam hinzu, dass Kameras teilweise unauffällig oder verdeckt angebracht waren und auf den Umstand der Überwachung nicht wirksam hingewiesen wurde.

Das Unternehmen rechtfertigte sich mit dem Schutz vor Diebstahl und Vandalismus, aber auch mit der Einhaltung von Hygienevorschriften durch die **Beschäftigten**. Nicht nur dass eine wirksame Rechtsgrundlage für die Überwachung der Beschäftigten fehlte, die Videoüberwachung war so umfangreich, dass selbst bei viel Verständnis für unternehmerische Gründe keine ausreichende Rechtfertigung bestand. Die optisch-elektronische Überwachung von Arbeitnehmerinnen und Arbeitnehmern greift umfassend in deren Persönlichkeitsrechte ein und kann einen Anpassungsdruck und Verhaltensänderungen bewirken. Anders als bei der Über-

wachung eines unbestimmten Personenkreises in öffentlich zugänglichen Räumen, sind sie persönlich bekannt; jede Verhaltensweise und Kommunikation unterliegt der Beobachtung, Kontrolle und der grundsätzlich unbegrenzten Bildreproduktion und -auswertung durch den Arbeitgeber. Wer nicht sicher ist, zu welchem Zweck und wann er überwacht wird, wird versuchen, sich angepasst zu verhalten. Dieser Anpassungsdruck wird durch die wirtschaftliche Abhängigkeit der Beschäftigten vom Arbeitgeber verstärkt. Auch im nicht öffentlichen Bereich darf durch technische Überwachung kein Duckmäusertum erzeugt werden.

Betroffen sind zudem die **überwachten Gäste**, welche die Gasträume und die bereitgestellten Bereiche vor allem in ihrer Freizeit aufsuchen, z. B. zur Erholung und zur Kommunikation mit Freunden. In dieser Situation sind die Betroffenen besonders schutzwürdig; Freizeitverhalten ist gekennzeichnet durch eine geringere Beachtung gesellschaftlicher Konventionen. Üblicherweise benimmt man sich in solchen Situationen ungezwungener und weniger förmlich. Durch die Videoüberwachung verliert der Augenblick seine Flüchtigkeit. Das private Verhalten wird zum Gegenstand einer potenziell dauerhaften und in jedem Fall intransparenten Kontrolle. Wegen der fehlenden klaren Information konnten die Kundinnen und Kunden nicht erkennen, ob und in welchem Maße sie einer Videoüberwachung ausgesetzt waren.

Das ULD sah sich veranlasst, im konkreten Fall die Datenschutzverstöße mit einem **Bußgeld** in nicht unerheblicher Höhe zu ahnden.

Videokontrolle ist ein immer häufiger zu beobachtendes Phänomen in der Gastronomie. In einem anderen Fall stellte der Betreiber eines Strandcafés Aufnahmen des Außenbereichs und der dort sitzenden Gäste ins Internet. Weltweit konnte so nachvollzogen werden, wer sich hier mit wem traf und was konsumierte. Der Betreiber wollte sein Unternehmen derart werbewirksam **im weltweiten Netz präsentieren**, übersah jedoch, dass er massiv in die Persönlichkeitsrechte der Kundinnen und Kunden eingriff. Darauf hingewiesen, änderte er umgehend den Erfassungsbereich der Kamera, sodass Personen nicht mehr erkennbar waren. Der Werbeeffekt der Kamera blieb erhalten, und die Rechte der Betroffenen werden gewahrt.

Für **Liveaufnahmen im Internet** gilt wie für eingestellte Inhalte generell, dass die Betreiber unverzüglich die Kontrolle über die Inhalte und diese ihre Flüchtigkeit verlieren. Die Bildsequenzen können weltweit von Unbekannten nicht nur eingesehen, sondern auch gespeichert und reproduziert werden. Den Betroffenen ist es unmöglich zu erfahren, was mit diesen Aufnahmen geschieht. Gegen deren Missbrauch gibt es praktisch kein wirksames Mittel. Zahlreiche Beispiele auf einschlägigen Internetdiensten wie z. B. Youtube zeigen dies eindringlich. Die Speicherung und Reproduktion der Aufnahmen ist selbst für Laien kein Problem.

Durch Webcams ins Internet gestellte Videosequenzen beeinträchtigen die Betroffenen unabhängig vom Kontext der Aufzeichnung. Sie können deren Verbreitung und Nutzung weder lenken noch verhindern. Auch für die Betreiber von Webcams können die Kameras zum **unkalkulierbaren Risiko** werden, z. B. wenn ein Betroffener seine persönlichkeitsrechtlichen Ansprüche zivilrechtlich geltend

macht. Dies kann immer passieren, wenn Personen erkennbar sind, selbst wenn diese nur mit Zusatzwissen identifiziert werden können.

Was ist zu tun?
Videoüberwachung betrifft die Persönlichkeitsrechte der Menschen und ist daher nur in Ausnahmefällen gerechtfertigt. Die Veröffentlichung von per Webcam erstellten Personenaufnahmen im Internet ist in jedem Fall unzulässig. Beim Webcam-Einsatz muss jedes Mal sichergestellt werden, dass die Persönlichkeitsrechte Dritter nicht verletzt werden.

5.7.2 Videoüberwachung im Rauchmelder

Bei zwei Datenschutzkontrollen fielen Arbeitgeber durch besonders perfide Überwachungsmaßnahmen auf: Sie hatten illegal Videokameras als Rauchmelder getarnt installiert.

Die falschen Rauchmelder wurden vom ULD bei einem Hersteller von Orthopädiegeräten und bei einem Zahnarzt entdeckt. Die optisch-elektronische Überwachung von öffentlich zugänglichen Bereichen, also Räumen, die für den Zugang eines unbestimmten Personenkreises bestimmt und geeignet sind, darf nach dem Gesetz nur offen erfolgen. Betroffene müssen in der Lage sein, ohne Weiteres zu erkennen, ob sie sich im **Erfassungsbereich einer Kamera** befinden. Als Rauchmelder getarnte Kameras verschleiern den Umstand der Überwachung und sind daher unzulässig. Entsprechendes gilt für den Einsatz solcher Kameras im nicht öffentlichen Bereich.

Risikohaft kann zudem sein, dass sich Menschen darauf verlassen, dass der vermeintliche Rauchmelder im Fall eines Feuers Alarm schlägt. Beim Einsatz in der Zahnarztpraxis kam erschwerend hinzu, dass die Kamera so angebracht war, dass auch Patientinnen und Patienten erfasst wurden. Damit war die Gefahr der Verletzung des Arztgeheimnisses gegeben. In beiden Fällen führte die Intervention des ULD zum **Abbau der Geräte**.

Was ist zu tun?
Eine Überwachungskamera muss offen und als solche erkennbar installiert sein. Auf den Umstand der Überwachung muss unzweifelhaft hingewiesen werden. Wird dies missachtet, ist der Einsatz der Kamera unabhängig von Einsatzzweck und -ort unzulässig.

5.7.3 Bild und Ton im Bordell

Kein Bereich des gesellschaftlichen Lebens wird von der Videoüberwachung verschont. So prüfte das ULD Bild- und Tonaufnahmen in einem Bordell.

Die Betreiber eines Laufhauses hatten auf den **Gängen und Treppen** eine Video- und Tonüberwachungsanlage installiert. Kunden der dort tätigen Frauen und die

geführten Gespräche wurden nicht nur visuell, sondern auch akustisch überwacht, jedoch – nach unseren Erkenntnissen – nicht gespeichert. Die überwachten Bereiche konnten durch einen Bordellmitarbeiter auf einem Monitor eingesehen und abgehört werden. Die gewonnenen Erkenntnisse wurden von uns auch anderen Bordellen im Land mitgeteilt, verbunden mit der Aufforderung, die Datenschutzregeln einzuhalten.

Das ULD geht von einem hohen Schutzbedürfnis der in einem Bordell tätigen Frauen aus und erhob keine Einwände gegen die **Bildüberwachung** der Flure und Treppen. Das Gefährdungspotenzial für Leib und Leben der Frauen in diesem Bereich ist so hoch einzuschätzen, dass die Persönlichkeitsrechte der Kunden zurückstehen und diese die Videobeobachtung dulden müssen. Voraussetzung ist aber, dass die Videoüberwachung schon vor dem Betreten des Bordells erkennbar ist, d. h. gut sichtbar angezeigt wird, die Daten nicht gespeichert und ausschließlich zum Schutze der Frauen genutzt werden.

Anderes gilt für die **Tonüberwachung**. Damit ist kein signifikanter Sicherheitsgewinn für die Frauen verbunden. Vielmehr werden diese unter dem Eindruck, es könnten Dritte das Gespräch mithören, gehindert, offene Gespräche mit Freiern zu führen, aber auch z. B. mit Vertretern der Ordnungsbehörden oder der Polizei. Unser Strafgesetzbuch stellt das Abhören des nicht öffentlich gesprochenen Wortes unter Strafe.

Was ist zu tun?
Videoüberwachung in der Privatwirtschaft, die dem Schutz von Leib und Leben dient, kann nach Interessenabwägung zulässig sein. Tonüberwachung ist generell unzulässig.

5.7.4 Videoüberwachung im Bus – Weitergabe an die Presse

Der Beitrag eines Fernsehsenders machte das ULD auf ein Linienbusunternehmen aufmerksam, das seine Mitarbeiterinnen und Mitarbeiter in den Fahrerkabinen einer permanenten Videoüberwachung aussetzt und Aufnahmen eines Zwischenfalls an die Presse weitergab.

Der Fernsehsender hatte Bilder über den **Zusammenbruch eines Busfahrers** ausgestrahlt, der beinahe zu einem Unfall geführt hätte. Der betroffene Fahrer war ohne Weiteres zu erkennen. Er hatte der Weitergabe an die Presse und der Ausstrahlung nicht zugestimmt.

Die Installation einer Videokamera am Arbeitsplatz setzt das Vorliegen eines berechtigten Grundes voraus, der gegenüber den schutzwürdigen Interessen der Beschäftigten überwiegt. Die Unternehmensleitung begründete die Kontrolle der Fahrerkabine mit dem Schutz der Mitarbeiterinnen und Mitarbeiter vor Überfällen. Es gab weder eine **Betriebsvereinbarung** noch anderweitige Regelungen zu Löschfristen, Verwendungszweck, Zugriff oder Dauer.

Das Verfahren ist noch nicht abgeschlossen. Schon jetzt ist klar, dass insbesondere die Weitergabe der unverfremdeten Aufnahmen an die Presse einen Verstoß gegen geltendes Datenschutzrecht darstellt, da weder eine **Rechtsgrundlage** ersichtlich ist, noch die Einwilligung des betroffenen Busfahrers vorlag. Die Installation einer Videoanlage zur Überwachung von Arbeitnehmern setzt eine sorgfältige Abwägung der Interessen beider Seiten voraus. Das pauschale Argument höherer Sicherheit genügt nicht als Rechtfertigung. Ist ein Betriebsrat vorhanden, sollte in jedem Fall eine schriftliche Betriebsvereinbarung erarbeitet werden, in der Zweck, Dauer und Umfang der Überwachung geregelt werden. Eine Verarbeitung zum Zweck der Leistungs- und Verhaltenskontrolle muss schriftlich ausgeschlossen werden, insbesondere wenn es auschließlich um Sicherheitsinteressen der Mitarbeiter geht.

Einwilligung der Betroffenen nach § 4 Abs. 1 Bundesdatenschutzgesetz

§ 4 Abs. 1 Bundesdatenschutzgesetz fordert u. a. für die Übermittlung personenbezogener Daten das Vorliegen einer Rechtsgrundlage oder der Einwilligung (vorherige Zustimmung) des Betroffenen. Im Arbeitsverhältnis müssen aufgrund des Abhängigkeitsverhältnisses stets hohe Anforderungen an die erforderliche Freiwilligkeit der Einwilligung gestellt werden.

Was ist zu tun?
Videoüberwachung im Unternehmen sollte in jedem Fall mit dem Betriebsrat in einer Betriebsvereinbarung geregelt werden. Eine Weitergabe von unverfremdeten Aufnahmen an die Presse ohne die ausdrückliche Einwilligung des Betroffenen muss unterbleiben. Auch verfremdete Aufnahmen sollten nicht ohne Einwilligung an Dritte übermittelt werden.

5.8 Einzelfälle

5.8.1 Mülltonnen – Spiegel funktionierender Datenvernichtung

Aufmerksame Bürgerinnen und Bürger haben das ULD in zwei Fällen auf die unzulässige Entsorgung von teilweise sensiblen personenbezogenen Datenbeständen in Mülltonnen hingewiesen.

Im ersten Fall wurden ganze **Bewerbungsmappen** in einem öffentlichen Abfalleimer gefunden. Das ULD hat zunächst die betroffenen Bewerberinnen und Bewerber benachrichtigt. Das verantwortliche Unternehmen gab auf unsere Fragen nach den konkreten Umständen und den bestehenden generellen Regelungen an, ein Auszubildender, der inzwischen nicht mehr im Unternehmen tätig sei, habe die „Entsorgung“ ohne Wissen der Verantwortlichen vorgenommen. Bewerbungsunterlagen, die neben Adressdaten meist ausführliche Informationen über Werdegang und Persönlichkeit eines Menschen enthalten, sind – sollten sie nach einer erfolglosen Bewerbung nicht an die Bewerberin bzw. den Bewerber zurückgesandt werden – ordnungsgemäß zu vernichten. Mit Einwilligung der Betroffenen können die Unterlagen auch über die Frist des Allgemeinen Gleichbehandlungsgesetzes

hinaus aufbewahrt werden, um sie zu weiteren Auswahlverfahren hinzuzuziehen. Allgemein sollte festgelegt werden, an welchem Ort die Bewerberdaten aufzubewahren sind und wer Zugriff auf sie erhält.

Im zweiten Fall wurde versucht, teilweise sehr sensible Unterlagen der **Zweigstelle einer großen Versicherungsgruppe** zu beseitigen. Das Material wurde in einer Mülltonne auf einem Hinterhof, auf die alle anderen Bewohner des Hauses Zugriff hatten, gefunden. Da die Verantwortlichen angaben, keine Kenntnis von den Vorfällen gehabt zu haben, hat das ULD die zuständige Hauptstelle benachrichtigt und Nachweise einer grundsätzlich ordnungsgemäßen Aktenvernichtung und einer entsprechenden Schulung der Mitarbeiterinnen und Mitarbeiter gefordert.

Was ist zu tun?
Unterlagen mit Personenbezug sind, sobald sie nicht mehr benötigt werden, ordnungsgemäß zu vernichten. Regelungen zu Aufbewahrung und Zugriff sollten festgelegt werden, um das Risiko des Abhandenkommens oder eines unberechtigten Zugriffs möglichst gering zu halten. Unzulässiger Datenentsorgung wird durch Schulungen der Mitarbeiter und durch ein geregeltes Abfallmanagement mit Einsatz von Aktenvernichtern entgegengewirkt.

5.8.2 Wertpapierhandelsgesetz – die umfangreichen Kundenfragebögen

Die Versendung von Fragebögen durch Sparkassen in Schleswig-Holstein löste eine Beschwerdewelle beim ULD aus. Es handelte sich um Bögen für die Durchführung von Wertpapierdienstleistungen mit detaillierten Fragen zum Bildungsstand, Beruf der Betroffenen und vieles mehr.

Die Petenten zeigten sich verwundert über die umfängliche Datenerhebung. Die Erfassung der Daten ihrer Art und ihrem Umfang nach entspricht im Grunde der Gesetzeslage. Eine europäische Richtlinie verpflichtet die nationalen Gesetzgeber, die Wertpapierdienstleistungsunternehmen zu veranlassen, Daten über Bildungsstand, Beruf, Einkommen und Wertpapiererfahrungen zu erheben, um sicherzustellen, dass eine für den Verbraucher verständliche und an seinen Bedürfnissen orientierte Beratung erfolgt. Wird ausweislich dieser Angaben falsch beraten, so erhöht dies für den Dienstleister das Haftungsrisiko. Die Regelung dient also im Grundsatz dem Verbraucherschutz. Die Daten unterliegen dem „Beratungsgeheimnis“ und dürfen nur **streng zweckgebunden** gespeichert und verwendet werden und nicht an andere Sparten bzw. Unternehmensteile des Wertpapierdienstleisters weitergegeben und dort genutzt werden.

Allerdings ist der versendete Fragebogen in einigen Teilen intransparent und führt zu Verunsicherungen bei den Kunden. So wird z. B. nicht darauf hingewiesen, dass die Angaben bei einer bloßen An- oder Verkauforder ohne weitere Beratung nicht erhoben werden müssen. Zudem wird aus dem Fragebogen nicht deutlich, dass die Daten ausschließlich zum Zweck der Prüfung von Angemessenheit und Geeignetheit einer bestimmten Wertpapierdienstleistung in Bezug auf den individuellen Kunden erhoben und verarbeitet und anderweitig nicht genutzt werden dürfen. Es

entspricht zudem nicht dem **Grundsatz der Erforderlichkeit** und dem Verbot einer Vorratsdatenerhebung, wenn Daten erhoben und erfasst werden, die für die konkret beabsichtigten Geschäfte nicht nötig sind, wohl aber im „Interesse einer umfassenden Geschäftsbeziehung". Diese in den Fragebögen zu findende Formulierung ist zudem missverständlich, da sie die strenge Zweckbindung der Daten faktisch aufhebt. Es muss erkennbar sein, dass für unterschiedliche Beratungssituationen auch ein unterschiedlicher Umfang an Daten erforderlich ist.

Bei der Formulierung von Fragebögen, Anträgen usw., mit denen Daten beim Kunden erhoben werden, ist ein aussagekräftiger und unmissverständlicher Datenschutzhinweis aufzunehmen. Insbesondere ist der Kunde darüber zu informieren, zu welchem Zweck die Daten Verwendung finden sollen und welche konkreten Folgen es hat, wenn Angaben verweigert werden. Im Falle einer gesetzlichen Verpflichtung zur Erhebung von Daten ist die entsprechende Vorschrift zu zitieren. Wenn Angaben für das abzuwickelnde Geschäft nicht erforderlich sind, so sind sie als freiwillige Angaben explizit zu kennzeichnen. Es darf nicht der Eindruck erweckt werden, dass die Verweigerung von freiwillig zu machenden Angaben zu einem Ausschluss der Leistung führt. Das ULD steht im Austausch mit dem Sparkassenverband, um eine **datenschutzkonforme Änderung der Fragebögen** zu erreichen.

Was ist zu tun?
Die Formulare müssen gemäß den Datenschutzvorgaben, also transparent und unter Wahrung der Datensparsamkeit, gestaltet werden.

5.8.3 Laptop auf Abwegen

Ein Computerunternehmen hatte ein repariertes Notebook mit einer Fülle sensibler personenbezogener Daten auf der Festplatte anstatt dem Besitzer einem Dritten zugeschickt.

Das Brisante an dem Vorfall: Bei dem Empfänger des Notebooks handelte es sich um den **geschiedenen Ehemann der jetzigen Lebensgefährtin** des Bürgers. Auf der Festplatte des reparierten Notebooks befanden sich Informationen, die gerichtlich gegen den irrtümlichen Empfänger des Gerätes verwendet werden sollten und nun der Gegenseite bekannt geworden waren. Das Computerunternehmen erklärte, dass die Daten des geschiedenen Ehemannes, der ebenfalls Kunde war, im Zusammenhang mit der Seriennummer des Gerätes versehentlich für die Versendung des Notebooks verwendet wurden. Eindeutige schriftliche Regelungen hinsichtlich der Rücksendung von Geräten mit Datenspeichern existierten in der Firma nicht.

Die Rücksendung des Notebooks an den falschen Empfänger war eine unzulässige Datenübermittlung und wurde vom ULD zudem wegen fehlender technischer und organisatorischer Sicherheitsmaßnahmen beanstandet. Das Unternehmen wurde aufgefordert, entsprechende **innerbetriebliche Arbeitsanweisungen** zu erstellen, um derartige Fehler künftig möglichst zu vermeiden. Dem kam die Firma –

zögerlich – nach. Der geschädigte Bürger wurde auf die Möglichkeit aufmerksam gemacht, gegebenenfalls gerichtlich gegen das Computerunternehmen vorzugehen.

Was ist zu tun?
Speziell Computerfirmen müssen streng darauf achten, dass Geräte mit Datenspeichern nach der Reparatur nur an den Berechtigten zurückgegeben werden.

5.8.4 Werbewiderspruch – mit guten Augen klar im Vorteil

Das Bundesdatenschutzgesetz verlangt, die Adressaten von Werbung deutlich darauf hinzuweisen, dass sie der Nutzung ihrer Daten zu Werbezwecken widersprechen können.

Ein norddeutsches Unternehmen mit mehreren Filialen führt regelmäßig umfangreiche persönlich adressierte Briefkampagnen durch, um mit interessanten Neuigkeiten und Informationen zum Kauf zu werben. In den verwendeten Werbeflyern konnten wir den gesetzlich geforderten Widerspruchshinweis aufgrund der Fülle der Informationen erst nach mehrmaligem Durchsehen der gesamten Werbeinformationen entdecken. Dies ist nicht Intention des Gesetzes. Es gibt zwar keine Formvorschriften für den Widerspruchshinweis, jedoch muss die Gestaltung der Bedeutung des Widerspruchsrechts entsprechen. Es bedurfte mehrmaliger Versuche von Werbegestaltern, bis diesem Erfordernis genügt wurde. Künftig enthalten die Werbesendungen **zwei Widerspruchshinweise**: Einer wird bereits auf dem Briefumschlag, der zweite – deutlich vom übrigen Text getrennt – im persönlichen Anschreiben der Werbeflyer platziert.

Was ist zu tun?
Bei der Ansprache des Betroffenen zu Werbezwecken ist es erforderlich, den gesetzlich geforderten Widerspruchshinweis optisch hervorzuheben und von allen anderen Informationen deutlich zu trennen.

5.8.5 Es gibt kein Konzernprivileg

Ein Bürger bekam von einer privaten Briefzustellfirma einen Telefonanruf, obwohl seine Telefonnummer seit Jahren in keinem öffentlich zugänglichen Telefonverzeichnis und auch nicht im Internet enthalten ist.

Bei dem Telefonanruf ging es um die Abholung einer unzustellbaren Briefsendung. Auf die Nachfrage des Bürgers, woher die Briefzustellfirma seine Telefonnummer habe, erhielt er keine zufriedenstellende Antwort. Erst nach Einschaltung des ULD und Zuziehung eines Rechtsanwalts durch das Unternehmen fand sich des Rätsels Lösung. Die Briefzustellfirma ist Tochtergesellschaft eines großen **Zeitungsverlages**. Bei diesem Zeitungsverlag hatte die Ehefrau des Bürgers seit vielen Jahren ein Abo für eine Tageszeitung. Die Daten der Ehefrau einschließlich der Telefonnummer waren in der EDV-Anlage des Verlages gespeichert. Die Mitarbeiterin der

Briefzustellfirma beschaffte sich die Telefonnummer – die auch die Telefonnummer des Ehemannes war – vom Verlag, also der Muttergesellschaft, und rief an.

Der anwaltlich vertretene Verlag meinte tatsächlich, die Übermittlung der nicht veröffentlichten Telefonnummer von der Mutter- an die Tochtergesellschaft sei zulässig. Im Konzern gebe es einen einheitlichen Verarbeitungszweck der Daten. Dem mussten wir widersprechen. Das Bundesdatenschutzgesetz kennt nicht den Begriff des Konzerns und auch **kein Konzernprivileg**. Jede einzelne Gesellschaft als juristische Person, auch die Mutter, ist Normadressat des Gesetzes. Datentransfers innerhalb eines Konzerns – soweit keine Auftragsdatenverarbeitung vorliegt – sind ebenso zu behandeln wie Übermittlungen aus dem Konzern heraus.

Es liegt nicht im Rahmen der Zweckbestimmung eines Abonnementvertrages mit einem Zeitungsverlag, eine Kundentelefonnummer einer Briefzustellfirma zu übermitteln, auch nicht wenn die Empfängerfirma zum gleichen Konzern gehört. Die Übermittlung der Telefonnummer war unzulässig. Das schutzwürdige Interesse des Betroffenen an der Nichtweitergabe einer **nicht veröffentlichten Telefonnummer** überwiegt in jedem Fall gegenüber dem berechtigten Interesse der Briefzustellfirma. Im Rahmen einer Beanstandung hat das ULD den Zeitungsverlag aufgefordert, derartige Übermittlungen in Zukunft zu unterlassen.

Zuletzt teilte der Verlag dem ULD mit, die Telefonnummer der Ehefrau sei vom Ehemann bei der Aufgabe von mehreren Anzeigen **selbst angegeben** und dann an die Briefzustellfirma weitergegeben worden. Dieser Vortrag ändert nichts an der rechtlichen Bewertung. Das überwiegende schutzwürdige Interesse an der Nichtweitergabe einer nicht veröffentlichten Telefonnummer bleibt bestehen. Gleichzeitig machte der Verlag den Vorschlag, zusammen mit dem ULD eine wirksame Einwilligungserklärung für derartige Fälle zu erarbeiten. Vielleicht kann das grundsätzlich bestehende Problem so zu einem guten Ende geführt werden.

Was ist zu tun?
Der Aufklärungsbedarf scheint groß zu sein: Gerade große Unternehmen müssen endlich begreifen, dass es im Datenschutzrecht kein Konzernprivileg gibt. Andere Konzerngesellschaften sind zu behandeln wie Fremdfirmen.

5.8.6 Veröffentlichung von Spielergebnissen im Internet

Das Mitglied eines Tischtennisvereins wandte sich dagegen, dass regionale Turnier- und Meisterschaftsergebnisse ausführlich im globalen Internet präsentiert werden und von Internetsuchmaschinen zu finden sind.

Neben den reinen Spielergebnissen und der Vereinszugehörigkeit der Spielerinnen und Spieler konnten Informationen wie Mannschaftsaufstellungen und Ähnliches abgerufen werden – alles **ohne Einwilligung** oder auch nur vorherige Informationen der Betroffenen. Insbesondere die Möglichkeit, über eine **Suchmaschine** an persönliche Daten zu gelangen, stieß beim Petenten auf Unverständnis, da so jeder Internetnutzer leicht darauf Zugriff erhält.

Die Einstellung der Informationen ins Internet erfolgt auf Veranlassung des zuständigen Sportverbands. Wegen der großen Anzahl betroffener Verbandssportler wurde auf die Einholung und Berücksichtigung von Einwilligungen verzichtet. Das ULD schlug vor, den Vereinen im Rahmen der nächsten Versammlung des Verbandes zu erläutern, dass eine Veröffentlichung von personenbezogenen Daten – etwa in Form von Spielergebnissen unter Nennung der Namen – im Internet ohne Einwilligung unzulässig ist. Sodann sollen die **Vereine an ihre Mitglieder herantreten** und entsprechende Einwilligungen einholen. Bei Nichtvorliegen einer Einwilligung dürfen keine Informationen über eine Spielerin oder einen Spieler und auch nicht deren Spielergebnisse veröffentlicht werden.

Einfacher umzusetzen ist der alternative Vorschlag des ULD. Bei Mannschaftssportarten können die Ergebnisse ohne Nennung der einzelnen Spielerinnen und Spieler veröffentlicht werden. Um der Problematik des Zugriffs auf die Ergebnisse über eine Internetsuchmaschine entgegenzuwirken, kann die gesamte Webseite so markiert werden, dass sie beim Suchen nicht erfasst wird. Möglich ist auch, einen **geschlossenen Mitgliederbereich** einzurichten. Allerdings müssen auch hierbei Einwilligungen der Betroffenen eingeholt werden.

? Einwilligung

Bei Einholung einer Einwilligung ist darauf zu achten, dass diese freiwillig erteilt wird, jederzeit widerrufen werden kann und dass den Betroffenen die Tragweite ihrer Einwilligung bewusst ist.

Was ist zu tun?
Zur Veröffentlichung von personenbezogenen Daten im Internet ist im Vereinsbereich die Erteilung einer Einwilligung der betroffenen Mitglieder notwendig, da der Adressatenkreis im Internet nahezu unbegrenzt ist. Die Einwilligung kann bereits bei Vereinseintritt im Rahmen des Aufnahmeantrags eingeholt werden.

5.8.7 Radio-Gewinnspiel – Rückruf trotz Rufnummernunterdrückung?

Ein schleswig-holsteinischer Radiosender veranstaltete ein Telefongewinnspiel, wobei Anrufer ohne Hauptgewinn durch Drücken der Telefontaste „1“ die Möglichkeit hatten, kostenlose Lottotipps abzugeben. Die Teilnehmenden wussten nicht, dass der Sender hierzu die Rufnummernunterdrückung der Anrufenden aufheben konnte.

In beiden Ansagevarianten, die den Anrufenden vorgespielt wurden, wurde zwar darauf hingewiesen, dass die Rufnummer gespeichert werden sollte. Dass der Gewinn der kostenlosen Lottotipps allerdings zwingend mit einem Rückruf des Partnerunternehmens des Radiosenders verbunden ist und zu diesem Zweck auch Rufnummernunterdrückungen ohne ausdrückliche Einwilligung der Anrufenden aufgehoben werden, wurde nicht deutlich gemacht.

Die sich beschwerende Bürgerin war davon ausgegangen, ihre freien Lottotipps sofort abgeben zu können. Von einer Übermittlung ihrer Daten, insbesondere ihrer Telefonnummer, ahnte sie nichts. Die Telefonnummer fällt nicht unter das sogenannte **Listenprivileg** des Bundesdatenschutzgesetzes, ihre Nutzung ist ohne Einwilligung des Betroffenen grundsätzlich unzulässig. Das ULD verlangte daher die Ergänzung der Ansagen um Informationen zur Aufhebung der Rufnummernunterdrückung sowie zur Weitergabe der Daten an das kooperierende Lottounternehmen, das ebenfalls näher bezeichnet werden sollte.

? Das Listenprivileg

Personenbezogene Daten, die unter das Listenprivileg nach dem Bundesdatenschutzgesetz fallen, also Name, Beruf, Anschrift und Geburtsjahr, dürfen zu Zwecken der Werbung oder Markt- und Meinungsforschung, soweit keine schutzwürdigen Interessen des Betroffenen entgegenstehen, genutzt oder an Dritte übermittelt werden. Der Betroffene hat allerdings die Möglichkeit, diesem Vorgehen zu widersprechen.

Zudem wurde während des Telefonats auf die **Teilnahmebedingungen**, die man bereits durch Verbleiben in der Leitung akzeptierte, im Internet hingewiesen. Die Teilnehmenden hatten bei diesem Ablauf keine Möglichkeit, sich im Vorhinein über die Rahmenbedingungen des Gewinnspiels zu informieren. Das ULD schlug vor, bereits während der entsprechenden Radiobeiträge auf die Teilnahmebedingungen im Internet hinzuweisen und denjenigen, die nicht über einen Internetzugang verfügen, die Möglichkeit zu geben, die Teilnahmebedingungen postalisch zu erhalten.

Was ist zu tun?
Die technische Unterdrückung von Rufnummern darf nur mit Einwilligung der Betroffenen und unter Festlegung des Zwecks aufgehoben werden. Auf Teilnahmebedingungen im Internet sollte bereits bei Ankündigung des Gewinnspiels hingewiesen werden. Interessierte ohne Internetzugang müssen eine alternative Kenntnismöglichkeit erhalten.

5.8.8 Creditreform – Aufforderung zum Datenabgleich an Betroffene

Die Wettbewerbszentrale machte das ULD darauf aufmerksam, dass Auskunfteien Personen anschrieben und diese aufforderten, ein beigefügtes Datenblatt mit den bei der Auskunftei über die Person gespeicherten Daten zu überprüfen und zu korrigieren, sollten die Daten nicht richtig sein. Werde auf das Anschreiben nicht reagiert – so wurde teilweise ausgeführt – „gehe man davon aus", dass die Darstellungen korrekt seien.

Betroffen waren Kleinstgewerbetreibende, Einzelkaufleute sowie ein Verein und seine Vorstandsmitglieder. Auf den Anschreiben fehlte ein ausdrücklicher Hinweis, dass die **Angaben freiwillig** sind. Die Auskunfteien wollten keinen datenschutzrechtlichen Verstoß erkennen. Den Angeschriebenen stehe es frei, auf das Schreiben zu reagieren oder dies zu ignorieren. Diese Auffassung teilte das ULD nicht und beanstandete das Vorgehen.

Das Anschreiben der Auskunfteien initiiert eine Datenerhebung, auch wenn es nur um die Korrektur vorhandener Angaben geht, und ist Teil eines Erhebungsvorganges. Im Anschreiben muss daher den gesetzlich geforderten Unterrichtungsverpflichtungen genügt werden. Richtig ist, dass die Mitteilung des Datensatzes einen für den Betroffenen positiven Effekt haben kann. Gegenüber der verbreiteten Auskunfteivorgehensweise erfolgt die Erhebung in diesem Fall nicht hinter dem Rücken der Betroffenen bei Dritten, sondern direkt bei diesem selbst. Der Betroffene kann Korrekturen oder Gegendarstellungen veranlassen, die ansonsten bis zur Selbstauskunft unaufgedeckt geblieben wären. Damit werden **Transparenz und Einwirkungsmöglichkeiten** erhöht. Zugleich erhält der Betroffene eine kostenlose Selbstauskunft.

> **? *Personenbezogene Daten – Daten juristischer Personen***
>
> *Grundsätzlich fällt die Verarbeitung von Angaben zu juristischen Personen nicht unter das Bundesdatenschutzgesetz, da dieses nur personenbezogene Daten, d. h. Daten von natürlichen Personen erfasst. Wenn sich die Unternehmensdaten allerdings auf natürliche Personen beziehen lassen und die Einzelperson, z. B. den Firmeninhaber, persönlich betreffen, handelt es sich auch hier um personenbezogene Daten.*
>
> *Bei Einzelgewerbetreibenden, Einzelfirmen, Freiberuflern und Einmann-GmbHs steht hinter der juristischen Person regelmäßig eine natürliche Person, sodass Personenbezug gegeben ist und das Datenschutzrecht Anwendung findet.*

Diese positiven Effekte stellen sich allerdings nur ein, wenn der Betroffene ausreichend darüber informiert wird, ob und wie seine Daten verarbeitet werden, und ihm hinreichend deutlich gemacht wird, dass die Angabe von Daten freiwillig ist. Dies ist nicht der Fall, wenn der Betroffene mit dem Anschreiben **indirekt zur Mitwirkung gezwungen** wird, indem an die Nichtäußerung eine bestimmte Konsequenz geknüpft wird. Das ULD hat die betroffenen Auskunfteien aufgefordert, ihr Vorgehen zu ändern und ihre Anschreiben entsprechend umzugestalten.

5.8.9 Unberechenbare Fotobestellung

Celluloid ist out. Digitalfotografie ist in. Wer aber weiterhin Papierbilder in ein Fotoalbum kleben möchte, der muss bei einem Anbieter eine digitale Fotobestellung vornehmen. Dabei dürfen nicht mehr Daten als unbedingt nötig erfasst werden.

Digitale Fotobestellungen erfolgen über das Internet oder über einen Terminal in einem Fotoladen. Eine Kundin war sehr erstaunt, dass sie, nachdem sie per USB-Stick Bilder bestellt hatte, nicht nur diese Bilder, sondern auch eine CD-ROM erhielt, auf der nicht nur ihre Bilder, sondern viele andere private Dateien in verschiedenen Bild- und Textformaten gespeichert waren, die sich gemeinsam mit den Bildern auf dem zur Bestellung genutzten USB-Stick befanden. Der Anbieter erklärte uns lapidar, dass „aus technischen Gründen“ **alle Daten des Datenträgers** kopiert würden. Bearbeitet würden nur die Fotodateien. Erst nachdem das ULD dem Unternehmen ankündigte, öffentlich auf die Risiken hinzuweisen, die mit der Fotobestellung verbunden sind, sah sich der Anbieter

veranlasst, inhaltlich zu antworten. Die ursprünglich eingesetzte Software, die eine vollständige Kopie des Ausgangsdatenträgers erstellt, sei inzwischen weitgehend ausgetauscht. Soweit dies noch nicht möglich war, wurden an den Terminals Warnhinweise aufgenommen. Das Unternehmen versicherte, dass alle nicht benötigten Daten zwar kopiert, aber nicht genutzt würden. Sofort nach Erledigung des Auftrags würden sämtliche Daten gelöscht. Nach Rückgabe der CD-ROM an den Kunden blieben keine Dateien mehr vorrätig.

Was ist zu tun?
Datensparsamkeit setzt voraus, dass nur benötigte Daten erhoben werden; hierfür müssen die technischen Voraussetzungen geschaffen werden. Wer Kunden nicht über eine übermäßige Datenerhebung informiert, handelt rechtswidrig.

5.8.10 Der Rechtsanwalt und sein Freund

Man sollte denken, es sei selbstverständlich, dass Anwaltskanzleien den Datenschutz und die Anforderungen der Datensicherheit routinemäßig beachten. Dies ist leider allzu oft nicht der Fall.

Immer wieder erhält das ULD Eingaben zur Datenverarbeitung von Rechtsanwälten. Nicht selten wird offensichtlich versucht, über eine Kritik der Datenverarbeitung beim Anwalt des Prozessgegners die eigene Situation in einem Prozess zu verbessern. Insofern respektiert das ULD selbstverständlich die besondere Rolle des Anwaltes und dessen Vertrauensverhältnis zum Mandanten, das durch das **Mandatsgeheimnis** geschützt wird. Dies kann und darf auch nicht über den Umweg einer Datenschutzkontrolle ausgehebelt werden.

Es kommt aber immer wieder vor, dass von Rechtsanwälten die **Kontrollkompetenz** des ULD generell mit dem Verweis auf das Mandatsgeheimnis bezweifelt wird. Würde das ULD dies akzeptieren, so würde der Anwaltsberuf generell weitgehend kontrollfrei gestellt. Bei einem direkten Bezug zum Mandatsgeheimnis verweist das ULD schon an die Rechtsanwaltskammer, die kontrollieren darf, ob sich ein Anwalt nicht standesrechtskonform verhalten hat. Außerhalb des klassischen Mandatsverhältnisses, insbesondere hinsichtlich technisch-organisatorischer Maßnahmen, kann sich ein Anwalt gegenüber der Aufsicht aber nicht seiner Verantwortung entziehen.

Ein Beispiel: Weil eine Anwaltskanzlei kein eigenes Faxgerät vorhalten wollte, nutzten die dortigen Anwälte die freundschaftlichen Verbindungen zu einem Firmeninhaber und Besitzer eines **Faxgerätes**. Über Jahre wurden anwaltliche Faxe auf dem Faxgerät der Firma empfangen und versendet. Wurde dies Mandanten bewusst, so konnte dies schon auch zur Auflösung des Mandatsverhältnisses kommen. Als wir eingeschaltet wurden, haben wir noch am selben Tag der Kanzlei die weitere Nutzung des Faxgerätes untersagt. Nun überlegt man, ob künftig auf technischen Fortschritt verzichtet oder ein eigener Faxanschluss installiert werden soll.

Was ist zu tun?
Anwälte sind in besonderem Maße verpflichtet, das BDSG zu beachten. Sie können sich nicht einfach mit der pauschalen Behauptung, ihr Mandatsgeheimnis werde verletzt, einer Datenschutzkontrolle entziehen.

5.8.11 Ein Rechtsanwalt, der zu viel wusste

E-Mails fallen unter das Fernmeldegeheimnis – auch in einer Anwaltskanzlei.

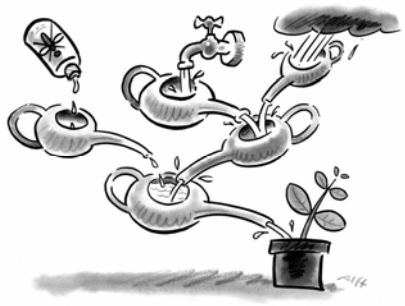
Die Eingabe des Ehemannes einer angestellten Rechtsanwältin verblüffte selbst uns. In ihrer Kanzlei war die private Nutzung von Kommunikationsmitteln, also auch des E-MailDienstes, erlaubt. Nach einer gesundheitlich bedingten längeren Abwesenheit stellte die Rechtsanwältin bei der Rückkehr an ihren Arbeitsplatz fest, dass während der Abwesenheit eine Umleitung der auf ihrem Konto eingehenden Nachrichten auf das Konto der Bürovorsteherin eingerichtet war; die an die Anwältin adressierten Nachrichten wurden also an die Bürovorsteherin übermittelt. Diese druckte die Nachrichten teilweise aus und legte sie dem Kanzleiinhaber vor. Der Bitte der Rechtsanwältin, die Umleitung zu löschen, wurde nur zum Schein entsprochen. E-Mails des Ehemannes an die Rechtsanwältin landeten weiterhin auf dem Rechner der Bürovorsteherin. Nach Beendigung des Beschäftigungsverhältnisses wandte sich der Ehemann an die Rechtsanwaltskammer. Er sah seine Privatsphäre durch diese Verhaltensweise verletzt. Die Rechtsanwaltskammer sah jedoch in dem Verhalten des Inhabers der Kanzlei keinen Verstoß gegen standesrechtliche Regeln. Daher wandte sich der Petent an das ULD. Aufgrund des unzulässigen Zugriffs auf personenbezogene Daten wurde gegen den Rechtsanwalt eine Verwarnung mit einem Verwarngeld ausgesprochen.

Was ist zu tun?
Private E-Mail-Kommunikation unterfällt dem Fernmeldegeheimnis. Das muss auch respektiert werden, wenn die Umleitung von Nachrichten vom Empfängerkonto auf ein anderes Konto technisch einfach zu realisieren ist.

6 Systemdatenschutz

6.1 Wer testet, sündigt nicht

Das ULD erreichen immer wieder Anfragen, wie man datenschutzgerecht aus einer Projektphase in den Produktivbetrieb eines Verfahrens übergehen kann. Dieser Übergang ist entscheidend, da die Arbeiten zur Inbetriebnahme des Verfahrens abgeschlossen sein müssen und das Verfahren getestet und freigegeben werden muss.



Programme und Sicherheitsmaßnahmen sind vor der Aufnahme der Verarbeitung personenbezogener Daten zu testen. Die konkrete Durchführung der Tests ist aus gutem Grund nicht vorgegeben. Die Verfahrensweisen zu Test und Freigabe müssen nämlich auf das jeweilige Verfahren und die aktuelle **Einsatzsituation angepasst** werden. Häufig wird die Einführung eines Verfahrens zur Verarbeitung personenbezogener Daten in einzelne Phasen gegliedert und im Rahmen eines Projekts durchgeführt; Ähnliches gilt für wesentliche Verfahrensänderungen (28. TB, Tz. 6.2 und Tz. 6.3). Beim Übergang in die sogenannte Pilotphase müssen alle wesentlichen Tests und Freigaben erfolgt sein. Typischerweise wird in einer Pilotphase in einem beschränkten Umfeld die volle Funktionalität mit Echtdaten für einen begrenzten Zeitraum ausprobiert. Sie ist bereits eine Phase des Produktivbetriebs. Alle Testmaßnahmen und Ergebnisse müssen protokolliert werden. Die Freigabe des Verfahrens für eine Pilotphase hat schriftlich zu erfolgen.

Unabhängig von der jeweiligen Phase, in der sich ein Projekt befindet, ist eine **Dokumentation** erforderlich, der Folgendes zu entnehmen ist:

- die definierten Ziele,
- die technischen Mittel und Instrumente,
- die Festlegung der einzelnen Projektphasen mit Beginn und Ende,
- die Benennung der verantwortlichen Personen und
- die Entscheidung der verantwortlichen Person über den Beginn einer Projektphase, die Dokumentation des Projektverlaufs sowie die Ergebnisse und Schlussfolgerungen.

Der Detaillierungsgrad dieser Dokumentation kann sich nach der Entwicklungsphase richten, in der sich ein Verfahren zur Verarbeitung personenbezogener Daten befindet.

Bei unseren Beratungen empfehlen wir stets, eine grobe Einteilung in einen „Projektbetrieb“ und in einen „Produktivbetrieb“ durchzuführen. Die Regelungen des Landesdatenschutzgesetzes (LDSG) und der Datenschutzverordnung (DSVO)

für die Verarbeitung personenbezogener Daten gelten unabhängig davon, ob diese bereits im Produktivbetrieb oder noch im Projektbetrieb erfolgt. Wird die Inbetriebnahme eines Verfahrens in einzelne Phasen aufgeteilt, kann man die **Dokumentation** und notwendigen Regelungen genau wie das Verfahren selbst **schrittweise entwickeln** und fortschreiben. In unseren Beratungsprojekten hat sich eine weitere Unterteilung des Projektbetriebs und des Produktivbetriebs als zweckmäßig erwiesen, die im Folgenden dargestellt wird: nämlich zum einen die Funktionstests sowie Integrations- und Abnahmetests als Teil des Projektbetriebs, zum anderen die Phasen des Piloten und des Regelbetriebs, die beide dem Produktivbereich zuzurechnen sind.

Insbesondere bei **komplexeren Verfahren** sollten aufeinander aufbauende Tests und Freigaben durchgeführt werden. Denn immer gilt: Personenbezogene Daten sind vor der Freigabe eines Systems nicht weniger schutzbedürftig als nach dessen Freigabe. IT-Verantwortliche müssen sich im Klaren darüber sein, dass jede Verarbeitung personenbezogener Daten den gesetzlichen Regelungen unterliegt, unabhängig davon, welchen Namen man ihr gibt.

- **Funktionstests**

Der Zweck des Funktionstests ist es, die Verwendbarkeit von Programmen und Geräten für die nachfolgenden Projektphasen sicherzustellen. Ein Funktionstest zeichnet sich durch die folgenden Merkmale aus:

- **Keine Anwender, nur Tester:**

  Es gibt außer einer kleinen Gruppe von Testern mit genau umrissenen Aufgaben keine regulären Anwender des Verfahrens.

- **Keine Verbindungen zu und kein Datenaustausch mit anderen Verfahren im Produktivbetrieb:**

  Tests finden in einer isolierten Testumgebung statt.

- **Keine Verwendung personenbezogener Daten:**

  In einem Test dürfen keine realen personenbezogenen Daten verarbeitet und auch nicht aus anderen Produktivsystemen übernommen werden. Gegebenenfalls sind Echtdaten vor ihrer Übernahme in das Testverfahren zu anonymisieren bzw. zu pseudonymisieren.

Werden gemäß diesem Muster in Funktionstests keine personenbezogenen Daten verarbeitet, so sind im Testbetrieb auch keine Datenschutzanforderungen zu erfüllen. Verbindungen mit anderen Produktivsystemen der automatisierten Verarbeitung personenbezogener Daten sind ausgeschlossen. Durch die Funktionstests kann es so auch nicht zu gravierenden Auswirkungen auf andere Verfahren und deren Datenschutz- und Datensicherheitsniveau kommen.

- **Integrations- und Abnahmetests**

Der Zweck der Integrations- und Abnahmetests besteht darin, das Konzept und die Implementierung vor dem Auftreten von z. B. im Funktionstest nicht erkannten Designschwächen oder Implementierungsfehlern in einer quasiproduktiven Umgebung mit realistischen Lastszenarien abzusichern. Mithilfe von Integrations- und Abnahmetests sollen vor dem Pilotbetrieb oder der Freigabe des Regelbetriebs eventuell vorhandene oder vermutete Risiken ausgeschlossen werden, die unter den Bedingungen des Funktionstests nicht abgeschätzt werden konnten. Derartige Tests sind zeitlich limitiert auf detailliert beschriebene Szenarien zu beschränken. Sie sollten **wenn möglich nicht personenbezogen** durchgeführt werden. Personenbezogene Daten dürfen jedoch im Rahmen zusätzlicher, eng zugeschnittener Tests verwendet werden. Grundlegende Funktionen müssen bereits im Funktionstest mit ausreichend anonymisierten Daten überprüft worden sein. Auf die ersten Funktionstests darf nicht wegen der ohnehin geplanten Integrations- und Abnahmetests verzichtet werden.

Zu Testzwecken darf eine **Kopie der Originaldatensätze** verwendet werden, wenn eine Rechtsvorschrift dies ausdrücklich erlaubt. Fehler können auch im begründeten Ausnahmefall mit Originaldaten aufgeklärt werden, wenn

- eine bereichsspezifische Rechtsvorschrift dies nicht ausdrücklich untersagt,
- eine Anonymisierung der Originaldaten für die vorgesehene Testkonstellation nur mit einem unvertretbar hohem Aufwand verbunden wäre,
- die verantwortliche Stelle dem Vorgehen schriftlich zugestimmt hat,
- bei der Durchführung oder Auswertung des Tests die schutzwürdigen Belange der Betroffenen und die Datensicherheit angemessen berücksichtigt werden,
- nur die für die Fehlerbehebung und Durchführung des Tests erforderlichen Personen die Daten nutzen können und
- Zugang zu diesen Daten nur Personen erhalten, die den jeweils maßgebenden Vertraulichkeitsgrundsätzen und insbesondere datenschutzrechtlichen Vorschriften unterliegen.

Das Kopieren und das Verwenden der Originaldaten muss dokumentiert werden. Nach Beenden des Tests muss die Kopie der Originaldaten gelöscht oder anonymisiert werden. Der oder die behördliche Datenschutzbeauftragte muss vorab informiert werden.

Die Integrations- und Abnahmetests müssen in einer **definierten und kontrollierten Umgebung** stattfinden, um nachvollziehbar und aussagekräftig zu sein. Soll eine Netzanbindung ausprobiert werden, sind die Risiken durch zusätzliche Sicherheitsmaßnahmen zu beschränken, z. B. durch eine geeignete Auswahl der Datensätze.

Werden personenbezogene Daten im Integrations- und Abnahmetest verwendet, bedarf es zumindest einer Kurzfassung eines IT-Konzeptes sowie eines auf die Testbedingungen angepassten **Sicherheitskonzeptes**. Gegenstand der Integrations- und Abnahmetests ist insbesondere auch die Prüfung und die eventuell notwendige Korrektur der erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen. Diese Tests dienen als Grundlage für die Erstellung der abschließend gültigen Sicherheitsdokumentation und der Risikoanalyse für den späteren Regelbetrieb. Die Durchführung von Integrations- und Abnahmetests ist Voraussetzung, um das System unter Sicherheitsgesichtspunkten für den Regelbetrieb freigeben zu können.

- **Pilotbetrieb**

Der Zweck des Pilotbetriebs besteht darin, einen Echtbetrieb in einem **zeitlich und sachlich begrenzten Bereich** durchzuführen. Es soll überprüft werden, ob das Verfahren den technischen und organisatorischen Anforderungen in der Praxis genügt. Beim Pilotbetrieb wird der führende Datenbestand bearbeitet. Es darf kein Parallelbetrieb stattfinden, bei dem ein eventuell noch vorhandenes altes Verfahren das führende System bleibt. In einem Piloten dürfen im zeitlich definierten Rahmen personenbezogene Daten verarbeitet werden.

Voraussetzung für einen Pilotbetrieb ist ein IT-Konzept, aus dem sich der Zweck des Verfahrens sowie das Ziel des Pilotbetriebs ergeben. Soweit im Piloten personenbezogene Daten verarbeitet werden, bedarf es eines **vollständigen Sicherheitskonzeptes** und einer hierauf aufbauenden Risikoanalyse. Wird der Pilotbetrieb nur in eingeschränktem Umfang aufgenommen, kann sich auch das Sicherheitskonzept hierauf beschränken. Entspricht der Pilot bereits dem Regelbetrieb der Verarbeitung personenbezogener Daten, so hat sich das Sicherheitskonzept vollständig an diesen Anforderungen zu orientieren.

Ein Pilotbetrieb bedarf der **Freigabe durch die Dienststellenleitung**, wenn personenbezogene Daten verarbeitet werden. Für den Pilotbetrieb kann die Freigabe von der Dienststellenleitung auch an eine befugte Person delegiert werden.

- **Regelbetrieb**

Der Zweck des Regelbetriebs besteht darin, ein automatisiertes Verfahren gemäß den definierten Anforderungen und vereinbarten Zielen zu betreiben. Die geltenden **Regeln zur ordnungsgemäßen Verarbeitung** personenbezogener Daten sind zu beachten. Der Regelbetrieb erfolgt mit der schriftlichen Freigabe durch die Dienststellenleitung. Vor dem Beginn des Regelbetriebs sind die eingesetzten Programme und Sicherheitsmaßnahmen zu testen. Solche Tests dürfen z. B. mit Daten von Personen durchgeführt werden, die für das Verfahren verantwortlich oder Mitarbeiter des Projekts sind und diesen Tests zugestimmt haben. Gut dokumentierte Funktionstests sowie Integrations- und Abnahmetests aus den vorherigen Projektphasen können den Aufwand für diesen letzten Schritt eines notwendigen Test- und Freigabeverfahrens erheblich reduzieren.

Was ist zu tun?
Test und Freigabe erfordern vorab eine gute Planung, eine Gliederung in einzelne Phasen und eine Kontrolle der korrekten Umsetzung beim Übergang von einer Phase in die andere. Dies garantiert den Projekterfolg: Datenschutz ist dann gleich „mit eingebaut“.

6.2 Die neue Datenschutzverordnung

Seit Januar 2009 ist die neue Datenschutzverordnung in Kraft. Was ist geblieben, was wurde verändert?

Wie schon die alte, hat die neue Datenschutzverordnung vor allem ein Ziel: die **Transparenz der automatisierten Verarbeitung** personenbezogener Daten zu verbessern. Transparenz ist die wichtigste Voraussetzung, um technische und organisatorische Systeme beobachtbar und prüfbar zu machen. Ohne eine Prüffähigkeit der Verfahren und Systeme gibt es kein funktionierendes Datenschutzmanagement: Transparenz ist auch für die Beherrschbarkeit komplexer Systeme essenziell.

Das Einhalten von Datenschutzanforderungen kontrollierbar zu machen ist eine Herausforderung. Für das Prüfen von Zweckbindung und Erforderlichkeit personenbezogener Datenverarbeitung reicht ein formaler Check von Maßnahmen der Datensicherheit nicht aus. Man muss die **Wirklichkeit vor Ort** verstehen, die mit automatisierten Verfahren abgebildet werden soll. Nur so lässt sich das Maß für eine zweckgemäße und datensparsame Verarbeitung finden. Auf dieser Grundlage können dann effektive und effiziente technische Maßnahmen und organisatorische Regelungen gefunden werden.

Die neue Landesverordnung über die Sicherheit und Ordnungsmäßigkeit automatisierter Verarbeitung personenbezogener Daten (Datenschutzverordnung – DSVO) verbessert die Transparenz und Überprüfbarkeit der Datenverarbeitung durch präzise Dokumentationsanforderungen. Es wurden vor allem diejenigen Regelungen der DSVO überarbeitet und vereinfacht, die in Schulungen und Beratungen für Nachfragen und Diskussionen gesorgt hatten. Die Überarbeitung brachte einen angenehmen Nebeneffekt: Die neue DSVO ist schlanker als die alte, rein formal schon durch deren Verkürzung um drei Paragrafen auf nunmehr sieben. Neben der Bestimmung des Anwendungsbereichs, der Begriffe und den Regeln zum Übergang und Inkrafttreten konzentriert sich der Kern der DSVO auf nur noch drei Paragrafen. Es handelt sich hierbei um die **Verfahrensdokumentation**, die **Dokumentation der Sicherheitsmaßnahmen** sowie um **Test und Freigabe**.

Es wurde darauf geachtet, dass die Dokumentationsregelungen mit **internationalen Sicherheitsstandards** wie BSI-Grundschutz oder der ISO-27000er-Reihe kompatibel sind. Anders formuliert: Wer sich an internationalen Sicherheitsstandards orientiert, erfüllt viele Anforderungen der DSVO quasi nebenbei.

Die Bestandteile der **Verfahrensdokumentation** werden in zehn Punkten aufgeführt. Diese sind als Grobgliederung für das zu erstellende Dokument nutzbar. Zunächst ist der Zweck darzulegen, dann müssen die eingesetzten Geräte und Programme sowie deren Vernetzung beschrieben werden. Die technischen und organisatorischen Vorgaben und deren Umsetzung in einem Berechtigungskonzept sind ebenso zu beschreiben wie die Art und Weise der Protokollierung von Zugriffen und Veränderungen am Verfahren. Finden Datenübermittlungen an andere Stellen oder eine Datenverarbeitung im Auftrag statt, so muss dies nachvollziehbar sein. Zum Abschluss sind die Maßnahmen darzustellen, wie Ansprüchen von Betroffenen auf Auskunft entsprochen wird und wie die Berichtigung, Löschung und Sperrung personenbezogener Daten erfolgt. Die Verfahrensdokumentation muss für sachkundige Personen in angemessener Zeit nachvollziehbar sein. Sie ist dauernd fortzuschreiben und unterliegt einer Aufbewahrungsfrist von mindestens fünf Jahren.

Nicht neu, aber klarer formuliert ist, dass die **Dokumentation mehrerer Verfahren** oder mehrerer Verfahrensteile zusammengefasst werden kann. Daten verarbeitende Stellen, die sich für eine gemeinsame Nutzung von IT-Verfahren entscheiden, können hiervon profitieren. Ein Großteil der Verfahrensdokumentation kann einmal zentral erarbeitet und dann bei jeder Stelle in die eigene Dokumentation übernommen werden.

Auf der Grundlage der Verfahrensdokumentation ist die **Dokumentation der Sicherheitsmaßnahmen** zu erstellen. Nach einer Analyse der vorliegenden Risiken müssen die getroffenen Sicherheitsmaßnahmen dokumentiert werden, die diese Risiken minimieren. Sofern für einzelne Risiken keine angemessenen Maßnahmen getroffen werden können oder sollen, sind diese als Restrisiken zu dokumentieren. Neu in der DSVO sind Bestimmungen zum Umgang mit Verschlüsselung sowie genauere Ausführungen zur Auswertung von Protokolldaten und zu Dokumentationspflichten bei einer Datenverarbeitung im Auftrag. Außerdem wurde der in Schleswig-Holstein bereits gängige Begriff des Datenschutzmanagementsystems aufgenommen, unter dem die Tätigkeiten eines Datenschutzbeauftragten zusammengefasst sind.

Bezüglich **Tests und Freigaben** ist eine Bestimmung hinzugekommen, dass beim Testen festgestellte Mängel entsprechend ihrer Bedeutung zu gewichten sind (Tz. 6.1). Eine Freigabe ist nur zulässig, wenn entsprechend der Gewichtung keine wesentlichen Mängel mehr bestehen; geringfügige Mängel müssen in angemessener Zeit beseitigt werden. Testergebnisse anderer Stellen können mit eigenen Ergebnissen kombiniert werden. Eine entsprechende Eigenorganisation vorausgesetzt, können mehrere Daten verarbeitende Stellen, die dasselbe Fachverfahren oder dieselbe technische Infrastruktur einsetzen, kooperativ und verteilt testen und so ihren Testaufwand reduzieren.

Die neue DSVO ist schlank und gut mit anderen Vorgehensweisen wie der Methodik nach BSI-Grundschutz kombinierbar. Sie **unterstützt kooperative Infrastrukturen** und Vorgehensweisen im Bereich der Informations- und Kommunikationstechnik durch die Möglichkeit, eine modulare Dokumentation aufzubauen.

Die neue DSVO ist im Gesetz- und Verordnungsblatt Schleswig-Holstein (GVOBl. Schl.-H. 2008, S. 841) und unter

https://www.datenschutzzentrum.de/material/recht/dsvo.htm

veröffentlicht.

Das ULD bietet kostenfreie Beratungen und Schulungen zur neuen DSVO an.

Was ist zu tun?
Neue Verfahren müssen den Regelungen der überarbeiteten DSVO entsprechen. Bei laufenden Verfahren sollte die bestehende Dokumentation trotz der Übergangsregelungen zeitnah überprüft werden. Datenschutzbeauftragte und IT-Verantwortliche sollten die Angebote des ULD und der DATENSCHUTZAKADEMIE zur Information und Weiterbildung wahrnehmen.

6.3 Die Europäische Dienstleistungsrichtlinie

Die Richtlinie über Dienstleistungen im Binnenmarkt 2006/123/EG von Ende 2006 soll sicherstellen, dass alle Verfahren und Formalitäten, die mit der Aufnahme oder Ausübung bestimmter Dienstleistungstätigkeiten verbunden sind, europaweit elektronisch über einen „Einheitlichen Ansprechpartner" abgewickelt werden können.

Über die EU-Dienstleistungsrichtlinie (EU-DLR) sollen sich die Verwaltungen europaweit über **regionale Anerkennungsverfahren** für Dienstleistungstätigkeiten austauschen und zudem problematische Antragsteller identifizieren können. In einem Binnenmarktinformationssystem („Internal Market Information System", IMI) sollen die relevanten Informationen bereitgestellt und ausgetauscht werden (30. TB, Tz. 11.3). Die Richtlinie muss bis Ende 2009 umgesetzt werden. Sie bedeutet für den Datenschutz eine ganze Reihe an Chancen und Risiken.

Der **Einheitliche Ansprechpartner** (abgekürzt: EAP) soll als Verfahrensvermittler zwischen einem Dienstleistungsanbieter aus dem europäischen Raum und den Behörden agieren, die die entsprechenden Prüfungen in ihrer Region vornehmen und Genehmigungen erteilen. Die Zuständigkeiten der Verwaltungen bleiben durch den EAP unangetastet.

Das Land Schleswig-Holstein hat deutschlandweit die Federführung zur Ausarbeitung einer Vorlage für die **rechtliche Umsetzung** der EU-Dienstleistungsrichtlinie in den Bundesländern übernommen. Die sogenannte „Blaupause", eine 172 Seiten umfassende Vorlage (Stand: September 2008), enthält einige datenschutzrechtliche Ausführungen sowie eine Vielzahl technischer Empfehlungen, die zum Teil auf noch nicht praxiserprobten Technologien aufsetzen.

Das in Schleswig-Holstein für die Umsetzung der EU-DRL zuständige Finanzministerium hat frühzeitig alle Beteiligten, die mit einem EAP kooperieren müssen,

an einen Tisch geholt und will den **EAP als Anstalt des öffentlichen Rechts**, die für ganz Schleswig-Holstein zuständig ist, institutionalisieren. Daneben wurde begonnen, ein Prozesskataster aufzubauen, das all die Gesamtprozesse beschreibt, in denen einzelne Verwaltungen an einem Genehmigungsverfahren beteiligt sind. Bislang waren es die Antragsteller, die beim Durchlaufen der einzelnen Verwaltungsstationen das gesamte Beantragungsverfahren kennenlernen und durchlaufen mussten. Die Anstalt wird gemeinsam vom Land, den Kommunen und den Kammern getragen.

Aus Datenschutzsicht sind bei der vorgesehenen Ausgestaltung zunächst zwei Fragen relevant: Welche **Zuständigkeiten** sollen bei dem viele Verwaltungstätigkeiten zentralisierenden EAP per Gesetz zusammengezogen werden? In welchem Ausmaß muss oder darf der EAP Kenntnis nehmen von den Inhalten der Anträge, obwohl er laut Richtlinie keine Zuständigkeit für deren inhaltliche Bearbeitung und die Erteilung oder Verweigerung von Genehmigungen hat?

Fällt ein relevanter Anteil inhaltlich-orientierter Verwaltungstätigkeit auf den EAP, dann muss eine Behörde aufgebaut werden, die **hohen Anforderungen** genügt in Bezug auf Personal, Verbindlichkeit und Validität der Auskünfte und Tätigkeiten, Fallmanagement und Wissensbasis, Aktenführung und nicht zuletzt Beachtung der (datenschutz-)rechtlichen Vorgaben. Die einzurichtende Informationstechnik muss Sicherheit gewährleisten und zugleich die zentralen bzw. dezentralen Zuständigkeiten berücksichtigen. Schließlich müssen die beteiligten Verwaltungen kooperieren.

Das ULD hat angesichts der schwierigen Anforderungen ein **Alternativmodell für den EAP** entwickelt, bei dem Controlling und Operating der Prozesse funktional getrennt werden. Es geht darum, die Kontrolle des Gesamtprozesses zu optimieren und zugleich die fallbezogene Datenverarbeitung und die Kommunikation zwischen dem Dienstleister und der Verwaltung diesen zu überlassen. Die Verantwortung des EAP erstreckt sich dann nicht auf eine eigene umfassende Hochleistungsinformationstechnik mit „Datensafes“ zur Dokumentenablage, sondern nur auf sichere Abwicklungsverfahren für die Direktkommunikation zwischen Antragstellern und Genehmigungsbehörden. Der integre und vertrauliche Transport von Daten ließe sich über OSCI 2.0 (Online Services Computer Interface, Tz. 6.4) und die notwendige Authentisierung von Personen und Maschinen über den E-Government-Standard SAFE (Secure Access to Federated E-Justice/E-Government, Tz. 6.4) realisieren.

Die Einrichtung eines EAP forciert die **Digitalisierung und Automatisierung vieler Verwaltungstätigkeiten**. Damit diese Technisierung gelingt, müssen die Verwaltungsverfahren als Prozesse zuvor standardisiert und formal beschrieben sein. Notwendige Bedingung ist also eine Transparenz der Verfahren der Organisation sowie der Datenverarbeitung. Etwaige rechtliche Regulierungs-, Zuständigkeits- bzw. Verantwortlichkeitslücken werden damit offenkundig.

Zur Beschreibung der Datenstrukturen im XML-Format kommen sogenannte XÖV-Standards zum Einsatz. Der Transport derartig strukturierter Daten geschieht

über den **internationalen Standard** der sogenannten WebServices. Das bedeutet, dass die organisatorischen Prozesse, die Schnittstellen, Kommunikationskanäle, Formate, Daten und Datenflüsse auch zwischen den Verwaltungen offengelegt und abgestimmt werden müssen. Bei der Realisierung sind die Gebote zur Datensparsamkeit und zur Zweckbindung zu beachten. Die WebServices ermöglichen zudem, dass Daten dezentral, sozusagen an den Quellen, erhoben, gehalten und gepflegt werden können, was sich positiv auf die Datenqualität auswirkt. Die Daten können dort, wo sie gebraucht werden, zusammengeführt werden.

Aus Datenschutzsicht bedeutet die Technisierung der Verwaltung, dass auch die Methoden zur Kontrolle der Datenverarbeitung stärker technisiert werden müssen**,** im Sinne einer automatisierten Qualitätssicherung im Allgemeinen und eines internen und externen Datenschutzmanagements im Besonderen. Noch sind viele Punkte offen, die sich zu **Risiken für den Datenschutz** entwickeln können:

- Zum jetzigen Zeitpunkt zeigt die Blaupause an vielen Stellen Regelungslücken auf. Als ungeklärter Punkt ist das **europaweite Handling von Zertifikaten** herauszuheben, was für die Sicherstellung der Integrität und Authentizität von Dokumenten von zentraler Bedeutung ist. Es heißt bisher nur lapidar: „Elektronische Dokumente von Behörden aus anderen Mitgliedstaaten sind in der Regel als gültig anzuerkennen." Hier ist durch konkretere Vorgaben nachzubessern.
- Bei der Nutzung von WebServices ist nicht in jedem Fall klar festgelegt, welche Instanz unter welchen Bedingungen die Daten tatsächlich verarbeitet. Hier gilt es, rechtliche Anforderungen in technisch ausführbare **WebService Privacy Policies** umzuformulieren und dann zu implementieren, um den Transport und die Verarbeitung personenbezogener Daten über WebServices unter festgelegte Bedingungen zu stellen und dadurch Verbindlichkeit und Nachweisbarkeit von derartigen Transaktionen sicherzustellen.
- Nicht zuletzt besteht das Risiko, dass eine effiziente Technisierung der Datenverarbeitung **neue Begehrlichkeiten zur Überwachung** von Mitarbeitern (Leistungs- und Verhaltenskontrollen), Bürgern und Kunden wecken kann. Dem kann durch eine datenschutzrechtliche Projektbegleitung entgegengewirkt werden.

Was ist zu tun?
Nach der frühzeitigen Festlegung des Finanzministeriums auf ein Organisations- und Technikmodell müssen jetzt die konkreten Rahmenbedingungen für den Einheitlichen Ansprechpartner geschaffen werden. Die automatisierte Datenverarbeitung beim EAP muss den Anforderungen des LDSG und der DSVO genügen.

6.4 OSCI-Transport 2.0 und SAFE: es gibt einiges zu tun

Beim Aufbau einer E-Government-Infrastruktur müssen viele einzelne Bausteine miteinander gekoppelt werden. Um das Rad nicht jedes Mal neu zu erfinden, sind viele Teilbereiche inzwischen standardisiert. Datenschutz muss hierbei noch mehr berücksichtigt werden. Das ULD beteiligt sich gemeinsam mit den Kollegen anderer Bundesländer an den Standardisierungsbemühungen im E-Government, insbesondere bei OSCI (Online Services Computer Interface) und SAFE (Secure Access to Federated E-Justice/E-Government).

OSCI-Transport ist eine technische Infrastruktur zur Datenübermittlung und gilt als Schlüsseltechnik für die medienbruchfreie Abwicklung von Geschäftsprozessen über das Internet. OSCI-Transport erfüllt sicherheitstechnische Anforderungen an Vertraulichkeit, Unveränderbarkeit, Sicherstellung des richtigen Absenders und richtigen Empfängers sowie Nichtabstreitbarkeit dessen, dass Daten verschickt bzw. empfangen wurden. OSCI-Transport trennt die für die Weiterleitung benötigten Informationen wie Absender und Empfänger strikt von den Inhaltsdaten. Seit Juni 2002 ist es in der Version 1.2 in vielen E-Government-Projekten auf Kommunal-, Landes- und Bundesebene im Einsatz. OSCI-Transport wird insbesondere dann verwendet, wenn Daten über eigene Organisations- oder Ländergrenzen hinweg verschickt werden. Es spielt beispielsweise bei der Vernetzung der bundesweit über 5.400 Meldebehörden, die seit 2007 ihre Daten untereinander ausschließlich elektronisch austauschen müssen, eine tragende Rolle.

Viele der von OSCI-Transport erfüllten **Sicherheitsanforderungen** werden seit einigen Jahren international unter dem Stichwort „sichere WebServices“ umgesetzt. Dies führte dazu, dass der „Kooperationsausschuss Automatisierte Datenverarbeitung“ (KoopA ADV), der von Bund, Ländern und kommunalen Spitzenverbänden getragen wird und gemeinsame Grundsätze des Einsatzes der Informations- und Kommunikationstechniken (IT) und wichtige IT-Vorhaben in der öffentlichen Verwaltung erarbeitet und abstimmt, die OSCI-Leitstelle zur Entwicklung von OSCI-Transport Version 2.0 beauftragt hat. Ziel ist es, WebService-Mechanismen entsprechend den deutschen Rechtsgrundlagen zu gestalten und gegebenenfalls mit Eigenentwicklungen zu ergänzen. Der Abschluss der Spezifikation von OSCI 2.0 war für Juli 2008 zugesagt, ist aber bislang nicht erfolgt (Stand: Ende Oktober 2008). Ein Grund für die Verspätung sind zusätzliche Anforderungen an eine sichere Infrastruktur im Rahmen der Umsetzung der EU-Dienstleistungsrichtlinie (Tz. 6.3) und der Bürgerportale.

Aus Datenschutzsicht sind zwei Eigenschaften von OSCI-Transport 2.0 herauszuheben: Die Nutzung dieser WebServices setzt **keinen zentralen Intermediärserver** wie noch OSCI 1.2 voraus, auf dem zentrale Sicherheitsfeatures abgebildet werden müssen. Sicherheitsrelevante Dienste, z. B. Signatur- und Authentisierungsprüfungen sowie Protokollierung, können von unterschiedlichen Komponenten eines Informationsverbunds erbracht werden. OSCI 2.0 erlaubt in diesem Sinne eine dezentrale Datenverarbeitung bei gleichzeitig effizienter Abrufmöglichkeit auf Basis einer nach dem Stand der Technik sicher betreibbaren Infrastruktur.

In WebServices wird die Datenverarbeitung über sogenannte **Policies** gesteuert. Hierfür müssen rechtliche Anforderungen zunächst in technische Maßnahmen überführt werden, die dann in das maschinenlesbare Format der WebService Policies übertragen werden. Über Policies lässt sich regeln, welche Sicherheitsstandards für eine Datenverarbeitung gefordert sind, also z. B. ob die Datenübermittlung verschlüsselt erfolgen muss, ob Nachrichtenbestandteile zu signieren sind, in welcher Qualität dies zu geschehen hat und wie das Protokoll darüber zu führen ist. Diese **technische Umsetzung rechtlicher Anforderungen** steigert die Transparenz der Datenverarbeitung und macht für die Betreiber die Einhaltung der Sicherheitsregeln für Geschäftsvorfälle im E-Government leichter. Sie erlaubt außerdem den von der Datenverarbeitung Betroffenen, den Auftraggebern und den internen und externen Kontrolleuren, die Art der Datenverarbeitung zu kontrollieren. Die Beachtung von Zweckbindung, Datenvalidität und Erforderlichkeit wird erleichtert.

Durch Herausnahme der Datenverarbeitung aus einem eigenen Rechenzentrum und das Verteilen auf viele **Betreiber mit unterschiedlichen Sicherheitsniveaus** steigt zugleich das Risiko, dass gegen Regeln verstoßen wird, dass unberechtigt auf Daten zugegriffen wird und die Daten verfälscht oder zweckentfremdet verarbeitet werden. Um diese Risiken zu begrenzen, muss mit der Einführung dieser Techniken die Kontrollierbarkeit der Systeme, der Policies und der Prozesse bewahrt werden. Techniken müssen entwickelt werden, die die Überwachung und Steuerung der Systeme ermöglichen.

Diese Anforderungen und Eigenschaften gelten sowohl für OSCI 2.0 als auch für SAFE (**Secure Access to Federated E-Justice/E-Government**). SAFE definiert im Kontext von WebServices und unter Berücksichtigung von OSCI 2.0 ein technisches Rahmenwerk für die sichere Nutzung digitaler Identitäten über administrative Domänengrenzen (Trust-Domains) hinweg. Mit SAFE kann sich ein Notar über das Internet sicher an einer Stelle als ein solcher authentisieren, um dann im gesamten (unter Umständen europaweiten) Verbund entsprechend seiner zugebilligten oder entzogenen Zugriffsrechte zu agieren.

Die WebService Policies der Sicherheitskonfigurationen von OSCI 2.0 und SAFE bilden nur einen standardisierten Rahmen. Dieser Rahmen muss mit konkret operativ umsetzbaren Anweisungen ausgefüllt werden. Hieran mangelt es in den ambitionierten Projekten. Bisher wurden **datenschutzspezifische Aspekte** nicht ausreichend betrachtet. Es gibt konkrete Zusagen der Projektgruppen, dass in Nachfolgeprojekten diese Lücke geschlossen wird. Zusammen mit den Datenschutzkollegen der anderen Länder versuchen wir, bereits in der Standardisierungsphase die für einen funktionierenden Datenschutz wichtigen Aspekte zu verankern.

Was ist zu tun?
Rechtliche Regelungen mit technischem Bezug sollten so formuliert werden, dass sie technisch umsetzbar sind. Die Verbindlichkeit von Policies muss in der Form gesichert werden, dass eine Organisation einer anderen nachweisen kann, dass sie sich nicht an die Spezifikation der Datenverarbeitung gehalten hat. Das Finanzministerium muss, gerade im Rahmen des Betriebs des Einheitlichen Ansprechpartners, auf Ebene der Policies eine Kontrolle und Steuerung ermöglichen.

6.5 Kontodatenskandal – Datenverarbeitung im ULD

Als das ULD im Sommer mehrere Datenträger mit insgesamt fast acht Millionen Kundendatensätzen erhielt, musste intern eine Vorgehensweise mit diesen hochsensiblen Daten festgelegt werden. Das ULD ist eine Daten verarbeitende Stelle mit einer hohen Verantwortung für die Daten der vom Skandal Betroffenen.

Die Daten auf den CDs lagen vollkommen ungeordnet, aufgeteilt in unzählige Teildateien in unterschiedlichen Formaten vor. Damit **Anfragen von Bürgern und Ermittlungsbehörden** beantwortet werden konnten, mussten die Daten in einer geeigneten Form aufgearbeitet werden. In welcher Form das geschehen sollte, wurde gemeinsam von der Dienststellenleitung, der behördlichen Datenschutzbeauftragten sowie technischen und juristischen Mitarbeitern des ULD erarbeitet. Es musste geprüft und festgelegt werden,

- auf welcher rechtlichen Grundlage die Daten verarbeitet werden,
- wer Zugriff auf die Daten erhält,
- in welcher Form und wo die Verarbeitung erfolgt und
- in welchem Umfang die Daten protokolliert und in welchen Abständen die Protokolle überprüft werden.

Unter Berücksichtigung dieser Überlegungen konnten folgende **Entscheidungen umgesetzt** werden:

- Für diese Daten wurde exklusiv ein Server bereitgestellt, auf dem das Datenbanksystem und die Abfrageschnittstelle, mit der auf die Kontodaten zugegriffen werden kann, laufen.
- Die Daten sind auf dem Server durch eine vollständige Festplattenverschlüsselung gesichert; das entsprechende Passwort wird in einem Safe gelagert.
- Der Server wird in einem vom Dienststellennetz komplett getrennten Netz betrieben ohne Schnittstellen zu externen Netzen.
- Um zu vermeiden, dass ein unbefugter Zugriff auf Datensicherungsmedien (z. B. Back-up-Sicherungsbänder) eintritt, wird der Server nicht gesichert. Bei einem Ausfall wird der Server neu installiert. Sämtliche Schritte, die aus den verteilten

und uneinheitlich vorliegenden Datenbeständen einen zentralen Datenbestand erschließen, sind in maschinell durchführbaren Anweisungen festgehalten und können bei Bedarf auf Basis der Ausgangsdaten wiederholt werden.

- Die Anzahl der Beschäftigten mit lesendem Zugriff ist streng begrenzt. Jede Abfrage erfolgt mit einer persönlichen Kennung. Sämtliche administrativen Kennworte sind in einem Safe hinterlegt und werden in regelmäßigen Abständen geändert.
- Sowohl Änderungen an den Datenbeständen und der Konfiguration des Servers als auch alle An- und Abmeldevorgänge und Datenabrufe werden automatisiert protokolliert. Die Protokolle werden durch die Datenschutzbeauftragte regelmäßig kontrolliert und ausgewertet.
- Die Datenträger mit den originalen Datensätzen werden in einem Safe aufbewahrt.

Alle festgelegten Prozesse, die Konfiguration des Servers und der Anwendungssoftware, die Berechtigungskonzeption sowie die Protokollierungsmaßnahmen und die Datenschutzkontrollen werden in der **Verfahrensakte** schriftlich dokumentiert. Nach Abschluss des Ermittlungsverfahrens werden die elektronischen Kontendaten gelöscht, die Datenträger mit den originalen Datensätzen zerstört und die Akte für fünf Jahre gespeichert.

6.6 Einsatz privater Geräte

In Behörden besteht zunehmend der Wunsch, personenbezogene Daten auf privat genutzten Geräten zu bearbeiten. Die Daten verarbeitende Stelle hat die technischen und organisatorischen Maßnahmen zur sicheren Verarbeitung zu ergreifen. Geht das überhaupt beim Einsatz von privaten Geräten?

Die Ausgestaltung der PC-Arbeitsplätze, mit denen auf Daten innerhalb einer Behörde zugegriffen wird, wird in Bezug auf die Hard- und Software, die Konfiguration und Nutzung verbindlich in den IT- und Sicherheitsfestlegungen der Daten verarbeitenden Stelle geregelt. Diese Konzeption setzt im Grunde voraus, dass die IT-Ausstattung vom Arbeitgeber zur Verfügung gestellt wird. Datenschutz- und Sicherheitskontrollen nach der organisatorischen Vorgabe der Daten verarbeitenden Stelle können innerhalb der Diensträume jederzeit gewährleistet werden. Der Einsatz privater Computer zur Verarbeitung dienstlicher Daten ist im LDSG und der DSVO nicht vorgesehen. Eine ordnungsgemäße Ausgestaltung der Hardware, Art und Umfang der zulässigen Nutzung und eine effektive Kontrolle der technischen und organisatorischen Sicherheitsmaßnahmen gemäß der IT- und Sicherheitskonzeption der Daten verarbeitenden Stelle können nicht wirkungsvoll gewährleistet werden. Im Einzelnen:

- Auf einem privaten Computer kann technisch nicht verhindert werden, dass sich nur befugte Personen am System anmelden können. Eine **private Nutzung z. B. von Familienmitgliedern** kann nicht ausgeschlossen werden. Es lässt sich auch nicht verhindern, dass unbefugte Personen die Benutzerkennung des Mitarbeiters verwenden. Daher können die Daten verarbeitende Person, der Zeitpunkt

und der Umfang der Verarbeitung nicht eindeutig protokolliert und kontrolliert werden. Es lassen sich hauptsächlich organisatorische Regelungen treffen, was in puncto Sicherheit als schwach zu bewerten ist.

- Auf einem privaten Computer werden **in der Regel andere Sicherheitsmaßnahmen** getroffen als innerhalb der Daten verarbeitenden Stelle. Es lässt sich technisch nicht sicherstellen, dass regelmäßig Service Packs, Sicherheitspatches und Antivirussoftware auf den privaten Computern eingespielt werden. Wieder sind nur – als schwach zu bewertende – organisatorische Regelungen möglich. Die Daten verarbeitende Stelle muss sich bewusst sein, dass bei dem privaten Computer meistens ein deutlich schwächeres Sicherheitsniveau besteht als innerhalb des Behördennetzes.
- Auch bei der Nutzung privater Computer muss sichergestellt werden, dass Administratoren der Daten verarbeitenden Stelle die notwendigen Sicherheitsmaßnahmen für das automatisierte Verfahren installieren, konfigurieren und warten können. Das gilt besonders für eine Verschlüsselung, wie sie bei der Verarbeitung außerhalb der Daten verarbeitenden Stelle gesetzlich gefordert ist. Daher müssen die Administratoren einen administrativen Fernzugang und unter Umständen einen **physikalischen Zugang** zum Gerät haben. Die Änderungen, die die Administratoren auf dem System durchführen, sowie die ordnungsgemäße Anwendung der automatisierten Verfahren müssen protokolliert und durch eine Kontrollinstanz (z. B. behördlicher Datenschutzbeauftragter oder Prüfungsamt) kontrolliert werden. Das ist bei privaten Geräten in privaten Umgebungen, wenn überhaupt, nur sehr schwer machbar.

Eine **Ausnahme** beim Einsatz privater Geräte für die Verarbeitung personenbezogener dienstlicher Daten ist mit **Terminalserverdiensten** möglich. Dabei wird zusätzlich zur Authentifizierung am privaten Computer eine weitere Authentifizierungs- und Autorisierungsebene zum separaten Aufbau einer Terminalserversitzung eingefügt. Hierbei werden nur Bildschirminhalte übertragen, und die Dateien bleiben auf dem Server der Daten verarbeitenden Stelle. Mit einer sorgfältigen Planung und mit detailliert dokumentierten organisatorischen Maßnahmen können Risiken, die aufgrund mangelnder Kontroll- und Eingriffsmöglichkeit beim Einsatz privater Geräte entstehen, mit technischen Maßnahmen so verringert werden, dass kein Widerspruch zu einer ordnungsgemäßen Datenverarbeitung besteht. Bei allen Begehrlichkeiten: Aufwand und Schutzbedarf müssen in einem angemessenen Verhältnis bleiben.

Insbesondere bei der Nutzung der Terminalserverdienste sind gewisse Sicherheitsmaßnahmen einzuhalten. So muss

- die Nutzung der Terminalserverdienste an eine **Zwei-Faktor-Authentifizierung** gebunden sein, z. B. durch Eingabe einer PIN und die Nutzung eines Tokens,
- eine **Dateiübertragung** sowohl auf Ebene der Terminaldienste, über die Netzebene als auch über die Konfiguration der verwendeten Software **ausgeschlossen** sein,

- jeder privat genutzte Computer mit den in der IT- und Sicherheitskonzeption beschriebenen **Sicherheitsmaßnahmen der Daten verarbeitenden Stelle** ausgerüstet sein (z. B. Virenschutz, Patches, Updates); die Ausstattung der Computer mit diesen Sicherheitsmaßnahmen muss vor der Nutzung durch einen Automatismus sichergestellt werden,
- durch **regelmäßige Prüfungen** der verwendeten Computer durch eine Kontrollinstanz gewährleistet werden, dass die technischen Sicherheitsmaßnahmen eingehalten werden.

Werden alle erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen umgesetzt und so dokumentiert, dass die Anforderungen der DSVO erfüllt sind, so ist der Einsatz privater Geräte zur Verarbeitung personenbezogener dienstlicher Daten ausnahmsweise möglich, da die eigentliche Datenverarbeitung auf Geräten der Behörde stattfindet und durch angemessene Sicherheitsmaßnahmen das Risiko der Einsichtnahme und Veränderungen von personenbezogenen Daten auf den privaten Geräten ausreichend verringert wurde. Die Verarbeitung von Daten, die einem **Berufs- oder Amtsgeheimnis** unterliegen, darf aber auch unter diesen Voraussetzungen nicht mit privaten Geräten stattfinden.

Was ist zu tun?
Der Einsatz privater Computer zur dienstlichen Verarbeitung personenbezogener Daten ist nach dem LDSG und der DSVO grundsätzlich unzulässig. Eine Ausnahme ist bei Benutzung von Terminalserverdiensten möglich, sofern spezielle technische und organisatorische Sicherheitsmaßnahmen umgesetzt werden.

6.7 IP-Adressen 1: Grundsätzliches

Eigentlich überall, wo zwei oder mehr Rechner miteinander vernetzt sind, werden Protokolldateien erstellt. Das gilt vom kleinen Heimnetz bis hin zum World Wide Web. Diese Protokolldateien erfüllen durchaus ihren Sinn zum Zweck der Sicherheitsanalyse, Revision oder statistischen Auswertung. Allerdings wird hierbei gern vergessen, dass die zu den genannten Zwecken erhobene IP-Adresse ein personenbezogenes Datum sein kann.

Für Protokolldateien, in denen IP-Adressen oder andere möglicherweise personenbezogene Daten gespeichert sind, gelten die Anforderungen der Datenschutzgesetze, insbesondere das Gebot der **Datensparsamkeit und die Zweckbindung** von den erhobenen Daten. Oftmals lässt sich nach klarer Anforderungsanalyse das Erheben der IP-Adresse umgehen oder ein frühzeitiges Löschen bzw. Anonymisieren der Protokolldaten realisieren.

Zumeist ist die Erfassung der IP-Adressen in der **Standardkonfiguration** des protokollierenden Dienstes verankert, um eine möglichst breit gefächerte Weiterverarbeitung (z. B. für Zwecke der Forensik oder der Statistik) zu gewährleisten. Die Erzeugung von standardisierten Protokolldateien erleichtert es den Analysetools, auf diese Dateien zuzugreifen und sie für eine bessere Lesbarkeit aufzubereiten. Häufig übernimmt die IP-Adresse die Funktion eines eindeutigen Identi-

fikators, um einen bereits bekannten Computer wiederzuerkennen. Diese Zuordnungsmöglichkeit kann für einige Anwendungen erforderlich sein, z. B. zum Erkennen eines wiederholten Angriffsversuchs von einem bestimmten Rechner aus.

Häufig wird allerdings **zu viel und zu lange protokolliert**, frei nach dem Motto „Man kann ja nie wissen!“ Jeder IT-Verantwortliche ist jedoch verpflichtet, sich über einige Grundsätze der datenschutzgerechten Datenerhebung Klarheit zu verschaffen: Welche Daten werden wirklich für meine gestellten Anforderungen benötigt? Wie lange müssen die erhobenen Daten vorgehalten werden? Werden die erhobenen Daten für andere Zwecke weitergegeben oder -verarbeitet? Nach vollständiger Klärung dieser Fragen werden sich einige Datenbestände stark reduzieren lassen. Die Gesetze stellen klar, dass IP-Adressen nur für die Erbringung des Dienstes und für Abrechnungszwecke kurzfristig gespeichert werden dürfen.

Besteht das Erfordernis, die IP-Adresse zu erheben, um eine bestimmte Funktionalität der Anwendung gewährleisten zu können, sind die **Methoden der Anonymisierung, der Pseudonymisierung und des frühzeitigen Löschens** in Betracht zu ziehen. Dient die IP-Adresse als eindeutiger Identifikator, kann diese auch gekürzt oder ersetzt werden. Das Streichen des letzten Oktetts einer IP-Adresse wird bei Protokolldateien mit überschaubarer Anzahl von Einträgen kaum Qualitätseinbußen der anschließenden Anwendung zur Folge haben. Bei sehr großen Protokolldateien kann diese Streichung bewirken, dass unterschiedliche IP-Adressen anschließend nicht mehr zu differenzieren sind. Hier bietet sich eine **Substitution der IP-Adressen** an, d. h., die IP-Adressen werden automatisch durch andere Zeichenfolgen ersetzt, wodurch weiterhin die statistische Auswertung von sogenannten Klickstreams ermöglicht wird. Dabei muss sichergestellt sein, dass die neue Zeichenfolge keine Rückschlüsse auf die ursprüngliche IP-Adresse erlaubt.

In jedem Fall sollten Protokolldateien so früh wie möglich gelöscht oder anonymisiert werden. Müssen z. B. die IP-Adressen zum Zweck von Sicherheitsanalysen kurzzeitig vorgehalten werden, ist ein **Löschen oder Anonymisieren der Daten innerhalb von 24 Stunden** anzuraten. Spätestens nach fünf Tagen dürfte eine Speicherung für diesen Zweck nicht mehr erforderlich sein. Werden die IP-Adressen für statistische Zwecke benötigt, so sollten gleich Tools eingesetzt werden, die diese entsprechend anonymisieren bzw. pseudonymisieren. Meist werden Anwendungen für Protokolldateien täglich ausgeführt, sodass ein längeres Vorhalten der Originaldateien nicht erforderlich ist. Sind hingegen die personenbezogenen Daten vollständig anonymisiert, also ist keine Reidentifikation mehr möglich, sollte die Löschung auch dieser Protokolldateien aus Gründen der Übersichtlichkeit regelmäßig stattfinden.

Was ist zu tun?
IP-Adressen in Protokolldateien unterfallen den Datenschutzgesetzen. Für jede Daten verarbeitende Stelle gilt: Nach einer Anforderungsanalyse, welche Daten zu welchem Zweck wie lange protokolliert werden müssen, ist diese technisch umzusetzen. Dabei gelten die Prinzipien der Datensparsamkeit und der Zweckbindung.

6.8 IP-Adressen 2: Umsetzung in Schleswig-Holstein

Das Internetportal des Landes Schleswig-Holstein stellt dem Nutzer eine Vielzahl an Informationen sämtlicher Ministerien, Kreise, Gemeinden und Städte des Landes sowie eine kleine Anzahl von Services zur Verfügung. Das Speichern der IP-Adressen der Nutzer ist dabei auf ein den Anforderungen entsprechendes Minimum reduziert worden.

Der **Internetauftritt der Landesregierung** wurde mit einem überarbeiteten Layout versehen und die redaktionelle Bearbeitung der Inhalte auf die Basis eines neuen Content-Management-Systems gestellt. Im Zuge dieses Relaunches ist von der Staatskanzlei der Wunsch geäußert worden, das Webangebot datenschutzkonform aufzuarbeiten und das ULD hierbei einzubeziehen. Zwei Schwerpunkte waren ein korrektes Impressum und eine verständliche und richtige Datenschutzerklärung. Zwangsläufig stellten sich zudem Fragen zur Rechtmäßigkeit der Verarbeitung, zu den Verantwortlichkeiten sowie zur Sicherung der Zweckbindung. Für eine bestmögliche Vermittlung der Inhalte möchte die Regierung ihren Internetauftritt stetig optimieren. Daher werden die Seitenaufrufe der Nutzer protokolliert, um sie mithilfe eines Auswertungstools statistisch aufzubereiten. Damit dies datenschutzgerecht geschieht, ist das ULD um Unterstützung gebeten worden.

Bei der Erstellung der Datenschutzerklärung eines Internetangebotes muss der Betreiber sämtliche Prozesse der Erhebung, Verarbeitung und Löschung von personenbezogenen Daten exakt definieren und einer **datenschutzrechtlichen Prüfung** unterziehen. Welche Daten werden wann, wo und zu welchem Zweck erhoben? Wo und wie lange werden diese gespeichert? Wer hat Zugriff auf diese Daten? Wann und wie werden diese gelöscht? Sind sämtliche Prozesse datenschutzkonform? Das Hauptaugenmerk wird im Folgenden auf die protokollierten IP-Adressen gelegt, die häufig zur statistischen Auswertung des Nutzerverhaltens notwendig sind.

Die Staatskanzlei hat bei der Einführung des neuen Content-Management-Systems eine Dokumentation mit sämtlichen Verträgen, Beschreibungen und Konzepten nach Vorgabe der DSVO angelegt. Ein Dokument beschreibt die Anforderungen an die statistische Auswertung der Protokolldateien. Danach ist das Verhalten eines einzelnen Nutzers – über welche Pfade er an bestimmte Informationen gelangt – nicht von Interesse. Die protokollierte IP-Adresse wird somit nur als eindeutiger Identifikator genutzt, um verlässliche Aussagen über die Besucherzahl des Landesportals treffen zu können. Die IP-Adressen dürfen nicht länger als nötig gespeichert werden. Die Staatskanzlei verständigte sich mit dem ULD, die Protokolldateien mit den IP-Adressen **zu Sicherheitszwecken für maximal vier Tage** zu speichern. Danach wurden die IP-Adressen aber nicht vollständig aus dem System eliminiert. Diese fanden sich an anderen Orten im System wieder.

In jeder gut administrierten IT-Umgebung werden in regelmäßigen Abständen **Datensicherungen** durchgeführt. Das Landesportal einschließlich seiner Systemkomponenten wird täglich gesichert, was zur Folge hat, dass auch die Protokoll-

dateien mit den IP-Adressen gesichert werden. Eine Reproduktion sämtlicher IP-Adressen der letzten Wochen oder sogar Monate wäre dann mithilfe der Datensicherungen möglich gewesen. Eine regelmäßige Löschung der gesicherten Originalprotokolldaten war somit unumgänglich.

Die zweite Falle lauerte im **Auswertungstool**. Dieses erstellt nach jedem Durchlauf eine aktualisierte History-Datei, die die IP-Adressen der ausgewerteten Protokolldateien beinhaltet, um Auskunft erteilen zu können, wann ein Nutzer erneut das Angebot in Anspruch nimmt. Diese Funktion war nicht in der Anforderungsanalyse der Staatskanzlei enthalten, also nur ein „nice to have". Ein eigens geschriebenes Skript, das nach jeder erfolgten Auswertung gestartet wird, löscht nun die IP-Adressen aus dieser Datei. Die IP-Adressen zum Zweck der statistischen Auswertung haben somit eine maximale Speicherfrist von 24 Stunden.

Was ist zu tun?
Jeder Betreiber eines Internetangebotes muss sich die Frage beantworten, was er unbedingt wissen muss, um das Angebot zu gestalten. Welches sind nur nette Gimmicks? Ist das Speichern von IP-Adressen wirklich notwendig? Bei notwendig angesehenen IP-Adressdaten sollte der Gebrauch von Anonymisierungstools geprüft werden. Vom Abschneiden des letzten Oktetts bis zur vollständigen Substitution sind unterschiedliche Anonymisierungsgrade möglich.

6.9 Modularisierung der Dokumentation – sinnvoll nicht nur beim Geoserver

Geodaten sind Basis- und Referenzinformationen für viele Verfahren. Diese sollen über einen Geoserver zentral bereitgestellt werden. IT-Konzept und Sicherheitskonzept zum Geoserver sind stilbildend für die kommenden E-Government-Verfahren des Landes.

Das federführende Innenministerium hat sich aus dem „Baukasten E-Government-Infrastruktur" die für den Geoserver benötigten Bausteine herausgenommen und zusammen mit dem Fachverfahren eines Drittanbieters zu einem neuen Paket geschnürt. Das ULD hat beim Erstellen des IT-Konzepts und des Sicherheitskonzepts beraten. Die Herausforderung bestand vor allem darin, die bestehende Dokumentation der einzelnen Bestandteile in einem „Dachdokument" zusammenzuführen. Hierbei ergab sich eine **modulare Vorgehensweise**, die das ULD auch anderen Verfahren der E-Government-Infrastruktur empfiehlt.

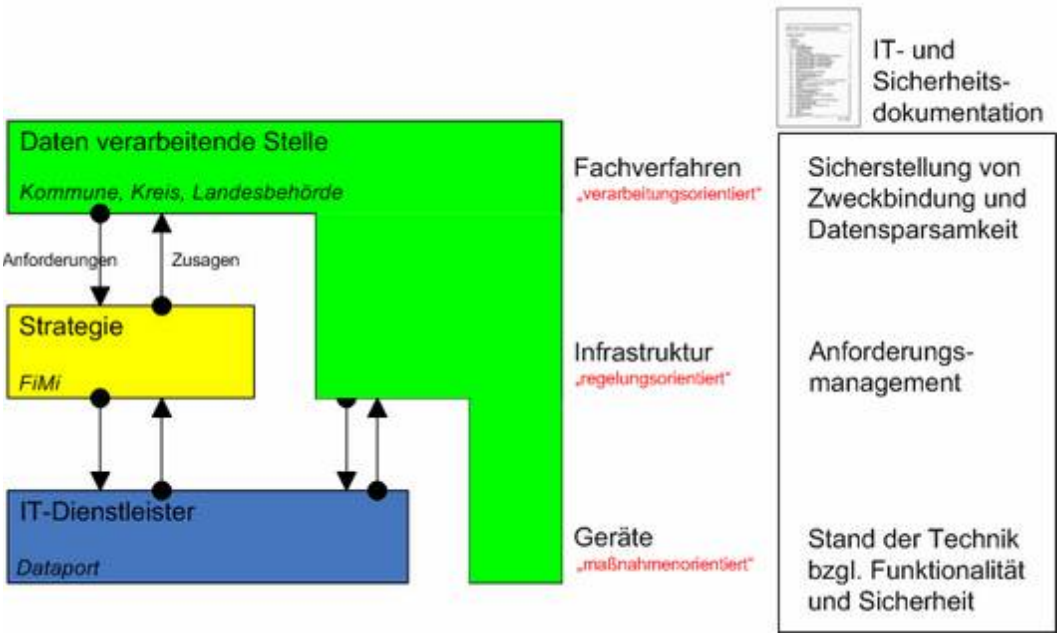
Ein IT-Konzept enthält die wesentlichen Ziele und Entscheidungen zur einzusetzenden Technik. Daraus ergeben sich die nötigen Sicherheitsmaßnahmen, die entsprechend LDSG und DSVO zu dokumentieren sind. Der Geoserver soll auf der vom Finanzministerium zu verantwortenden E-Government-Infrastruktur aufsetzen und mit den IT-Gerätschaften Dataports betrieben werden. Soll für eine solche **Informationstechnik über Organisationsgrenzen hinweg** eine Dokumentation erstellt werden, so ist besonders schwierig zu entscheiden, welche Themenbereiche in welchem Abschnitt in welcher Auflösung darzustellen sind.

Ein Vorgehen in drei Schichten bietet sich an:

- Schicht 1 erfasst ausschließlich technische und organisatorische Maßnahmen, die direkt den Fachverfahren zuzuordnen sind.
- In Schicht 2 werden die Infrastrukturbausteine der E-Government-Infrastruktur betrachtet.
- Schicht 3 kümmert sich schließlich um konkrete Maßnahmen auf Ebene der Geräte, wie z. B. Serversysteme oder Netzkomponenten.

Ordnet man die Sachverhalte schichtbezogen den jeweiligen Zuständigkeiten zu, so kommt man zu einem modularen Aufbau der Dokumentation mit speziellen Anforderungen an Datenschutz und Datensicherheit sowie eigenen Kontrollanforderungen für jeden Bereich.

Die IT-Dokumentation im Bereich des Fachverfahrens muss zunächst den **Zweck des Verfahrens und die zu erfüllenden Rechtsgrundlagen** ausweisen. Im entsprechenden Pendant der Sicherheitsdokumentation ist darzulegen, wie dieser Zweck **datensparsam umgesetzt** und wie die Einhaltung der Anforderungen durch technisch-organisatorische Vorkehrungen durchgesetzt und durch Regularien wie Dienstvereinbarungen auf der Fachverfahrensebene kontrolliert wird. Auf dieser Ebene muss die Spezifikation der Nutzerrollen erfolgen. Hier ist auch der Nachweis des rechtskonformen Verwaltungshandelns zu führen. Es ist festzulegen, wie die Kontrolle bezüglich der Einhaltung der Regularien geschieht und welche Prozesse eingerichtet sind, wenn gegen Regeln verstoßen wurde. Aus datenschutzrechtlicher Sicht muss gezeigt werden, welche Mitarbeiteraktivitäten wie protokolliert werden – unter Vermeidung einer Leistungs- und Verhaltenskontrolle.



Ein Fachverfahren setzt entweder auf einer übergreifenden IT-Infrastruktur des Landes sowie den konkreten Gerätschaften eines IT-Dienstleisters auf oder wird lokal in Eigenregie betrieben. Wenn ein Fachverfahren an technischen Dienstleistungen anderer Organisationen anknüpft, muss dies entweder durch eine **gesetzliche Grundlage**, etwa eine Verordnung, oder einen **Vertrag** geregelt sein. In dem Vertrag sind **Anforderungen** seitens des Auftraggebers und **Zusicherungen** seitens des dienstleistenden Auftragnehmers bezüglich Funktionalität, Sicherheit und Datenschutz enthalten. Solche Verträge gehören zur Sicherheitsdokumentation, damit klargestellt ist, auf welche Aspekte die Kontrollfunktionen zur Überwachung des Auftragnehmers abzielen. Anforderungen und Zusagen müssen gegeneinander abgeglichen werden. **Es dürfen keine Lücken entstehen**, bei denen für eine Anforderung keine entsprechenden Zusagen vorhanden sind.

Im Bereich der Infrastruktur müssen im IT-Konzept und im Sicherheitskonzept solche Aspekte angeführt werden, die das Anforderungsmanagement (Anforderungen/Zusicherungen) und deren Controlling betreffen. Hier wird auch festgelegt und gerechtfertigt, was als **Stand der Technik** bezüglich der Applikation für das Fachverfahren, der Infrastruktur und der eingesetzten Hardware gilt und welche Schutzziele bezüglich dieser drei Aspekte zu verfolgen sind. Hier müssen die Verfahren beschrieben werden, mit denen die Zugriffe auf Daten geschehen dürfen. Auch ist darzulegen, welche Instanz auf welche Art und Weise welche Personen autorisiert. Zudem werden bestimmte Fachverfahren und deren Anforderungen in die der vorhandenen Infrastruktur eingepasst. Unter Kontrollaspekten muss hier dokumentiert sein, welchem Paradigma das Controlling aller beteiligten Seiten folgt und welche organisatorischen Prozesse im Rahmen des Sicherheits- und Datenschutzmanagements, insbesondere bei Regelverstößen, zu durchlaufen sind.

Im Bereich des IT-Dienstleisters müssen im IT-Konzept die für das Fachverfahren eingesetzten **Gerätschaften und deren Konfigurationen** entlang dem physikalischen Netzplan **dokumentiert** werden. Neben den Anforderungen der DSVO ist eine Orientierung an den BSI-Grundschutzkatalogen und -Maßnahmen empfehlenswert. Besonderes Augenmerk ist dabei auf die Dokumentation der Zugriffsmöglichkeiten der Systemadministration und deren Protokollierung zu legen.

Führt man diese Art der modularen Dokumentation ein, so **kümmert sich jede beteiligte Organisation nur um ihre originäre Zuständigkeit**. Jede Organisation muss lediglich die Schnittstellen festlegen. Dies geschieht über den Mechanismus der Anforderungen und Zusagen. Werden diese genau und verständlich formuliert, so kann eine **schlanke Dokumentation** entstehen, die allen Beteiligten nützt und gleichzeitig die Anforderungen des LDSG und der DSVO erfüllt.

Beim Geoserver wurden all diese Punkte berücksichtigt. Von dieser Verfahrensweise zur Erstellung der Dokumentation können nun andere E-Government-Projekte profitieren.

Was ist zu tun?
Gerade im Bereich der E-Government-Verfahren sollten sich IT-Verantwortliche vor Projektstart mit dem ULD in Verbindung setzen, um eine modulare Dokumentation und insbesondere eine Sicherheitskonzeption zu entwickeln.

6.10 ISMS Dataport

Das im vergangenen Jahr bei Dataport eingerichtete Informationssicherheitsmanagementsystem (ISMS) konnte erfolgreich fortentwickelt und auf weitere Kundenverfahren und Infrastrukturen angewandt werden.

Schon im vorangegangenen Jahr hatte Dataport begonnen, ein **Managementsystem für Informationssicherheit (ISMS)** aufzubauen und auf erste Verfahren (ZIAF) und Infrastrukturen (Landesnetz, KITS.system) anzuwenden. Eine schrittweise erfolgende Implementierung des ISMS bei Dataport war vorgesehen (30. TB, Tz. 9.1.3). Diese Planungen wurden konkretisiert und umgesetzt, vor allem in der Fortentwicklung der Aufbauorganisation des ISMS und in der Weiterentwicklung zahlreicher Dokumente wie Leit- und Richtlinien. Diese Aktivitäten haben auch im erheblichen Maße zur erfolgreichen Zertifizierung bei ZIAF (Tz. 9.2.2) beigetragen.

Nach und nach wird das ISMS auf weitere Verfahren und Infrastrukturen bei Dataport ausgerollt. In diesem Umfeld sind die folgenden **Audits** bei Dataport und im Zuge von Fachverfahren von Kunden geplant:

- der Verfahrensbetrieb über Terminaldienste (ABS) – in dieser Infrastruktur werden auch die MLUR-Verfahren K3 und BalVI betrieben,
- das Druck- und Kuvertierzentrum (DuK),
- das ebenfalls von der Finanzverwaltung des Landes Schleswig-Holstein genutzte Data Center Steuern (DCS) mit seinen Standorten Rostock und Schwerin.

Für das DCS und das DuK hat die Auditierung schon begonnen – die Phase der Erhebung wurde bereits erfolgreich abgeschlossen. Auch für K3, BalVI und das DCS ist ein **Abschluss der Auditierung im Jahr 2009** geplant.

Was ist zu tun?
Die erfolgreich begonnene, schrittweise erfolgende Implementierung des ISMS ist fortzusetzen und weitere, im Auftrag von Kunden betriebene Fachverfahren sind einzubeziehen.

6.11 Zielarchitektur Basis-Infrastruktur bei Dataport

Dataport erfindet sich neu: Eine neue Zielarchitektur soll einen wirtschaftlichen, sicheren und datenschutzfreundlichen Betrieb von Fachverfahren ermöglichen. Die neue Zielarchitektur existiert jedoch bisher größtenteils nur in den Köpfen der Planer.

Die vier strategischen Partner von Dataport, die Firmen Cisco, EMC, Fujitsu Siemens Computers und Microsoft, haben für Dataport ein Konzept für die Neuausrichtung der technischen Basisinfrastruktur entwickelt. Die Arbeitsergebnisse des Projekts mit dem Namen Zielarchitektur Basis-Infrastruktur (ZaBI) sollen es Dataport ermöglichen, eine transparente, einheitliche und **skalierbare Architektur** für die im Kundenauftrag betriebenen Komponenten zum Transportieren, Verarbeiten und Speichern von Daten aufzubauen. Das ULD berät Dataport mit dem Ziel einer datenschutzfreundlich gestalteten Infrastruktur. Dies bedeutet insbesondere, dass

- eine lückenlose Protokollierung administrativer Tätigkeiten erfolgt,
- die Konfiguration aller an einem Fachverfahren beteiligten Systeme und Komponenten nachvollziehbar ist,
- die betrieblichen Prozesse vorab festgelegt, bei der Ausführung dokumentiert und regelmäßig überprüft werden,
- die in den jeweiligen Modulen von ZaBI geplanten Sicherheitsmaßnahmen angemessen und wirksam sind und
- das Datenschutz- und Sicherheitsmanagement sowohl bei Dataport, aber vor allem bei den Kunden unterstützt wird.

Die bisherigen Arbeitsergebnisse des Projekts ZaBI sind vielversprechend und stellen einen Qualitätsgewinn durch Vereinheitlichung der Technikplanung im Vergleich zur bisherigen Architektur in Aussicht. Dataport hat es bisher jedoch nicht geschafft, die neue Architektur umzusetzen. In vielen Bereichen fehlen noch **Detailkonzepte**, die auch den Kunden als Grundlage für eigene Sicherheitskonzepte dienen können.

http://www.rechenzentrum2010.de/

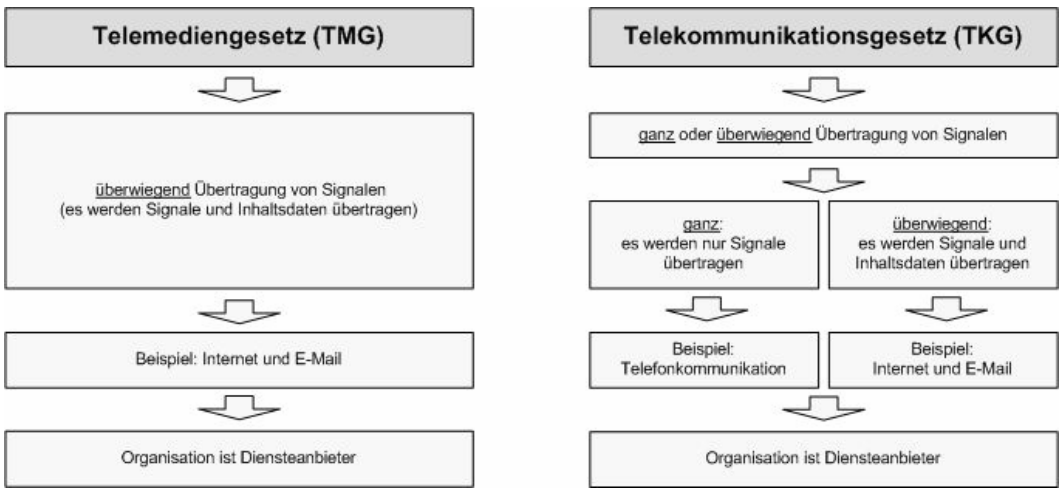
Was ist zu tun?
Das Ziel steht fest, der Weg ist in groben Zügen beschrieben. Dataport muss die in den Grobkonzepten erhobenen Anforderungen und die bereits festgelegte technische Ausrichtung schnell und konzeptkonform durch eine Feinkonzeption untermauern.

6.12 Internetnutzung: Privat oder rein dienstlich?

E-Mail-Kommunikation und Internetnutzung sind ein fester Bestandteil des modernen Behördenalltags. Doch der gesetzliche Rahmen zur Nutzung dieser Dienste verursacht in vielen Behörden Unsicherheit. Darf eine Behörde die private Internet- und E-Mail-Nutzung erlauben? Und wenn ja, unter welchen Bedingungen?

Der Einsatz von E-Mail-Kommunikation und Webnutzung in öffentlichen Stellen setzt eine funktionierende IT- und Sicherheitsdokumentation nach LDSG und DSVO voraus mit der Beschreibung der nötigen IT-Komponenten, deren Konfiguration, Datensicherheitsmaßnahmen und Kontrollflüssen. Auch bei Internetdiensten muss die Entscheidung über den **Umfang der Nutzung durch Mitarbeiter** von der Dienststellenleitung getroffen und dokumentiert werden. Das Fehlen einer geeigneten Regelung kann rechtliche Konsequenzen nach sich ziehen. Wird z. B. eine private Nutzung der Internetdienste fortwährend stillschweigend geduldet, so ist dieser Zustand als Erlaubnis durch „betriebliche Übung“ anzusehen.

Das Maß der erlaubten Nutzung von Internetdiensten hat Auswirkungen auf die Verpflichtungen der Daten verarbeitenden Stelle nach dem Telemediengesetz (TMG) und dem Telekommunikationsgesetz (TKG). Die nachfolgende Grafik stellt die beiden Gesetze in Auszügen grob gegenüber:

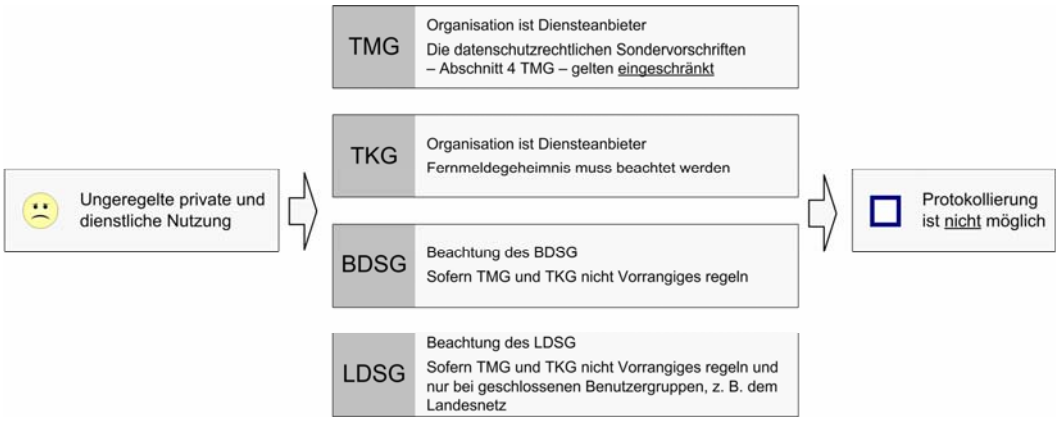


Die Nutzung der Internetdienste in einer Daten verarbeitenden Stelle kann in drei Szenarien unterteilt werden:

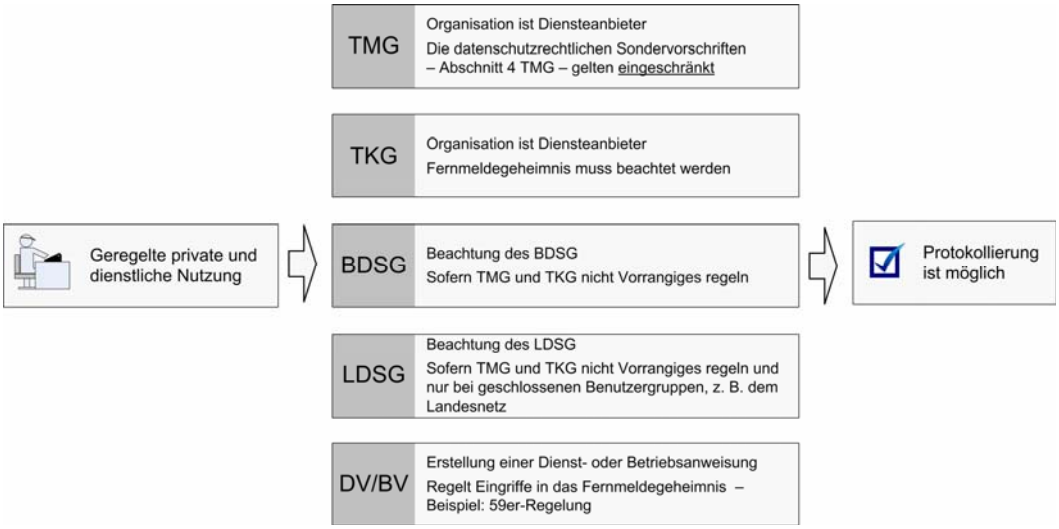
- geregelte rein dienstliche Nutzung,
- ungeregelte private und dienstliche Nutzung,
- geregelte private und dienstliche Nutzung.

Die folgenden Übersichten zeigen für jedes Szenario den rechtlichen Status der Daten verarbeitenden Stelle und die geltenden datenschutzrechtlichen Normen.

Wird die E-Mail-Kommunikation und Internetnutzung nur zu **rein dienstlichen Zwecken** erlaubt, nimmt die Daten verarbeitende Stelle den Status eines Diensteanbieters nach dem TMG ein. Die datenschutzrechtlichen Sondervorschriften zum Schutz der Nutzer finden aber keine Anwendung. Die Stelle darf daher die Benutzeraktivitäten im Rahmen von technisch-organisatorischen Datenschutzkontrollen prüfen.



Ist bei Internetdiensten die **Nutzung ungeregelt** und die Mitarbeiter nutzen diese zu privaten und dienstlichen Zwecken, so bekommt die Stelle den Status eines Diensteanbieters nach dem TMG und nach dem TKG. Das bedeutet, dass die Daten verarbeitende Stelle an das Fernmeldegeheimnis gebunden ist; eine Auswertung von Protokolldaten ist unzulässig.



Wird die private Nutzung der **Internetdienste eingeschränkt erlaubt**, so hat die Daten verarbeitende Stelle – ebenfalls – den Status eines Diensteanbieters nach dem TMG und nach dem TKG, und die Daten verarbeitende Stelle ist an das Fernmeldegeheimnis gebunden. Durch Einwilligung des betroffenen Beschäftigten sowie durch Betriebsvereinbarung im nicht öffentlichen Bereich bzw. Dienstvereinbarung im öffentlichen Bereich können aber Eingriffe in das Fernmeldegeheimnis zulässig sein.

Bei der Erarbeitung einer **Dienst- bzw. Betriebsanweisung** ist Folgendes zu beachten:

- Erlaubt eine Daten verarbeitende Stelle die private Nutzung, wozu sie nicht verpflichtet ist, so kann sie die Erlaubnis an einschränkende Voraussetzungen knüpfen. Die Kontrollmechanismen müssen datenschutzkonform sein.
- Eine Internetnutzung, die den Interessen der Daten verarbeitenden Stelle entgegensteht oder gegen strafrechtliche bzw. urheberrechtliche Vorschriften verstößt, sollte untersagt werden.
- Eingehende private E-Mails sind wie private (Papier-)Post zu behandeln. Fälschlich als Dienstpost behandelte E-Mails sind den betroffenen Mitarbeitern unverzüglich zur alleinigen Kenntnis zu geben.
- Die Inanspruchnahme kostenpflichtiger Angebote sowie die Verfolgung kommerzieller Zwecke im Rahmen der privaten Nutzung sollte untersagt werden.
- Für die private Nutzung des Internetzugangs kann ein separates Benutzerkonto zur Verfügung gestellt werden. Durch Protokollierung und Auswertung der Nutzungszeiträume des privaten Benutzerkontos kann festgestellt werden, ob zeitliche Vorgaben eingehalten werden.
- Die Protokollierung zu Zwecken der Datenschutzkontrolle, der Abrechnung, der Datensicherheit oder zur Vorbeugung strafrechtlich relevanten Verhaltens ist zulässig. Für darüber hinausgehende Kontrollen sind eine Betriebs- bzw. Dienstvereinbarung oder die Einwilligung des Betroffenen nötig.

Beispiel: Die **Richtlinie zur Nutzung von Internet und E-Mail** nach dem Mitbestimmungsgesetz des Landes (MBG) regelt die dienstliche und private Nutzung der dienstlich zur Verfügung gestellten Services Internetzugang und E-Mail und gilt für die Beschäftigten der unmittelbaren Landesverwaltung, deren PCs an das Landesnetz angeschlossen sind (Amtsbl. Schl.-H. 2005, S. 27 ff.). Diese Richtlinie kann für den Bereich der Kommunalverwaltung als Vorbild dienen.

Um datenschutzkonforme **Protokollierungs- und Kontrollmaßnahmen** durchzuführen, ist ein gestuftes Vorgehen zu empfehlen (Tz. 6.13).

Was ist zu tun?
Die erlaubte private Nutzung von Internetdiensten sollte über eine Dienst- bzw. Betriebsvereinbarung geregelt werden. Die Beschäftigten sind über die Regelungen zu informieren, die ein gestuftes Verfahren möglichst datensparsamer Kontrollen vorsehen.

6.13 Überwachung der Internetnutzung von Mitarbeitern

Was ist zu tun, wenn die Überwachung von Mitarbeiterinnen und Mitarbeitern notwendig wird? Grundsätzlich gilt, dass eine beabsichtigte Überwachung von Mitarbeitern zur Aufdeckung von Missbräuchen ausschließlich in einem für alle Mitarbeiter transparenten, geregelt-kontrollierten Verfahren geschehen darf. Erst auf einer rechtlich geregelten Grundlage stellt sich dann die Frage, wie das Zusammenspiel von Regelungen und Technik auszugestalten ist.

Heutige Firmen betreiben typischerweise an ihrer Schnittstelle zum Internet einen **Proxy**. Mit dessen Hilfe können die Inhalte des Datenverkehrs ins und aus dem Internet automatisiert geprüft werden, um beispielsweise

- die Filterungen von Inhalten mit Schadfunktion vorzunehmen,
- um eine Authentisierung und Autorisierung von Mitarbeitern durchzuführen,
- um die Internetnutzung zu protokollieren oder
- um an dieser zentralen Stelle bestimmte Regelungen, beispielsweise bezüglich der Anbindung mobiler Geräte, durchzusetzen.

Was an einem Proxy in welchem Ausmaß und welcher Form (z. B. als Rohdaten, pseudonymisiert, anonymisiert) zu welchem Zweck protokolliert und von welcher Abteilung dann kontrolliert wird, muss in einer **Betriebsvereinbarung** aufgeführt und festgelegt werden. Problematisch wird es insbesondere dann, wenn die private Nutzung des Internets erlaubt wird bzw. keine Dienstvereinbarung vorliegt, in der die private Nutzung der technischen Infrastruktur grundsätzlich ausgeschlossen ist. Dann liegt die Situation der „betrieblichen Übung“ vor, wonach die private Nutzung durch Mitarbeiter geduldet wird (Tz. 6.12). Im Falle der privaten Nutzung hat der Arbeitgeber das Telekommunikationsgeheimnis zu achten, darf insbesondere also nicht in den Mailverkehr der Mitarbeiter hineinsehen.

Wie kann ein **transparentes und zielführendes Kontrollverfahren** aussehen? Zunächst sind Zweck und die akzeptablen Anlässe einer Kontrolle als Bestandteile der Dokumentation schriftlich festzulegen, dann die Verfahrensabläufe, wie Kontrollen durchzuführen sind, zu beschreiben sowie eine Betriebsvereinbarung zu schließen, die die Mitarbeiter darüber in Kenntnis setzt. Eine Betriebsvereinbarung muss zumindest die folgenden Aspekte ansprechen:

- Festlegen des Umfangs der erlaubten Nutzung,
- Festlegen des Zwecks und möglicher Anlässe sowie des Umfangs von Kontrollen und Protokollierungen,
- Festlegung der Aufbewahrungsfristen von Protokolldaten,
- Festlegung der Ausgestaltung personenbezogener Auswertungen,
- Festlegung der Regelungen zu Sperrungen von Kommunikationspartnern oder Webseiten,
- Festlegung der Berechtigungen des Zugriffs auf Hard- und Software sowie
- Festlegen des Verfahrens, unter welchen Umständen Administratoren auf personenbezogene Datenbestände zugreifen dürfen.

All dies sollte in eine generelle IT- und Sicherheitsdokumentation, die auch Konfigurations- und Berechtigungseinstellungen zu enthalten hat, eingepasst sein.
Ein Kontrollverfahren zur Aufdeckung von Missbräuchen oder Regelverstößen sollte zumindest über die folgenden **vier Eskalationsstufen** verfügen:

Stufe 1: In der Firmenöffentlichkeit kommunizieren, dass Fälle von Missbräuchen oder Regelverstößen vorgekommen sind.

Weitergehende Sanktionen entsprechend den Ausführungen in der Betriebsvereinbarung (dies entspricht den nachfolgenden Stufen) ankündigen, sofern weiterhin Missbräuche und Regelverstöße festgestellt werden.

Stufe 2: Anonyme oder pseudonyme Protokollierung zentral am Proxy

- Beteiligung des Datenschutzbeauftragten und der Personalvertretung,
- Analyse der Protokolldaten,
- Kommunikation der Ergebnisse in der Firmenöffentlichkeit, z. B. in Form einer Top-Ten-Liste,
- Hinweis, dass bei fortgesetztem Missbrauch personenbezogene Kontrollen oder Protokollierungen durchgeführt werden,
- mögliche technische Unterstützung, z. B. können im Fall einer Internetnutzung mit unerwünschten Webseiten deren Adressen in eine „Blacklist“ eingetragen werden, sodass die entsprechenden Server nicht erreichbar sind.

Die Auswertung der Daten kann dazu führen, dass sich als Quelle eines Missbrauchs eine Abteilung identifizieren lässt. Auch darüber kann ein letzter Versuch gestartet werden, einen Appell an die Firmenöffentlichkeit zu richten, die unerwünschten Handlungen zu unterlassen.

Stufe 3: Personenbezogene Protokollierung auf einem Proxy

Hierbei muss man die folgenden Regelungen vorsehen:

- Datenschutzbeauftragten beteiligen,
- personenbezogene Protokollierung in der Firmenöffentlichkeit ankündigen,
- den genauen Zweck, den Umfang der Daten und den Zeitraum der Protokollierung und deren Auswertung vorab in einem Konzept festlegen; der Umfang der von der Protokollierung erfassten Personen muss dabei auf den Kreis der Verdächtigen begrenzt werden, es darf nicht das gesamte Personal überwacht werden,
- Auswertung der Protokolldaten nur unter Beteiligung der Personalvertretung und des Datenschutzbeauftragten,
- vollständige Dokumentation der Auswertung,
- Löschung der personenbezogenen Daten nach Auswertung,
- Kommunikation der Ergebnisse,
- Abwägung des weiteren Vorgehens unter allen Beteiligten entsprechend der Ergebnisse:
  - Einstellen der Kontrollen, keine weitere Überwachung,
  - Rückkehr zu Stufe 2, weil man nach wie vor mit Verstößen rechnen muss,
  - nochmaliges Verschärfen der Kontrolle, indem die Protokollierung auf dem Arbeitsrechner der Verdächtigen stattfindet (siehe Stufe 4).

Stufe 4: Personenbezogene Protokollierung auf dem Arbeitsrechner ohne Ankündigung

Hierfür gelten dieselben Anforderungen wie für die Stufe 3 mit Ausnahme der Ankündigung. Diese Protokollierung darf ebenfalls nur dann geschehen, wenn die Mitarbeiter in der Betriebsvereinbarung darüber aufgeklärt wurden, dass diese letzte Eskalationsstufe unter bestimmten Bedingungen zum Einsatz kommen kann. In dieser äußersten Eskalationsstufe sollte man erwägen, bereits eine Strafanzeige zu stellen und eine Strafverfolgungsbehörde hinzuzuziehen, um bei der Beweissicherung keine Fehler zu machen.

Was ist zu tun?
Die Möglichkeiten der Mitarbeiterüberwachung müssen den Mitarbeitern dargestellt werden. Es ist gestuftes, langsam eskalierendes Verfahren zur Mitarbeiterüberwachung festzulegen. Der Zweck der Abstufung einer Mitarbeiterüberwachung besteht darin, unerwünschte Handlungen zu vermeiden und, erst ganz zuletzt, Mitarbeiter zu überführen.

6.14 Kontrollen vor Ort

6.14.1 Prüfungen bei Stadtverwaltungen: Lob für Heiligenhafen

Das ULD kontrolliert die Einhaltung der Vorgaben des LDSG und der DSVO direkt vor Ort. Der Schwerpunkt der datenschutzrechtlichen Prüfungen der technischen und organisatorischen Sicherungsmaßnahmen lag wieder bei den Stadtverwaltungen des Landes.

Bei unseren Prüfungen stellen wir immer wieder fest, dass die Verwaltungen, die ihren „**Laden im Griff**" haben, auch in Fragen des Datenschutzes und der Datensicherheit kaum Anlass zur Kritik geben. Erweisen sich Defizite in der innerbehördlichen Steuerung, sind Zuständigkeiten nicht klar geregelt, und liegt schon das allgemeine Verwaltungshandeln im Argen, so steht es zumeist auch schlecht um Datenschutz und Datensicherheit.

Positiv tat sich die **Stadtverwaltung Heiligenhafen** hervor. Die geforderten Dokumentationen waren vorbildlich erstellt und auf dem neuesten Stand. Lediglich die durchgeführten Tests waren nicht nachvollziehbar. Der Administrator wusste nicht, wie dies datenschutzkonform zu bewerkstelligen ist. Nach Bereitstellung von Mustern versicherte uns der IT-Verantwortliche, die Dokumentation schnellstmöglich nachzuholen.

Die im Sicherheitskonzept dokumentierten Regeln waren technisch umgesetzt, u. a. durch die flächendeckende Installation von Programmen zur **Absicherung externer Schnittstellen**. Dies ist wichtig, denn personenbezogene Daten könnten leicht und unbemerkt auf Wechseldatenträgern die Organisationseinheit verlassen. Zudem könnte selbst ein durch eine Firewall und andere Sicherheitsmaßnahmen von außen gut geschütztes Netz von innen durch Computerviren verseucht werden. Über eine umfangreiche Schnittstellenkontrolle konnte die Administration steuern, welche Benutzer oder Gruppen auf USB- und FireWire-Ports, WiFi- und Bluetooth-Adapter, CD-ROMs, Disketten und andere entnehmbare Geräte Zugriff haben. Das sehr gute Prüfungsergebnis zeigte, dass das Thema Datenschutz in der Stadtverwaltung Heiligenhafen ernst genommen wird – ein dickes Lob!

Was ist zu tun?
Das ULD wird weiterhin Stadtverwaltungen prüfen und hat als zusätzlichen Schwerpunkt Verwaltungszusammenschlüsse gewählt.

6.14.2 Amtshilfe bei einer Prüfung

Das ULD berät auch andere Prüforganisationen: Das Rechnungsprüfungsamt des Kreises Pinneberg wurde durch das ULD bei der Bewertung technischer und organisatorischer Sachverhalte unterstützt.

Das ULD wurde vom Rechnungsprüfungsamt gebeten, die Umsetzung angemessener Sicherheitsmaßnahmen und die Qualität der Dokumentation des IT-Einsatzes

zu prüfen. Die geprüfte Verwaltung hat einen Großteil der Datenverarbeitung an Dataport **ausgelagert**. Sie nutzt dafür Teile der Produktlinie ABS.

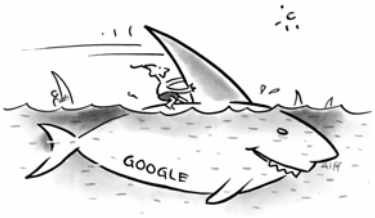
Das ULD stellte sowohl bei der Stadtverwaltung als auch beim Dienstleister Dataport datenschutzrechtliche Mängel fest, die daraufhin durch das Rechnungsprüfungsamt beanstandet wurden. Die Behebung dieser Mängel wird gemeinsam mit dem Rechnungsprüfungsamt überwacht. Unabhängig von der Prüfung arbeiten wir zusammen mit Dataport daran, die **Produktlinie ABS zu verbessern**: ABS-Kunden müssen besser darin unterstützt werden, die datenschutzrechtlichen Anforderungen an eine ordnungsgemäße Datenverarbeitung zu erfüllen.

Was ist zu tun?
Die geprüfte Verwaltung muss die aufgedeckten Mängel beheben und vor allem eine bessere Kontrolle über ihren Dienstleister ausüben. Das ULD wird die Mängelbehebung überwachen und gegebenenfalls durch eine eigene Prüfung kontrollieren. Dataport muss seine Produktlinie ABS datenschutzfreundlicher ausgestalten und die festgestellten Defizite schnellstmöglich beheben. Außerdem muss Dataport bei Neukundenanfragen zu ABS darauf achten, dass die Kunden ausreichend über die vorhandenen Sicherheitszusagen und -mechanismen informiert werden. So können die Auftraggeber ihre eigenen Sicherheitsmaßnahmen und Dokumentationspflichten besser planen und umsetzen. Dataport und das ULD haben hierzu regelmäßige Treffen und Beratungsgespräche vereinbart.

7 Neue Medien

7.1 Kundendaten? Google doch mal!

„Bitte reservieren Sie für mich die Romantiksuite mit Candle-Light-Dinner über Pfingsten und belasten Sie meine Kreditkarte." Diese und viele weitere intime Details waren im Netz zu erfahren. Auch E-Mail-Adressen, Postanschriften, Kontodaten und Telefonnummern von Kunden fanden sich im Internet.



Betroffen waren ein Erotikversandanbieter, ein Hotelbuchungssystem und ein Anzeigenblatt im Internet. Die Verfügbarkeit im Netz war allemal unzulässig, sie war aber auch äußerst geschäftsschädigend. Gerade für derartige Unternehmen ist das Vertrauen der Kunden in die Sicherheit der Daten eine Grundlage des Geschäfts. Was war geschehen? In allen Fällen führte die Fehlprogrammierung zu einer Freigabe der in Internetformulare eingegebenen Daten. Die Eingabe durch die Betroffenen hätte in geschützten Verzeichnissen abgespeichert werden müssen. Sie landeten jedoch in **über das Internet frei zugänglichen Verzeichnissen**. Das wiederum führte zur Erfassung durch Indizierungsdienste von Suchmaschinen. Suchte man bestimmte Angaben über einen Betroffenen oder verwendete man ein bestimmtes Suchschema, wurde der Einblick in die teilweise äußerst intimen Kundendateien möglich.

Das BDSG verpflichtet jeden Datenverarbeiter zu angemessenen **Datensicherheitsmaßnahmen**. Kundendaten müssen vor dem unberechtigten Zugriff Dritter und Verlust geschützt werden. Nutzen Unternehmen das Medium Internet, so haben sie sicherzustellen, dass Daten ihrer Kunden nicht einer weltweiten Öffentlichkeit zugänglich gemacht werden.

Anbieter von **Suchmaschinen** trifft ebenfalls eine Verantwortung zum Schutz der Persönlichkeitsrechte. Sie müssen Verfahren bereithalten, um unzulässig eingestellte Inhalte im Netz, die durch die Suchmaschine indiziert wurden, aus ihrem Zwischenspeicher schnell und effektiv wieder zu entfernen. Verfahren, bei denen der Nutzer erst einen Account anlegen muss oder die auf der Webseite der Suchmaschine so versteckt sind, dass eine Löschung nur mit Vorwissen oder intensiver Recherche erreicht werden kann, genügen nicht. Nicht akzeptabel ist eine Verfahrensdauer von zwei Wochen und teilweise erheblich mehr, um derartige Daten aus der Suchmaschine zu entfernen.

Was ist zu tun?
Unternehmen, deren Kundendaten ins Internet gelangt sind, müssen unverzüglich das Datenleck schließen, die Indizierung dieser Daten bei den gängigen Suchmaschinen aufheben lassen, die Löschung in den Zwischenspeichern der Suchdienste umgehend veranlassen, die Betroffenen über den Vorfall in geeigneter Weise unterrichten und eine Fehleranalyse durchführen, um derartige Vorfälle zukünftig zu unterbinden.

7.2 Google Analytics Services – Webtracking auf dem Prüfstand

Presseberichte und Hinweise durch Nutzer veranlassten das ULD gemeinsam mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit zu einer Prüfung des Einsatzes des Webtracking-Dienstes Google Analytics Services.

Wir forderten schleswig-holsteinische Webseitenbetreiber und Nutzer sowie parallel Google Germany auf, uns mitzuteilen, wie die Datenschutzanforderungen des Telemediengesetzes (TMG) bei diesem Dienst umgesetzt werden. Unter den Anwendern des Dienstes befinden sich äußerst **renommierte Unternehmen** aus allen Branchen. Diese sind für die Erhebung, Verarbeitung und Nutzung der Nutzerdaten mit dem Dienst datenschutzrechtlich verantwortlich.

Nach dem TMG ist es Telemediendiensteanbietern gestattet, unter **Verwendung von Pseudonymen** zum Zweck der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile zu erstellen. Voraussetzung ist, dass die Nutzerinnen und Nutzer der betreffenden Webseite vor der Erhebung ihrer Nutzungsdaten umfassend über Art, Umfang, Dauer und Verwendung der Erhebung und Speicherung informiert werden und ihnen die Möglichkeit eingeräumt wird, der Erstellung des Nutzungsprofils zu widersprechen.

Wir mussten feststellen, dass bereits die Konfiguration der kostenlos angebotenen Software die Umsetzung der gesetzlichen Anforderung durch die geprüften Webseitenbetreiber erschwert bzw. unmöglich macht (Tz. 10.6). Die von Google in den Nutzungsbedingungen verfasste Erklärung zu der Art, dem Umfang und dem Zweck der Erhebung der Daten **lässt die Nutzer im Unklaren** darüber, welche Daten konkret über sie zu welchem Zweck erhoben werden. Fehlanzeige auch bei der Beantwortung der Frage, wie lange die Nutzungsdaten bei Google Inc. mit Sitz in den USA gespeichert werden.

Google Inc. räumt sich ausdrücklich in seinen beim Einsatz zu akzeptierenden Regularien das Recht ein, die über den einzelnen Nutzer mittels einer eindeutigen Kennung gewonnenen Daten mit anderen bereits gespeicherten Daten zu verknüpfen und diese Informationen an Dritte weiterzugeben. Dies steht mit den Vorgaben des TMG im Widerspruch. Die Zusammenführung des pseudonymisierten Profils mit Angaben über die hinter dem Pseudonym stehenden natürlichen Personen ist unzulässig. Aufgrund der **weltweit verstreuten Standorte** der Server von Google ist wahrscheinlich, dass ein den deutschen Datenschutzbestimmungen nicht entsprechender Zugriff auf die Profile durch die staatlichen Behörden der jeweiligen Länder erfolgen kann. Nicht erkennbar ist, an welche Unternehmen konkret Google die gesammelten Informationen übermittelt. Derartige Übermittlungen lässt sich die Google Inc. in ihrer Datenschutzklausel einräumen. Die Software sieht auch keine Möglichkeit der Umsetzung von Widersprüchen seitens der Nutzer vor.

Bei allen **geprüften Stellen** wurden daher die Datenschutzregeln des TMG missachtet. Der Hinweis, Nutzer könnten durch die Konfiguration des Browsers das Setzen von Cookies – ein für die Erhebung der Nutzungsdaten erforderlicher Schritt – unterbinden und so ihr Widerspruchsrecht umsetzen, ist völlig unzureichend. Die technische Realisierung des Widerspruchs obliegt dem Webseitenbetreiber, der Nutzungsprofile erstellen will. Dieser muss die technische Infrastruktur dafür zur Verfügung stellen. Technisch nicht versierte Nutzerinnen und Nutzer würden ansonsten bei der Wahrnehmung ihres Widerspruchsrechts völlig überfordert.

Ungeklärt blieb bisher, wie mit den erhobenen Nutzerdaten bei Beendigung des Einsatzes der Google-Analytics-Software umgegangen wird. Google sieht derzeit kein Verfahren vor, das die **Löschung der gesammelten Informationen** ermöglicht. Die Internetsuchmaschine räumt sich selbst das Recht ein, nach Deaktivierung des Dienstes durch den Webseitenbetreiber die Daten weiter zu nutzen.

Unzulässig ist außerdem derzeit die Übermittlung der Nutzungsdaten an **Server außerhalb der Europäischen Union**. Als Rechtsgrundlage hierfür käme allenfalls eine Einwilligung durch die Betroffenen infrage, die unseres Wissens nicht eingeholt wird.

Was ist zu tun?
Derzeit ist die Nutzung des kostenlosen Google Analytics Services durch Webseitenanbieter unzulässig. Google muss dessen Konfiguration so ändern, dass die Betroffenen ihr Recht auf Widerspruch, Information und Auskunft sowie Löschung der Daten wirksam wahrnehmen können. Für den rechtswidrigen Einsatz des Dienstes haften die Webseitenbetreiber.

7.3 Google Street View

Die Firma Google bietet auf ihrem Internetportal Google Maps die Möglichkeit an, Standorte nicht nur über eine zweidimensionale Straßenkarte, sondern in Form von Rundumfotos als eingefrorene Straßenszene zu betrachten. Damit werden das Wohnumfeld und das Eigentum von allen Anliegern weltweit elektronisch verfügbar gemacht.

Diese neue Funktion im Portal von Google Maps heißt Google Street View. Im Unterschied zu dem von Google angebotenen Produkt Google Earth besteht hierbei nicht nur die Möglichkeit, von oben aufgenommene Fotos von Straßenzügen und Häusern anzusehen. Bei Street View kann der Nutzer aus der Perspektive eines Autofahrers die einzelnen Häuser sowie die gesamte Nachbarschaft als Videofolge von Bildern in Form einer **360-Grad-Panoramadarstellung** am Computerbildschirm an sich vorbeiziehen lassen.

Das Nützliche und Bequeme – man muss sich nicht bewegen, um einen realistischen und aussagekräftigen Eindruck einer bestimmten Umgebung zu erhalten – kann zur **Verletzung von Persönlichkeitsrechten** der aufgenommenen und der

ansässigen Personen führen. Die Fotofolgen werden nun auch von Häusern und Straßenzügen in Deutschland gemacht. Hierfür fahren Fahrzeuge von Google die Straßen ab. Bei diesen Fahrzeugen sind auf dem Dach Kameras installiert, die während der Fahrt rundum die Umgebung erfassen. Diese Fahrzeuge haben auch Schleswig-Holstein erreicht.

Wo liegt das Problem? Eine Veröffentlichung von personenbezogenen Daten im Internet ist nur mit Einwilligung des Betroffenen zulässig. Soweit auf den Fotos Personen, Autokennzeichen usw. zu sehen sind, müssen diese daher so **unkenntlich gemacht** werden, dass eine Identifizierung nicht mehr möglich ist.

Darüber hinaus handelt es sich bei den mit der Street-View-Funktion einsehbaren Aufnahmen von Grundstücken und Wohnungen um personenbezogene Daten der dort ansässigen Personen, deren Veröffentlichung ohne die Zustimmung der Betroffenen erfolgt. Zwar sind die von der Straße aus erfassten Panoramas zumeist als öffentlich zugänglich anzusehen – jede Person kann eine Straße entlangspazieren und sich die Häuser anschauen –, doch bereits das Abfotografieren kann zum Datenschutzproblem werden, erst recht wenn die erstellten Bilder **mit der Adresse verknüpft** oder verknüpfbar im Internet veröffentlicht werden. Relevant ist zudem, wie genau Häuser und Straßen auf den Bildern erkennbar sind, wie weit man heranzoomen kann, ob es sich um ein einzelnes Bild oder eine Bildfolge handelt.

Bei einer 360-Grad-Panoramadarstellung einer Wohnadresse mit der gesamten zugehörigen Nachbarschaft ist so ein hoher Detaillierungsgrad sowie ein Umfang von persönlichkeitsrelevanten Informationen erreicht, dass **schutzwürdige Interessen der Betroffenen** verletzt sein können. Der Grundstückseigner oder Bewohner hat ein Interesse daran, dass das Umfeld des persönlichen Lebensbereiches bzw. des Eigentums nicht von beliebigen Personen weltweit für beliebige Zwecke auf Knopfdruck zur Kenntnis genommen werden kann. Arbeitgeber können so eine erste Auswahl aus der Bewerberschar danach treffen, wie es bei diesen rund um ihr Zuhause aussieht, wie diese leben, welche Art von Leuten in der Nachbarschaft herumlaufen, wie sauber die Gegend ist. Oder Diebe verschaffen sich einen Eindruck von Wohnlage, erkennbaren Sicherheitsmaßnahmen und der Einstiegsmöglichkeit potenzieller Einbruchsobjekte bequem und unerkannt von zu Hause aus.

Das ULD hatte Google Germany aufgefordert, die Bilderfassung und -veröffentlichung in Bezug auf Schleswig-Holstein zu unterlassen. Google Germany teilte uns darauf im Auftrag der Google Inc. in den USA mit, dass nicht geplant sei, das **Gebiet von Schleswig-Holstein** für den Dienst Google Street View im Jahr 2008 aufzunehmen. Die Planung für 2009 habe noch nicht stattgefunden; es sei unklar, ob Schleswig-Holstein überhaupt Teil der Straßenansicht werden solle. Frühestens im Frühjahr 2009 solle die Erstellung der Aufnahmen wieder aufgenommen werden. In Schleswig-Holstein gesichtete Fahrzeuge wären aus logistischen Gründen unterwegs. Zwischenzeitlich hat sich auch der Schleswig-Holsteinische Landtag des neuen Google-Dienstes angenommen.

Im Düsseldorfer Kreis, dem Zusammenschluss der obersten deutschen Datenschutzaufsichtsbehörden, wurde im November 2008 die Thematik erörtert. Es wurde klargestellt, dass die Veröffentlichungen von **digitalen Straßenansichten** und Bilddaten von Gesichtern, Kraftfahrzeugkennzeichen oder Hausnummern unzulässig sind, wenn keine hinreichende Anonymisierung erfolgt und den betroffenen Bewohnern und Grundstückseigentümern keine ausreichenden effektiven Widerspruchsmöglichkeiten zur Verfügung gestellt werden.

https://www.datenschutzzentrum.de/geodaten/streetview.htm
https://www.datenschutzzentrum.de/geodaten/20081118-dk.html

Was ist zu tun?
Die Anbieter von Straßenansichten im Internet haben die vom Düsseldorfer Kreis festgelegten Anforderungen umzusetzen. Falls auf den Bildern Personen, Autokennzeichen usw. klar zu erkennen sind, sollte dies im Fall von Google unter dem Link „unangemessenes Bild“ mitgeteilt werden.

7.4 Rottenneighbor.com – Nachbarn an den Pranger!

Ein US-amerikanisches Online-Portal zur Bewertung der Nachbarschaft hat Deutschland erreicht. Fast harmlos rühmt sich der Dienst, „die erste flächendeckende Immobiliensuchmaschine“ zu sein, die es ihren Nutzern ermöglicht, bereits vor einem Umzug Informationen über die Nachbarschaft und die Wohngegend einzuholen.

Der Name des Portals – „rotten neighbor“ – lässt sich mit „**verkommene Nachbarn**“ übersetzen. Der Name ist Programm. Die bei dem Dienst vorgenommenen Einträge und Bewertungen kennen in puncto Beleidigung, Diffamierung und Anprangerung keine Grenzen. Über die Eingabe einer Adresse, eines Stadtteils oder einer Postleitzahl wird dem Nutzer im Internet ein Kartenausschnitt auf der Basis von Bildern von Google Maps angezeigt. Dort erscheinen dann rote oder grüne Häuschen, die zum Ausdruck bringen, dass zu bestimmten Adressen negative bzw. positive Nachbarschaftsbewertungen abgegeben wurden. Zudem kann ein Freitextkommentar zur jeweiligen Markierung eingetragen werden. Zu finden sind nicht nur Kommentare zur Einschätzung eines Nachbarn als gut oder schlecht. Viele der virtuellen Aushänge zeichnen sich durch wüste Beschimpfungen, Beleidigungen und Diffamierungen, insbesondere sexueller Natur, aus. Eine Identifizierung der Betroffenen erfolgt oft namentlich; die Adresse wird über die Häuschenmarkierung mitgeliefert.

Darüber hinaus kann der Nutzer ohne kartenbezogenen Zusammenhang in einem Forum seine Nachrichten, Kommentare usw. hinterlassen. Besonders pikant ist die auf der Homepage des Dienstes eigens eingerichtete „**Sex Offenders Search**“. Dabei handelt es sich um eine Suchmaschine, die bei Eingabe einer Adresse, einer Postleitzahl oder eines Stadtteils all jene Adressen mit roten Häusern markiert, in denen angeblich Straftäter von Sexualdelikten wohnhaft sein sollen. Woher diese Informationen stammen, wie diese überprüft werden oder ob eine Einwilligung zur

Veröffentlichung besteht, ist unbekannt und vollkommen intransparent. Jeder Nutzer scheint jede beliebige Person als Sexualstraftäter eintragen zu können.

Der Online-Dienst bietet eine Plattform für anonyme Diffamierungen jeder Art, die offensichtlich nicht kontrolliert werden und für den Betroffenen nicht kontrollierbar sind. Zwar besteht die Möglichkeit, einen Eintrag mit einer „flag of removal", also einer **Markierung zur Löschung**, zu kennzeichnen. Die Markierung garantiert aber nicht die tatsächliche Löschung des Eintrags. Viele Betroffene teilten uns mit, dass die von ihnen gesetzte Löschmarkierung nicht umgesetzt wurde und die Einträge nach wie vor zu finden sind. Zwischenzeitlich nahm das System von schleswig-holsteinischen Betroffenen Markierungen zur Löschung erst gar nicht an.

Zwar werden die Nutzer in den **Nutzungsbedingungen** verpflichtet, keine „unzulässigen" Informationen über die Webseite bereitzustellen. Als unzulässig gelten nach den Nutzungsbedingungen z. B. Anmerkungen oder Kommentare, die andere Personen belästigen und schikanieren, bzw. Anmerkungen, die Drohungen ausdrücken und die rassistisch sind oder mit welchen rechtswidriges Material übermittelt wird. Diese Vorgaben werden aber offensichtlich weder von den Nutzern beachtet noch vom Betreiber kontrolliert. Vielmehr laden die Nutzungsbedingungen ausdrücklich zu anonymen Meldungen ein.

Bereits die Bewertung von Nachbarn als gute oder schlechte Nachbarn wirft umfassende Datenschutzfragen auf: Ist die **Meinungsfreiheit** höher zu gewichten als das Recht auf informationelle Selbstbestimmung der von der Bewertung Betroffenen? Im Gegensatz zu Bewertungsportalen, die sich mit der ausgeübten beruflichen Tätigkeit oder Funktion von Personen auseinandersetzen, z. B. Professoren oder Ärzten, wird der Nachbar in seiner „Funktion" als Privatmensch, d. h. in Bezug auf sein angebliches Verhalten im grundrechtlich geschützten inneren Lebensbereich des Wohnens bewertet. Die Bewertung ist weder objektiv mess- oder feststellbar, noch ist überprüfbar, ob der Bewertende tatsächlich ein Nachbar des Betroffenen ist. Die virtuelle Meinungsäußerung kann weltweit abgerufen werden und der Betroffene hat faktisch keine Möglichkeiten, sich hiergegen schnell und effektiv zu wehren. Nutzungsbedingungen und Konzeption des Portals sehen keinen wirksamen Betroffenenschutz vor. Angesichts der über das Portal stattfindenden Straftaten der Beleidigung und Verleumdung und der erzielten Prangerwirkungen muss die Meinungsäußerungsfreiheit hinter dem Recht auf informationelle Selbstbestimmung zurückstehen. Ein solcher Dienst wäre nach deutschem Recht unzulässig.

Deutsches bzw. europäisches Datenschutzrecht gilt für den deutschen Nutzer, der personenbezogene Daten einstellt und Kommentare abgibt, nicht für den US-amerikanischen Portalbetreiber. Die Einmeldungen erfolgen in der Regel anonym, sodass es schwierig bis unmöglich ist, Urheber von unzulässigen Bewertungen auszumachen und in Deutschland datenschutz-, zivil- oder strafrechtlich **zur Verantwortung zu ziehen**.

Wir haben den **Anbieter in den USA** aufgefordert, uns mitzuteilen, ob er bereit ist, das Land Schleswig-Holstein aus dem Angebot herauszunehmen, da hierbei

gegen deutsches Recht verstoßen wird. Das ULD kann nicht beurteilen, inwieweit der Dienst gegen US-amerikanisches Recht, z. B. zum Datenschutz oder Verbraucherschutz, etwa gegen den Children's Online Privacy Protection Act, verstößt. Daher haben wir das Schreiben nachrichtlich der für die Handelsaufsicht zuständigen Behörde in den USA, der Federal Trade Commission (FTC) in Washington, zukommen lassen mit der Bitte zu prüfen, ob die FTC in Amtshilfe für das ULD als deutsche Aufsichtsbehörde tätig werden kann.

Wir haben bisher weder vom Anbieter noch von der FTC **eine Antwort** erhalten. Anfang des Jahres 2009 fand sich auf der deutschen Seite des Portals ein Aufruf an Unternehmen, die Interesse hätten, das Portal für Deutschland zu übernehmen. Sie seien nur „dumme Amis", so steht es dort, die kein Deutsch sprächen oder die Kultur verständen, um ein „konstraktes qualitaetes Netz" aufzubauen. Wir haben das Auswärtige Amt in Berlin gebeten, in Kooperation mit den US-Behörden Abhilfe zu schaffen. Kurz vor Redaktionsschluss wurde auf der deutschen Seite des Portals nur noch der Vermerk angezeigt: „We're sorry, we are down of maintenance."

https://www.datenschutzzentrum.de/presse/20081119-rottenneighbor-rufmord.htm

Was ist zu tun?
Wir raten dringend davon ab, dieses Portal oder ähnliche Internetangebote zu nutzen, um andere Menschen zu beleidigen, zu diffamieren, zu verfolgen oder negative Bewertungen vorzunehmen. Wird der Urheber des unzulässigen Eintrages bekannt, kann gegen diesen nach deutschem Datenschutz- und Strafrecht vorgegangen werden.

8 Modellprojekte und Studien

8.1 ULD-i – das Innovationszentrum Datenschutz & Datensicherheit

Das Innovationszentrum Datenschutz & Datensicherheit (ULD-i) berät Interessenten bei allen Fragen rund um Datenschutz und Datensicherheit. Die Serviceleistungen des ULD-i werden insbesondere Unternehmen aus der Region angeboten, um die Wirtschaftskraft im Norden zu stärken.

Das ULD-i unterstützt Forscher und Entwickler aus Wirtschaft und Wissenschaft dabei, Datenschutz und Datensicherheit in Produkte und Prozesse zu integrieren. Dadurch soll das **Vertrauen der Verbraucherinnen und Verbraucher** in die Produkte und in deren Anbieter gestärkt werden. Das ULD-i stand auch im letzten Jahr als kompetenter Ansprechpartner den Wirtschaftsunternehmen und Hochschulen zur Verfügung. Im vergangenen Jahr haben unterschiedlichste Projekte mit wirtschaftlicher und wissenschaftlicher Beteiligung Informationen und Know-how im Bereich Datenschutz und Datensicherheit in Anspruch genommen. Das ULD-i platzierte publikumswirksam das Thema Datenschutz auf verschiedenen Messen und Veranstaltungen. Dieselbe Zielsetzung wird auch im Jahr 2009 fortgeführt und weiter ausgebaut.

Was kann das ULD-i für Sie tun?

Nehmen Sie Kontakt mit uns auf:

ULD-i
Holstenstraße 98, 24103 Kiel
Tel.: 0431/988-1399
E-Mail: kontakt@uld-i.de
Homepage: www.uld-i.de/

8.2 Datenschutzdiskurse im „Privacy Open Space“

Die Erfahrungen von Entwicklern, Nutzern und Datenschutzbehörden haben gezeigt, dass die Anforderungen des Datenschutzes innerhalb aller Arten von e-Services bereits im frühen Stadium berücksichtigt, umgesetzt und in Prozesse integriert werden müssen. Ein neues Projekt des ULD – „Privacy Open Space“, kurz „PrivacyOS“ – will dabei helfen, die Sichtweisen der verschiedenen Akteure zusammenzubringen.

Mit PrivacyOS hat das ULD den Zuschlag für ein Projekt im Rahmen des „ICT Policy Support Programme“ der Europäischen Kommission erhalten. Das Projekt führt Vertreter aus den Bereichen **Wirtschaft, Wissenschaft, Regierung und Gesellschaft** zusammen, um die Entwicklung und die Anwendung von Daten-

schutzinfrastrukturen in Europa zu fördern und zu unterstützen. Alle 15 Projektpartner aus 12 europäischen Ländern und das ULD als Koordinator sind mit datenschutzrechtlichen Themen vertraut und können langjährige Erfahrungen in diesem Gebiet aufweisen.

Kern der Arbeit von PrivacyOS ist der Datenschutzdiskurs auf Konferenzen, die nach der sogenannten **Open-Space-Methode** ausgerichtet werden: Die Teilnehmer bringen eigene Themen ein und gestalten dazu Vorträge und Diskussionen. Die Agenda eines Open Space (engl. für „offener Raum“) wird erst zu Beginn der Konferenz erstellt. Jeder kann ein Thema mit datenschutzrechtlichem Bezug einbringen und bekommt in Abhängigkeit des Interesses der anderen Teilnehmer einen Zeitblock und einen Raum zugeordnet. Diese Dynamik ermöglicht es auch, neue und aktuelle Themen zu behandeln.

Innerhalb des Projektes PrivacyOS besteht die Möglichkeit, sich über Best Practices, datenschutzrechtliche Herausforderungen und mögliche Lösungen auszutauschen. Aus diesem Grund werden über einen Zeitraum von zwei Jahren vier Open-Space-Konferenzen **parallel zu Veranstaltungen** mit datenschutzrechtlicher Relevanz organisiert. Auf den PrivacyOS-Konferenzen werden eine Vielzahl von Themen wie etwa Electronic ID-Cards, eParticipation, Datenschutzsiegel oder Kryptomechanismen diskutiert und Anwendungsmöglichkeiten erarbeitet.

Die erste PrivacyOS-Konferenz wurde 2008 in den Räumen des Europäischen Parlaments zeitgleich mit der **30. Internationalen Konferenz der Datenschutzbeauftragten** veranstaltet. Nach dem erfolgreichen Start des Projekts wird das ULD die zweite PrivacyOS-Konferenz vom 1. – 3. April 2009 in Kombination mit der „re:publica“-Tagung in Berlin ausrichten.

www.privacyos.eu/

Was ist zu tun?
Es mangelt oft an einer Möglichkeit zur Vernetzung oder zum Austausch zwischen verschiedenen Bereichen im Datenschutz, insbesondere zwischen Forschungsansätzen, Geschäftsmodellen, zivilgesellschaftlichen Bedürfnissen und staatlichen Anforderungen. Durch PrivacyOS wird ein „Marktplatz“ für den Austausch zwischen allen interessierten Akteuren geschaffen.

8.3 Neue Datenschutzkonzepte im Identitätsmanagement

Das Thema „Identitätsmanagement und Datenschutz“ bleibt relevant bei Industrie, Forschung und ULD. Wieder investiert die Europäische Kommission Fördergelder in Projekte zu diesem Thema, das für die Zukunft unserer Gesellschaft essenziell sein wird.

Nach über vierjähriger Projektlaufzeit fand im Juli 2008 das Projekt **PRIME (Privacy and Identity Management for Europe)** in einer Abschlusskonferenz seinen Höhepunkt. Gemeinsam mit 19 Projektpartnern aus Industrie und Wissenschaft hat das ULD unter Förderung der Europäischen Kommission Konzepte für nutzergesteuertes Identitätsmanagement entwickelt. Die Arbeit von PRIME wurde von der International Association of Privacy Professionals (IAPP) durch Verleihung des „Privacy Innovation Technology Award 2008“, einer Auszeichnung für technische Innovation im Bereich Datenschutz, gewürdigt. Um diese Auszeichnung hatten sich international 15 Organisationen beworben.

In dem im März 2008 begonnenen Nachfolgeprojekt **PrimeLife (Privacy and Identity Management in Europe for Life)** treibt ein leicht verändertes Konsortium nun die Entwicklung, Forschung und Implementierung der Konzepte von PRIME weiter voran. Während PRIME einen Schwerpunkt auf die konzeptionelle Arbeit legte und Lösungen in Form von Prototypen demonstrierte, steht die Entwicklung von Softwarekomponenten für datenschutzförderndes Identitätsmanagement, die unmittelbar zum Einsatz kommen können, im Zentrum der Arbeit von PrimeLife. Diese Lösungen sollen zum Teil zur kostenfreien Benutzung unter freier oder Open-Source-Lizenz zur Verfügung gestellt werden – PRIME live sozusagen.

Daneben widmet sich PrimeLife neuen **technologischen Herausforderungen**, wie sie beispielsweise durch soziale Netzwerke entstehen. Die datenschutzrechtliche Einordnung der Datenverarbeitung in solchen Netzwerken wirft ebenso neue Fragen auf wie die Anforderungen an technisch-organisatorische Schutzmaßnahmen.

In **sozialen Netzwerken** sind es zumeist die Nutzer, die Daten über sich selbst, aber auch über Dritte zur Verfügung stellen. Hier trifft den Nutzer eine besondere Verantwortung, da er über Informationen, Bilder usw., die auch andere Personen betreffen, verfügt. PrimeLife entwickelt Lösungsansätze, um die Nutzer bei der Wahrung dieser Verantwortung zu unterstützen. Schließlich wendet sich PrimeLife der grundlegenden Frage zu, wie Datenschutz

> **?** ***Soziale Netzwerke***
>
> *In sozialen Netzwerken kommunizieren natürliche Personen mit gemeinsamen Interessen, Ideen, Aufgaben oder Zielen in einer virtuellen Gesellschaft über zeitliche, räumliche und organisatorische Grenzen hinweg. Beispiele sind Wikis, Blogs, Chats, Online-Spiele, Plattformen zum Einstellen von privaten oder beruflichen Profilen, Online-Auktionshäuser sowie Webportale zum Austausch von Videos, Fotos und anderen selbst geschaffenen Inhalten.*

während eines **ganzen Menschenlebens** und auch darüber hinaus realisiert werden kann. Moderne Informations- und Kommunikationstechnologien gibt es noch nicht lange genug, als dass die Gesellschaft mit diesen langfristigen Problemen schon umfangreiche Erfahrungen hätte sammeln können. Die wenigsten Techniklösungen haben einen längeren Zeithorizont als 10 Jahre im Blick. PrimeLife will sich auch dieser Frage zuwenden und Umsetzungskonzepte für lebenslangen Datenschutz entwickeln.

 www.primelife.eu/

Was ist zu tun?
Die Konzepte, die im Rahmen des abgeschlossenen PRIME-Projekts erstellt wurden, sollen in Anwendungen umgewandelt und verfügbar gemacht werden. Neue Fragen, wie die der Verantwortung der Nutzer in sozialen Netzwerken und die des lebenslangen Datenschutzes, müssen beantwortet werden.

8.4 Die Zukunft von Identität: Fortschritte im Exzellenznetzwerk FIDIS

Das von der EU geförderte Exzellenznetzwerk FIDIS hat weiter am Thema „Identität" gearbeitet. Wichtige Ergebnisse gibt es zum Identitätsmanagement in öffentlichen Verwaltungen, wozu auch elektronische Identitätsdokumente und Public Key Infrastructures (PKI) gehören.

Wie zuvor lag auch dieses Jahr der Schwerpunkt der Arbeit im Projekt FIDIS bei **verwaltungsnahen Aspekten** des Identitätsmanagements (30. TB, Tz. 8.3). Aus unterschiedlichen fachlichen Perspektiven werden vom ULD grundsätzliche und angewandte Datenschutzanliegen eingebracht.

Die Ergebnisse dieses Projekts fließen zunehmend unmittelbar in die Arbeit der Dienststelle ein, so auch die hier vorgestellten Themen:

? FIDIS

Im Projekt FIDIS (Future of Identity in the Information Society) arbeiten wir mit weiteren 23 Partnern aus 12 Ländern zusammen in einem sogenannten „Network of Excellence". Ergebnisse des Projekts sind europäische Studien, Berichte und Artikel zu verschiedenen Aspekten von Identität, Identifizierung und Identitätsmanagement, die unter www.fidis.net, als Broschüren oder in verschiedenen Zeitschriften publiziert werden.

- **ePass und elektronischer Personalausweis (ePA)**

Während die technische Sicherheit des deutschen ePasses in der 2. Stufe ab November 2007 verbessert werden konnte, ergeben sich mit der Integration der Fingerabdrücke in einem Rohdatenformat (JPEG-Bilder) gesteigerte Datenschutzrisiken. Nach wie vor werden diese Datenschutzrisiken von europäischen Passbehörden unterschätzt. Der neue deutsche elektronische Personalausweis (ePA), für den ein Grobkonzept in der Version 2.0 vorliegt, nutzt wesentliche technische Elemente des ePasses. Das Konzept beinhaltet aber auch Verbesserungen im

Zugriffsschutz für sensible Daten. Aus dem Projekt heraus wurde zur Stellungnahme der Datenschutzbeauftragten des Bundes und der Länder zu diesem Konzept fachlich beigetragen (Tz. 4.1.6).

- **Identitätsmanagement in der öffentlichen Verwaltung**

Derzeit arbeitet eine gemeinsame Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder sowie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) an einer Modernisierung der Sicherheitsleitlinien für elektronische Signaturen und Verwaltungs-PKI. In diese Arbeit fließen Ergebnisse des FIDIS-Projekts, insbesondere Erkenntnisse aus bestehenden PKI-Umsetzungen in europäischen Nachbarländern, ein.

- **Biometrie und Datenschutz**

Eng verknüpft mit dem ePass und dem Konzept für den ePA sind Datenschutzaspekte bei der Nutzung von Biometrie. Basierend auf den Ergebnissen einer aktuellen FIDIS-Studie, haben wir an einem „White Paper“ für Unternehmen zu diesem Thema beim Verein zur Förderung der Vertrauenswürdigkeit von Informations- und Kommunikationstechnik TeleTrusT Deutschland e.V. und an mehreren Publikationen mitgearbeitet. Die Ergebnisse dieser Arbeit wurden auf der CeBIT und drei Konferenzen im In- und Ausland vorgestellt.

Weitere Informationen rund um das Thema Identität und FIDIS-Projektergebnisse sind verfügbar unter:

www.fidis.net/

Was ist zu tun?
Das Exzellenznetzwerk FIDIS bietet interessante und wichtige Ergebnisse zu identitätsbezogenen Themen, die sowohl für die politische Debatte in Deutschland und in Europa als auch für praktische Anwendungen relevant sind. Der Informations- und Erfahrungsaustausch unter allen Interessierten sollte verstärkt werden.

8.5 AN.ON – Anonymität online in den Wirren der Vorratsdatenspeicherung

In Kooperation mit unseren Partnern bietet unser Anonymisierungsdienst AN.ON weiterhin eine Grundversorgung mit Anonymität beim Surfen im Internet. Ob und vor allem wie Anonymisierungsdienste von der Vorratsdatenspeicherung des Telekommunikationsgesetzes erfasst sind, ließ sich auch im Dialog mit der Bundesnetzagentur nicht abschließend klären.

Seit 2001 beschreiben wir in unseren Tätigkeitsberichten (zuletzt 30. TB, Tz. 8.4) die Fortschritte bei „AN.ON – Anonymität online“, einem Anonymisierungsdienst für Webzugriffe. Auch 2008 mussten wir einige **Anfragen der Strafverfolgungsbehörden** nach der Aufschlüsselung von IP-Adressen negativ beantworten. Entsprechend den geltenden gesetzlichen Regelungen durften wir keine derartigen Daten vorhalten.

> ***? Wie nutze ich AN.ON?***
>
> *Zum anonymen Surfen mit dem AN.ON-Dienst installiert man sich ein kleines Programm auf dem Rechner, das die Verbindung zu den Anonymisierungsservern (Mixe) aufbaut. Dieses Programm heißt JAP und läuft auf nahezu allen aktuellen Betriebssystemen. Die Kommunikation erfolgt dann verschlüsselt über die ausgewählte Reihe von verschiedenen Mixen (Kaskade). Zur Auswahl stehen unterschiedliche Mix-Anbieter. Neben dem ULD findet man dort auch z. B. die TU Dresden, die Firma Speedpartner GmbH und andere freie Betreiber. Mit der Firma JonDos GmbH existiert inzwischen auch ein kommerzieller Anbieter. Dessen Mixe sind nur dann nutzbar, wenn man zuvor einen bestimmten Geldbetrag gezahlt hat. Dafür verspricht JonDos auch eine höhere Geschwindigkeit und eine größere Auswahl an Kaskaden. Der ULD-Mix bleibt jedoch als Grundversorgung kostenlos für alle Bürger.*

Inzwischen sind die Regelungen zur **Vorratsdatenspeicherung** in Kraft getreten (ausführlich siehe Tz. 4.3.1). Nach dem Willen des Gesetzgebers müssen ab Januar 2009 auch Anbieter von Telekommunikationsdiensten bestimmte Verkehrsdaten für sechs Monate speichern. Gemäß der Gesetzesbegründung fallen auch Anonymisierungsdienste hierunter. Ob jedoch der AN.ON-Dienst davon betroffen ist, bleibt unserer Ansicht nach weiterhin fraglich: Dieser Anonymisierungsservice definiert sich als Telemediendienst und nicht als Telekommunikationsdienst. Zudem wird er unentgeltlich als Grundversorgung für die Bürger angeboten, damit diese ihre Rechte auf Anonymität im Internet durchsetzen können. Die Regelungen der Vorratsdatenspeicherung zielen – zumindest primär – auf kostenpflichtige Telekommunikationsdienste ab.

Ein Gespräch mit der Bundesnetzagentur in Bonn ergab allerdings, dass man dort die Regelungen der Vorratsdatenspeicherung auch im Fall des AN.ON-Dienstes für anwendbar hält. Unklar bleibt jedoch, **was und wie** genau gespeichert werden soll. So bekamen wir die Auskunft, dass nicht nur die anfallenden IP-Adressen, sondern in weiter Auslegung des Gesetzeswortlautes auch weitere Daten zu speichern seien. Der AN.ON-Dienst arbeitet durch Hintereinanderschaltung mehrerer sogenannter „Mix“-Rechner verschiedener Anbieter. So ist es möglich, dass das System den Nutzer sogar vor den Anbietern selbst schützt, da diese jeweils nur eine

Teilinformation über den Nutzer kennen, mit der allein eine Aufdeckung seiner Ursprungs-IP-Adresse nicht möglich ist. Aber selbst wenn, wie von der Bundesnetzagentur gefordert, Kennungen zur Verknüpfung dieser Informationen gespeichert würden, wäre eine Aufdeckung der Ursprungs-IP-Adresse in der Regel nicht eindeutig möglich, sodass der Nutzen der Vorratsdatenspeicherung zweifelhaft ist.

Unabhängig von der Vorratsdatenspeicherung schützt der AN.ON-Dienst jedoch weiterhin die Anonymität seiner Nutzer **gegenüber den Webseitenanbietern und den Betreibern des Dienstes**; dieser Mehrwert gegenüber Anonymisierungsdiensten, die nur einen Betreiber haben, bleibt bei einer Verpflichtung zur Vorratsdatenspeicherung bestehen.

www.anon-online.de/
www.datenschutzzentrum.de/anon/

Was ist zu tun?
Im Kontakt mit den verantwortlichen Behörden (Bundesnetzagentur, Bundesbeauftragter für den Datenschutz usw.) müssen Antworten auf Fragen zur Anwendbarkeit der Vorratsdatenspeicherung auf Anonymisierungsdienste gefunden werden. Es darf nicht zu einer Stigmatisierung von Nutzern dieser Dienste als potenzielle Straftäter kommen. Unnütze übermäßige Speicherung von personenbezogenen Daten ist zu vermeiden.

8.6 PRISE – Datenschutz für Sicherheitstechnik

Sicherheitsforschung und die Entwicklung von Sicherheits- und Überwachungstechnologien sind traditionelle Forschungsfelder. Aufgrund neu wahrgenommener Bedrohungsszenarien fördert nunmehr auch die Europäische Union umfangreich in diesem Bereich Projekte.

Der technische Fortschritt, den sich auch kriminelle Einzelpersonen und Organisationen zunutze machen, soll mit neuen Mitteln ebenfalls Sicherheitsbehörden zugutekommen. Im Fokus sicherheitsstaatlicher Bemühungen stehen neben dem Schutz einzelner Personen zunehmend auch der Schutz sogenannter kritischer Infrastrukturen vor

? Kritische Infrastrukturen

Als kritische Infrastrukturen werden Institutionen oder Einrichtungen mit hoher Bedeutung für das Allgemeinwesen bezeichnet, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere ernste Folgen eintreten würden.

U. a. werden die Sektoren Transport und Verkehr, Energie, Gefahrenstoffe, Informationstechnik und Telekommunikation und Finanzwesen als kritische Infrastrukturen angesehen.

Anschlägen. Sicherheitsforschung dient außerdem der Entwicklung von Technologien, die bei der **Verhinderung und Aufklärung** von Straftaten eingesetzt werden sollen.

Zumeist zielen Sicherheitstechnologien auf die Auswertung, Aufdeckung und Verhinderung bestimmten – strafbewehrten oder gefährlichen – menschlichen Verhaltens. Der Einsatz solcher Technologien stellt gleichzeitig in der Regel einen **Eingriff in die Grundrechte** der betroffenen Personen dar und hat eine hohe Relevanz für die Persönlichkeitsrechte.

Im Rahmen des EU Forschungsprojekts PRISE (Privacy Enhancing Shaping of Security Research and Technology) haben wir zusammen mit Projektpartnern aus Dänemark, Norwegen und Österreich **Anforderungen an einen Datenschutzmanagementprozess** in der Sicherheitsforschung entwickelt. Auf der Abschlusskonferenz in Wien hat das Projekt prozess- und produktbezogene Kriterien für datenschutzgerechte und datenschutzfördernde Sicherheitstechnologien präsentiert. Zu den Teilnehmern, für die diese Ergebnisse besonders interessant sind, gehörten der Europäische Datenschutzbeauftragte bei der Europäischen Kommission, für Sicherheitsforschung und ethische Evaluierung zuständige Kommissionsmitarbeiter sowie Industrievertreter.

Da insbesondere bei Technologien, die in den Kernbereich der Lebensgestaltung eingreifen, eine automatische Erkennung eines Eingriffs derzeit nicht möglich ist, sind neben technischen und rechtlichen Anforderungen auch **organisatorische Anforderungen** beim Einsatz von Sicherheitstechnologien zu beachten. Durch diese soll sichergestellt werden, dass es nicht zu unzulässigen Datenerhebungen oder -speicherungen kommt. Weitere Informationen zum EU-Projekt PRISE und die Projektergebnisse finden sich unter:

www.prise.oeaw.ac.at/

Was ist zu tun?
Bei der Entwicklung und dem Einsatz von Sicherheitstechnologien sind Möglichkeiten für die Umsetzung von Datensparsamkeit und anderen datenschutzfördernden Ansätzen wie Pseudonymität schon bei Festlegung der Funktionalität der Technologie zu prüfen. Vor dem Einsatz von Technologien ist deren Effektivität im Lichte des erwarteten Rechtsgüterschutzes und den verursachten Grundrechtseingriffen zu bewerten.

8.7 DOS – Datenschutz in Online-Spielen

Der Markt der Online-Spiele gehört zu den Boom-Branchen der Unterhaltungsindustrie. Systeme wie Xbox Live, World of Warcraft oder auch Online-Poker finden viele neue Nutzer. Durch Sammlung von Spielerprofilen, Online-Einbindung von Werbung oder Einsatz von Kameras und Mikrofonen bleiben Daten-, Jugend- und Verbraucherschutz immer wieder auf der Strecke. Der internationale Kontext darf dabei nicht aus den Augen verloren werden.

Das Projekt „Datenschutz in Online-Spielen“ (DOS) wird seit September 2007 vom Bundesministerium für Bildung und Forschung über zwei Jahre gefördert (30. TB, Tz. 8.10). Im Rahmen des Projekts wird erstmalig der Datenschutz bei Online-Spielen **wissenschaftlich analysiert**. Verwandte Aspekte aus Jugendschutz und Verbraucherschutz werden dabei ebenfalls unter die Lupe genommen. Gerade mit Blick auf kommende neue Entwicklungen ist es wichtig, sowohl Herstellern als auch Betreibern aufzuzeigen, welche rechtlichen Regelungen für sie gelten und wie sie die bestehenden Anforderungen konkret umsetzen können. Wie auch in anderen Bereichen der Softwareentwicklung und des Betriebs von Informationstechnik zeigt sich, dass Unachtsamkeit und Unkenntnis in Sachen Datenschutz zu rechtswidrigen Konzepten und Implementierungen führen – zum Schaden der Privatsphäre der Spielerinnen und Spieler.

Im bisherigen Projektverlauf wurden die Sichtweise und die Meinungen der Nutzerinnen und Nutzer von Online-Spielen in einer Umfrage abgefragt, an der mehr als 1.000 Personen teilgenommen haben. Die Nutzersicht fließt ebenso wie die Perspektive der Hersteller und Betreiber in das Projekt ein, um im Projektverlauf praxisnahe Ergebnisse zu erarbeiten. Dazu gehören insbesondere **Anforderungskataloge und Leitfäden** für die Online-Spiele-Branche. Zu diesem Zweck werden die Akteure und andere Interessierte zu insgesamt zwei Workshops eingeladen. Der erste Workshop stieß bereits auf großes Interesse. Durch diverse Vorträge und Veröffentlichungen konnten Teile der Zielgruppen des Projekts für das Thema und die dahinterstehenden Datenschutzrisiken sensibilisiert werden.

www.datenschutzzentrum.de/dos/

Was ist zu tun?
Bei Online-Spielen müssen Datenschutzstandards eingehalten werden. Hersteller und Betreiber von Online-Spielen sind eingeladen, sich in das Projekt einzubringen und zu gleichermaßen rechtlich einwandfreien und praxistauglichen Ergebnissen beizutragen.

8.8 Das Virtuelle Datenschutzbüro festigt seine Position

Seit acht Jahren ist das Virtuelle Datenschutzbüro die erste Anlaufstelle für alle Fragen rund um den Datenschutz im Internet. Die sich wandelnde Zusammensetzung der unterstützenden Projektpartner unterstreicht diesen Prozess und stärkt die Position des Virtuellen Datenschutzbüros als deutschsprachiges Datenschutzportal.

Im Dezember 2000 ging das Virtuelle Datenschutzbüro als europäisches Projekt online. Geplant war ein Datenschutzportal, das sich international als erste Anlaufstelle für Datenschutzfragen etablieren sollte. Die **internationale Zusammensetzung** der Projektpartner, die englisch- und deutschsprachigen Darstellungen und Inhalte sowie die Reservierung internationaler Domain-Namen waren die Basis. Die technische Grundlage hätte sogar Darstellungen in weiteren Sprachen schnell und problemlos ermöglicht. Die weitere Entwicklung sollte von der Nachfrage bestimmt werden.

Um einen Eindruck über die Akzeptanz des Internetangebotes zu erhalten, protokolliert das Virtuelle Datenschutzbüro jedes Jahr kurzzeitig die Seitenzugriffe. Hieraus wird ersichtlich, dass die Anzahl der Besucher stetig zunahm, dass das Interesse an internationalen Inhalten aber eher ein **Schattendasein** führte. Der Aufwand zur Pflege der englischsprachigen Inhalte stand in keinem vertretbaren Verhältnis zum Nutzen.

> **? *Das Virtuelle Datenschutzbüro***
>
> *Das **Virtuelle Datenschutzbüro** ist eine zentrale Anlaufstelle für Datenschutzfragen. In dem Internetportal werden online verfügbare Ressourcen zu rechtlichen und technischen Fragen des Datenschutzes mit Metainformationen systematisch verlinkt. Zudem bietet das Portal Hilfe bei der Suche der zuständigen Anlaufstelle bei konkreten Datenschutzfragen. Das ULD ist geschäftsführender Projektpartner des Virtuellen Datenschutzbüros.*

Zudem machte die Änderung in der **Struktur der Projektpartnergruppe** eine Aufrechterhaltung der internationalen Inhalte immer schwieriger. Die Gruppe der Projektpartner besteht aus unterschiedlichen Datenschutzinstitutionen. Alle deutschen Landesbeauftragten und der Bundesbeauftragte für den Datenschutz sind Mitglieder. Von Beginn an dabei sind der Datenschutzbeauftragte der katholischen Bistümer in Norddeutschland, der Datenschutzbeauftragte der Niederlande (ehemals Registratiekammer, jetzt College Bescherming Persoonsgegevens CBP), der Information and Privacy Commissioner Ontario (Kanada) und der Beauftragte des Schweizer Kantons Zürich. Mit der Zeit kamen die Datenschutzbeauftragten der evangelischen Kirche in Deutschland, des Südwestrundfunks (SWR), des Norddeutschen Rundfunks (NDR), der nationale Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte der Schweiz, das Büro des Generalinspektors für den Schutz personenbezogener Daten in Polen und der Datenschutzbeauftragte der Slowakischen Republik hinzu.

In den letzten zwei Jahren kündigten das College Bescherming Persoonsgegevens Nederland und das Amt zum Schutz von Personendaten der Slowakischen Republik

ihre Projektpartnerschaft. Die entgegengesetzte Entwicklung gab es bei deutschsprachigen Institutionen: Die Datenschutzbeauftragten des Kantons Basel-Landschaft, der Evangelischen Landeskirche Württemberg, des Fürstentums Liechtenstein und des Schweizer Kantons Zug traten dem Virtuellen Datenschutzbüro als neue Partner bei. Der Prozess der **Konzentration auf deutschsprachiges Datenschutzwissen** zeichnet sich somit nicht nur in den veröffentlichten Inhalten ab, sondern wird ebenso in der Projektpartnergemeinschaft deutlich sichtbar.

Diese Umstrukturierung des Virtuellen Datenschutzbüros führt allerdings nicht zur Stagnation. Die sich sammelnde Kompetenz für Datenschutz im deutschsprachigen Raum stärkt die Position als erste Anlaufstelle zu Fragen zum Datenschutz und mittlerweile auch zur Informationsfreiheit. Das Virtuelle Datenschutzbüro ist und bleibt das zentrale Datenschutzportal:

www.datenschutz.de/

Was ist zu tun?
Das Virtuelle Datenschutzbüro wird als zentrales Portal zu aktuellen Datenschutzthemen im Internet weiter ausgebaut, um verfügbare Veröffentlichungen zu bündeln und einen schnellen und gezielten Zugriff auf Informationen zu ermöglichen.

8.9 „Twinning Light“ mit Malta erfolgreich abgeschlossen

Das ULD hatte erneut Gelegenheit, in der Zusammenarbeit mit der Republik Malta zum Aufbau der Datenschutzkultur in einem anderen EU-Staat beizutragen. In einem erfolgreichen Projekt wurde eine Vielzahl von Schulungsveranstaltungen zum Datenschutz durchgeführt.

Das Projekt stellte die zweite Kooperation zwischen dem ULD und den zuständigen Behörden der Republik Malta dar. Während das erste Twinning-Projekt (29. TB, Tz. 11.3) einen allgemeineren Ansatz verfolgte, ging es diesmal ausschließlich darum, **Schulungen** zu unterschiedlichen Bereichen des Datenschutzes für Mitarbeiter der öffentlichen Verwaltung in Malta durchzuführen.

Einziger Projektpartner auf maltesischer Seite war diesmal das **Büro des Premierministers**, vergleichbar mit der Staatskanzlei in einem deutschen Bundesland. Diese Stelle hatte es sich zum Ziel gesetzt, die ohnehin schon gute Qualität des Datenschutzes in der täglichen Arbeit aller Bereiche der maltesischen Verwaltung durch Schulungen weiter zu verbessern. Der Bedarf für diese Schulungen war ein Ergebnis des ersten Projekts. Auf die EU-weite Ausschreibung hatte sich das ULD für die Bundesrepublik Deutschland beworben und den Zuschlag erhalten.

Organisiert durch das ULD wurden innerhalb von sechs Monaten mehr als 50 Schulungstage auf Malta durchgeführt. Datenschutzexperten aus Deutschland und anderen EU-Ländern unterrichteten die Mitarbeiter der maltesischen Behörden zu vielfältigen Themenbereichen und auf unterschiedlichen Schwierigkeitsniveaus, angefangen von Einsteigerkursen, bei denen zunächst Datenschutzbewusstsein geschaffen werden sollte, bis hin zu Expertenworkshops über die besten Methoden bei Datenschutzprüfungen. Insgesamt wurden so mehr als 1.000 Bedienstete der **maltesischen Verwaltung weitergebildet**; durch die Schulung von Multiplikatoren wurde für eine nachhaltige Verankerung des Datenschutzwissens gesorgt. Das Projekt wurde auf maltesischer Seite als eines seiner erfolgreichsten Twinning-Projekte bewertet.

8.10 Datenschutz für Biobanken

Die datenschutzrechtliche Dimension von Biobanken beschäftigte das ULD im Berichtszeitraum gleich in zwei Projekten. Im Ergebnis zeigte sich, dass viele Fragen offen sind und auf nationaler und europäischer Ebene Regelungsbedarf besteht.

8.10.1 bdc\Audit – Auditierung von Biobanken

Biobanken sind Sammlungen von menschlichen Körperproben und daraus extrahiertem, vor allem genetischem Material sowie von dazugehörenden Daten. Im Projekt bdc\Audit ging es um die Entwicklung von Methoden und Kriterien für eine praxisgerechte und zugleich datenschutzfreundliche Biobankforschung (30. TB, Tz. 8.11). Das Projekt ist weitgehend abgeschlossen. In dessen Rahmen organisierte das ULD einen Projektworkshop im Schleswig-Holsteinischen Landtag, wo die wesentlichen Ergebnisse der drei Teilprojekte einer interessierten Fachöffentlichkeit vorgestellt wurden. Eine zentrale Erkenntnis ist, dass es einen **regulatorischen Rahmen** für Biobanken geben muss. Dies ist umso wichtiger, als der Entwurf eines Gendiagnostikgesetzes den Forschungsbereich vollkommen ungeregelt lässt (Tz. 4.6.1).

Das ULD bekam für seine Ergebnisse und Vorschläge positives Feedback. Die Ergebnisse werden im Rahmen der Projektabschlussberichte und durch entsprechende Veröffentlichungen in die **wissenschaftliche Diskussion** eingebracht.

Was ist zu tun?
Geeignete Regelungen für Biobanken müssen in Gesetzesform gebracht werden. Damit würde auch die Motivation zur Durchführung von Audits in diesem Bereich gestärkt werden.

8.10.2 BMB-EUCoop

Das Akronym im Titel steht für die vorgesehene europaweite Kooperation von Biomaterialbanken (BMB). Getragen wurde dieses Projekt von der Telematikplattform für medizinische Forschungsnetze (TMF), deren Aufgabe es ist, als Dachorganisation für die **vernetzte medizinische Forschung** zu fungieren und dabei auftretende Fragestellungen zu beantworten.

Motiviert ist das Projekt durch die Beobachtung, dass sich Netzwerke für medizinische Forschung nicht nur auf nationaler, sondern auch auf europäischer Ebene bilden. Dies gilt auch für die Forschung mit Proben, die in Biobanken gespeichert sind. Beim gegenseitigen **Austausch von Proben oder Daten** ergeben sich komplexe Rechtsfragen. Unter welchen Voraussetzungen ist dies zulässig? Gelten unterschiedliche Anforderungen für Nicht-EU-Mitgliedstaaten oder sogar zwischen EU-Mitgliedstaaten?

Das Projekt BMB-EUCoop untersuchte diese Fragen zunächst für die Konstellation der Weitergabe von Proben und Daten aus Deutschland nach Österreich, Holland, England und in die Schweiz. Dabei wurden Anforderungen und Konsequenzen hinsichtlich der unterschiedlichen berührten Rechtsmaterien dargestellt, namentlich im Hinblick auf das jeweilige ausländische **Eigentums-, Datenschutz- und Persönlichkeitsrecht**. Weiterhin wurden auch die im Zusammenhang stehenden ethischen Fragen analysiert.

Abgeleitet aus diesen Erkenntnissen werden praktische Hinweise zur Vertragsgestaltung erarbeitet, um die nach deutschem Recht gegebene **Rechtsposition der Spender** abzusichern, auch wenn Proben oder Daten ins Ausland gehen sollten. Das ULD hat den umfangreichen Gutachtenteil zu den datenschutzrechtlichen Fragen abgeliefert. Eine zusammenfassende Veröffentlichung aller Gutachten, Empfehlungen und Mustertexte soll 2009 durch die TMF erfolgen.

Was ist zu tun?
Bei der europaweiten Zusammenarbeit zwischen Biobanken muss darauf geachtet werden, dass Rechtspositionen und Standards, die nach deutschem Recht existieren, nicht gefährdet werden. Betreiber von Biobanken sollten sich an die entsprechenden Empfehlungen aus dem Projekt halten.

8.11 RISER (Registry Information Service on European Residents)

Das Leuchtturmprojekt europäische Melderegisterauskunft RISER, der erste E-Government-Dienst für grenzüberschreitende Meldeauskünfte in Europa, setzt nach seinem kommerziellen Start weiterhin auf Datenschutz.

Das seit 2007 laufende Projekt RISERid (Registry Information Service on European Residents Initial Deployment) befindet sich weiterhin erfolgreich in der **Markteinführung**. Ca. 120.000 Adressanfragen bearbeitet RISER monatlich. Die Zielsetzung einer datenschutzfreundlichen Ausgestaltung hat sich von Beginn an

ausgezahlt. RISER verzichtet auf das Sammeln von Adressen für eigene Zwecke, das sogenannte Pooling.

Die jetzt im zweiten Jahr eigenständige RISER ID Services GmbH bietet einen elektronischen Dienst für **europäische Meldeauskünfte** an. Meldeadressen in Deutschland, Estland, Irland, Litauen, Österreich, Schweden, Schweiz und Ungarn können über das Kundenportal zentral angefragt und abgeholt werden. Der Dienst bietet seinen Kunden einen einheitlichen Zugang zu einer sehr heterogenen und unübersichtlichen Melderegisterlandschaft in Europa. Über das Serviceportal können Meldeanfragen als Datei- oder Einzelanfrage über das Internet an die zuständige Meldebehörde weitergeleitet werden. RISER übernimmt die Funktion eines Zustellers. Im Sinne der Auftragsdatenverarbeitung werden die von den RISER-Kunden überlassenen personenbezogenen Daten ausnahmslos zu dem vertraglich festgelegten Zweck und nach den vertraglich festgelegten datenschutzkonformen Verfahren verarbeitet. Auskünfte werden ausschließlich fallbezogen für den jeweiligen Kunden verarbeitet und die Ergebnisse ausschließlich für diesen bereitgehalten. RISER speichert keine Ergebnisse aus Melderegisterauskünften für eigene Zwecke oder macht diese Dritten zugänglich.

Im März 2004 war das von der Europäischen Kommission im Rahmen des eTEN-Programms geförderte **Vorprojekt RISER** gestartet worden. Aus Deutschland sind neben dem ULD das Landeseinwohneramt Berlin und das Fraunhofer-Institut FOKUS beteiligt. Nach dem Start des Pilotbetriebes konnten zunächst Online-Melderegisterauskünfte aus Deutschland und Österreich sowie aus dem Wahlregister in Irland angeboten werden. In einem Anschlussprojekt (RISERac) kamen Ungarn und Estland hinzu. Seit Beginn der dritten Förderphase (RISERid) können auch Melderegisterauskünfte aus Litauen, Schweden und lokalen Registern in der Schweiz über RISER eingeholt werden.

Ein Höhepunkt war auch in diesem Jahr die Veranstaltung der nunmehr **4. Internationalen Konferenz zum Europäischen Meldewesen** im Rathaus Schöneberg in Berlin. Von den insgesamt 155 Teilnehmenden aus 22 Ländern kamen 122 Delegierte aus öffentlichen Verwaltungen, einschließlich deutscher Vertreter des Bundesministeriums des Innern und der Landesbehörden. Querbezüge zur geplanten Einrichtung eines Bundesmelderegisters und zu aktuellen Datenschutzdiskussionen im Meldewesen stießen in den Fachkreisen auf großes Interesse. Das ULD thematisierte als eigenen Programmschwerpunkt die europaweite Durchsetzung des Datenschutzes im Meldewesen sowie den Adresshandel, Transparenz über Herkunft und Verarbeitung von Adressdaten sowie den Schutz von Adressdaten in Deutschland bei Auskunftserteilungen aus europäischen Ländern.

Der Schwerpunkt unserer Projektbegleitung liegt auf der **datenschutzgerechten Ausgestaltung** des Dienstes. Welche Daten dürfen in den nationalen Melderegistern abgefragt werden? Wie sind personenbezogene Daten vor unbefugten Zugriffen zu schützen? Was muss ein Dienst datenschutzrechtlich leisten, wenn er personenbezogene Daten im Auftrag abfragt und weiterleitet?

http://www.riserid.eu/

Was ist zu tun?
Die Berücksichtigung einheitlicher hoher datenschutzrechtlicher Standards muss bei der Ausweitung des Dienstes auf das gesamte Gebiet der Europäischen Union durch eine fachliche Begleitung gewährleistet werden.

8.12 IM Enabled

Instant-Messaging-Dienste liegen im Trend. Will auch eine Behörde online und in Echtzeit mit den Bürgern kommunizieren, sind besondere Anforderungen an den Providerdienst zu stellen. Im Projekt IM Enabled E-Government Services wurden vom ULD die Datenschutzanforderungen erarbeitet.

Das ULD arbeitet im Auftrag der Europäischen Kommission an dem im September 2006 gestarteten Projekt **Instant Messaging Enabled E-Government Services** (IM Enabled) unter der Führung des Waterford Institutes of Technology. Beteiligt sind neben dem ULD Partner aus Irland, Frankreich, Italien und Deutschland. Das Marktevaluierungsprojekt wird im Rahmen des eTEN-Programms von der Europäischen Kommission gefördert.

Welche Behördeninformationen können datenschutzgerecht über Instant Messaging zur Verfügung gestellt werden? Welche Anforderungen sind an Anbieter von Instant-Messaging-Diensten zu stellen, damit der Bürger sicher mit einer Behörde elektronisch kommunizieren kann? Von der öffentlichen Verwaltung genutzte Instant-Messaging-Dienste müssen die Bedingungen erfüllen, die für das Sammeln, Verarbeiten und die Weitergabe von **personenbezogenen Daten im öffentlichen Bereich** generell gemäß den jeweiligen nationalen Datenschutzbestimmungen gelten. Die vom ULD angefertigte Vergleichsstudie zeigt, dass die europäischen Staaten die für den Bereich des Instant Messaging anwendbaren europäischen Direktiven unterschiedlich in nationales Recht überführt haben.

Bei E-Government-Dienstleistungen kommt es zur Verarbeitung personenbezogener Daten. Das Recht in den europäischen Mitgliedsländern sieht dafür technische und organisatorische Schutzmaßnahmen vor. **Herausforderungen** bei der Implementierung von Instant-Messaging-Diensten sind die sichere Verschlüsselung von Daten während der Übertragung sowie die Authentifizierung der Nutzer. Diese Voraussetzungen liegen bei der Nutzung der am Markt vorhandenen Dienste generell nicht vor. Technische Grundvoraussetzung für sicheres Instant Messaging ist der Betrieb eines behördeneigenen Servers.

Das Projekt kommt zu dem Ergebnis, dass IM für die Übermittlung von **sensiblen Daten** nicht geeignet ist. Die Übermittlung der Daten, auch der technischen Nutzerdaten, mittels IM setzt eine spezifische datenschutzgerechte technische Ausgestaltung voraus. Datenschutzkonforme Anwendungen von Instant Messaging im Bereich der öffentlichen Verwaltung sind z. B. zur Kommunikation von Fahrplänen, Verspätungen im ÖPNV oder Theaterprogrammen denkbar.


www.imenabled.eu/

Was ist zu tun?
Die herausgearbeiteten technischen und datenschutzrechtlichen Voraussetzungen müssen bei der Implementierung von Instant-Messaging-Diensten im öffentlichen Bereich entsprechend umgesetzt werden.

8.13 EuroPriSe (European Privacy Seal)

Das europäische Datenschutz-Gütesiegel EuroPriSe startete erfolgreich in die Pilotphase. Das vom ULD geführte Konsortium aus namhaften internationalen Partnern erreichte, dass das neue Siegel auf Anhieb international stark nachgefragt wird.

Die Nutzung und der Kauf von IT-Produkten und -Dienstleistungen setzt beim Verbraucher ein hohes Maß an **Vertrauen** gegenüber Herstellern und Anbietern voraus. Dass dieses Vertrauen nicht immer berechtigt ist, zeigt die große Zahl aufgedeckter Datenskandale. Das **europäische Datenschutz-Gütesiegel** wird nach einer eingehenden Prüfung an IT-Produkte und IT-Dienstleistungen verliehen, die sich in puncto Datenschutz vorbildlich an die Vorgaben der Europäischen Datenschutzrichtlinie halten. Für den Verbraucher bietet das EuroPriSe-Siegel eine transparente und zuverlässige Orientierungshilfe. Unternehmen und Diensteanbieter können mit dem von einer unabhängigen Stelle verliehenen Siegel ihren Kunden effektiv nachweisen, dass ihre Produkte und Dienstleistungen dem europäischen Datenschutzrecht entsprechen und eine faire und rechtskonforme Datenverarbeitung ermöglichen, und so glaubwürdig für mehr Vertrauen werben.

In dem von der **Europäischen Kommission** im Rahmen des eTEN-Programms mit 1,3 Millionen Euro geförderten Projekt EuroPriSe (30. TB, Tz. 9.2) arbeitet das ULD seit Juni 2007 zusammen mit acht Partnern an der Umsetzung des schleswig-holsteinischen Gütesiegels (Tz. 9.3) auf europäischer Ebene. Die Projektlaufzeit konnte von 18 auf 21 Monate verlängert werden. An dem vom ULD geleiteten Projekt sind die Datenschutzbehörde APDCM von Madrid, die nationale französische Datenschutzbehörde CNIL, das Institut für Technikfolgenabschätzung der Österreichischen Akademie der Wissenschaften, das Institut für Menschenrechte der Metropolitan Universität in London, die TÜViT aus Deutschland, VaF aus der Slowakei, Borking Consultancy aus den Niederlanden und Ernst & Young aus Schweden beteiligt.

Die **Qualität eines Gütesiegels** ist abhängig von den zugrunde liegenden Kriterien und der Zuverlässigkeit, Fachkunde und Unabhängigkeit der Prüf- und Zertifizierungsstelle. Im ersten Arbeitspaket des Projekts (30. TB, Tz. 9.2.1) wurde das bewährte Prüf- und Zertifizierungsverfahren des schleswig-holsteinischen Datenschutz-Gütesiegels den europäischen Anforderungen angepasst (Tz. 9.4.1). Zusätzlich zu dem Kriterienkatalog wurde eine Kommentierung mit Hinweisen zum Europäischen Datenschutzrecht erarbeitet. Das ULD nimmt bei EuroPriSe die zentrale Aufgabe der Qualitätssicherung wahr.

Das zweite Arbeitspaket umfasste die **Ausbildung und Zulassung von Gutachtern** im rechtlichen und technischen Bereich. Erfreulich ist die große Anzahl an Experten, die sich für eine Zulassung als EuroPriSe-Gutachter qualifiziert haben. Nachdem der erste Workshop zur Anerkennung von Gutachtern im November 2007 in Wien mit 80 Teilnehmenden aus 13 EU-Ländern schnell ausgebucht war, wurde ein zusätzlicher Workshop im Juni 2008 in Kiel veranstaltet. Auch dieser war schnell ausgebucht und erhöhte die Zahl der anerkannten Gutachter von knapp 40 auf über 60 zum Ende des Jahres 2008. Die wachsende Warteliste zeigt das beständige Interesse von Fachleuten. Neben der Teilnahme am Workshop, der einen Überblick über das Verfahren und eine Einführung in die Bearbeitung und Durchführung von EuroPriSe-Gutachten gibt, ist für die Anerkennung ein **Trainingsgutachten** über ein fiktives IT-Produkt anzufertigen. Die Trainingsgutachten zeigen große Unterschiede hinsichtlich Prüftiefe und Anwendung der Kriterien bei den Gutachtern und machen anschaulich deutlich, dass nur eine Prüfung durch übergeordnete, unabhängige Zertifizierungsstellen ein gleichmäßiges Niveau gewährleisten kann. Die Trainingsgutachten werden unter den am Projekt beteiligten Datenschutzbehörden ausgetauscht und dienen der Überprüfung, ob sie gleiche Anforderungen an die Prüftiefe und Anwendbarkeit der Kriterien stellen. Für das Jahr 2009 sind drei weitere Workshops geplant (Tz. 9.4.3).

Das dritte Arbeitspaket umfasst die Durchführung von **Pilotverfahren** zur Zertifizierung. Innerhalb von nur zwei Monaten meldeten sich 24 Unternehmen aus dem In- und Ausland. An den Start gingen 18 Piloten. Sechs Verfahren konnten mittlerweile erfolgreich abgeschlossen werden (Tz. 9.4.4). Die Hersteller kommen aus den Niederlanden, Luxemburg, Deutschland, Spanien, Schweden und den USA. Seit dem Start der Pilotverfahren haben über 60 Unternehmen aus aller Welt ihr konkretes Interesse an einer Zertifizierung gegenüber dem ULD bekundet. 25 Verfahren befanden sich Ende 2008 in der Evaluierungsphase. Die Pilotverfahren wurden zum Teil gemeinsam mit den Datenschutzbehörden aus Madrid und Frankreich durchgeführt. Wichtig ist der Austausch und eine Abstimmung der Zertifizierungsanforderungen im Hinblick auf die Auslegung der Kriterien, der Plausibilitäts- und Vollständigkeitsprüfung.

Das erste EuroPriSe-Gütesiegel wurde anlässlich des 30. Jubiläums des Schleswig-Holsteinischen Datenschutzgesetzes im Rahmen einer Feierstunde im Schleswig-Holsteinischen Landtag vom Europäischen Datenschutzbeauftragten Peter Hustinx an die Metasuchmaschine Ixquick aus den Niederlanden **verliehen**. Die EU-Kommissarin für Informationsgesellschaft und Medien, Viviane Reding, beglückwünschte in einem Grußwort die Initiative EuroPriSe und den Preisträger, dessen Angebot es den Bürgerinnen und Bürgern erlaube, eine Suchmaschine zu wählen, die ihre Suchdaten nicht langfristig in Protokolldateien speichert. Die Wahrnehmung von EuroPriSe über die Grenzen Europas hinweg sei besonders erfreulich und unterstütze den Wirkkreis der Europäischen Datenschutzrichtlinie.

Ein im November 2008 durchgeführter, an Hersteller und Gutachter gerichteter Workshop bei Ernst & Young in Stockholm brachte ein positives Feedback zum Nutzen des Verfahrens. Die beteiligten Hersteller stellten übereinstimmend fest, dass die **Evaluierungen eingehender** sind als erwartet, sie ihre Produkte bzw. Dienstleistungen im Ergebnis verbessern und auch den Umsatz teilweise erheblich

steigern können. In Stockholm wurden drei weitere EuroPriSe-Siegel verliehen. Dabei wurde vom Europäischen Datenschutzbeauftragten die Unterstützung bekräftigt und eine enge Zusammenarbeit von EuroPriSe mit der Artikel-29-Datenschutzgruppe und den nationalen Datenschutzbehörden in Europa zugesagt.

EuroPriSe wurde **im In- und Ausland vorgestellt**, z. B. im Arbeitskreis Datenschutz Deutscher Unternehmen, bei der Deutschen Gesellschaft für Datenschutz und Datensicherheit, der Zeitschrift Datenschutz und Datensicherheit, der internationalen Konferenz Privacy, Laws & Business in Cambridge, der Internationalen Konferenz der Beauftragten für Datenschutz und die Informationsfreiheit in Straßburg, der Festveranstaltung des European eGovernment Data Protection Awards in Madrid oder der 7th European Congress & Exhibition on ITS (Intelligent Transport Systems). Interessierte Hersteller werden in englischer Sprache über eine Broschüre informiert. Informationen zum Projekt für Bürgerinnen und Bürger, Sachverständige und Hersteller befinden sich auch im Internet in deutscher und englischer Sprache.

www.european-privacy-seal.eu/
www.datenschutzzentrum.de/europrise/

Was ist zu tun?
EuroPriSe ist vom Projekt- in den Wirkbetrieb überzuleiten. Die Zusammenarbeit mit nationalen Datenschutzbehörden, der Artikel-29-Datenschutzgruppe sowie dem Europäischen Datenschutzbeauftragten ist fortzuführen. Für die Markteinführung ist das Siegel noch aktiver international bekannt zu machen.

9 Audit und Gütesiegel

9.1 Bundesauditgesetz – gute Absicht, schlecht gemacht

Die Bundesregierung hat das lang erwartete Bundesauditgesetz in Angriff genommen. Im Dezember 2008 wurde ein vom Bundesinnenministerium erarbeiteter Vorschlag vom Kabinett angenommen. Bis zu praktikablen Regelungen ist es noch ein weiter Weg.

Der Entwurf für das Datenschutzauditgesetz wurde vom Bundeskabinett gemeinsam mit Änderungsvorschlägen zum BDSG beschlossen (Tz. 2.3 und Tz. 5.1.2). So begrüßenswert es ist, dass nunmehr Bewegung in die Gesetzgebung kommt, so **kritikwürdig** ist leider der Entwurf. Das ULD hat sehr ausführlich zum Vorentwurf und zum Beschlussentwurf Stellung bezogen, ohne dass dies von der Bundesregierung in den Kernpunkten berücksichtigt wurde. Dies verwundert, zumal das ULD in Deutschland die einzige Stelle ist, die mit Datenschutz-Gütesiegeln und Auditverfahren in mehr als sieben Jahren umfangreiche und zudem gute Erfahrungen gemacht hat. Trotz mehrfacher Angebote war das ULD nur in geringem Maße in die Gesetzesdiskussion eingebunden.

Unsere Hauptkritikpunkte sind:

- Nach dem Entwurf sollen private Kontrollstellen die Zertifizierung allein vornehmen. Eine **Qualitätssicherung** wie bei Verfahren in Schleswig-Holstein durch eine unabhängige Stelle ist nicht vorgesehen. Dies birgt die Gefahr, dass die privaten Kontrollstellen im Zuge generellen finanziellen Drucks Gefälligkeitsgutachten erstellen.
- Es ist **keine obligatorische Grundprüfung** vorgesehen. Zur Verwendung des Zertifikats genügt vielmehr eine entsprechende Anzeige. Die Kontrolle erfolgt später, eventuell erst mit Verzögerung. Beim schleswig-holsteinischen Verfahren erfolgt die Prüfung vor der Auditverleihung. Nur so kann bei den relevanten Zielgruppen das Vertrauen in das Zertifikat entstehen und bewahrt werden.
- Im Entwurf ist die **Prüfung der Kontrollstellen** nur rudimentär geregelt. Die Rücknahme von Zertifizierungen ist schwierig und aufwendig. Beim Verfahren in Schleswig-Holstein erfolgt schon anlässlich der konkreten Auditierungsverfahren eine qualifizierte Rückmeldung an Gutachter und an die zu auditierende Stelle. Werden Unregelmäßigkeiten bekannt, so können schnell und gestuft die notwendigen Schritte eingeleitet werden.
- Der Entwurf sieht in einem aufwendigen Prozess unter Einbeziehung von dem Datenschutz gegenüber kritisch eingestellten Interessenvertretern die Erarbeitung von Auditkriterien vor. Deren Einhaltung wird nirgends nachvollziehbar dokumentiert und kann daher auch nicht geprüft werden. Die Auditierungen in Schleswig-Holstein werden über Kurzgutachten veröffentlicht und sind dadurch für Beteiligte und Interessierte **transparent und hinterfragbar**.

www.datenschutzzentrum.de/bdsauditg/20081029-stellungnahme-dsag-e.html

Firmen, die das Gütesiegelverfahren in Schleswig-Holstein durchlaufen haben oder dieses näher kennen, haben einhellig zum Ausdruck gebracht, dass vonseiten der Wirtschaft ein Wunsch nach einem starken und aussagekräftigen Siegel besteht. Der Entwurf der Bundesregierung hingegen würde nicht nur einen großen bürokratischen Aufwand mit sich bringen, sondern enthalte nur eine geringe Aussage über die Einhaltung der Datenschutzstandards. Solange diesbezüglich keine wesentliche Nachbesserung des geplanten Audits „mit kleiner Münze“ erfolgt, behält im Interesse der Wirtschaft und eines wirksamen präventiven Datenschutzes das Datenschutz-Gütesiegel „**Certified in Schleswig-Holstein**“ seine Daseinsberechtigung.

Begrüßenswert ist diese Situation nicht. Die Etablierung mehrerer staatlicher Siegel mit ähnlicher Ausrichtung birgt die Gefahr, dass die Unternehmen von Zertifizierungen generell abgehalten werden, und diskreditiert das Instrument des Datenschutz-Audits. Wir geben daher die Hoffnung nicht auf, dass sich aufseiten des Bundes Vernunft breitmacht und gemeinsam ein praktikabler **Weg zu einem wirksamen Bundesaudit** gefunden wird. Der Bedarf ist da.

Was ist zu tun?
Die Erarbeitung eines Bundesauditgesetzes ist konstruktiv zu unterstützen. Auf offensichtliche Fehlentwicklungen muss jedoch nachdrücklich hingewiesen werden.

9.2 Datenschutz-Audits

Auditverfahren sind nichts anderes als Projekte. Werden Projekte gut geführt, verfügen sie über ausreichende Ressourcen, sind alle Entscheider und Interessierten eingebunden und gibt es den Willen, das Projekt zu einem vorzeigbaren Ende zu bringen, dann sind sie auch erfolgreich.

Einige Auditverfahren sind im letzten Berichtszeitraum in Ressourcenengpässe gelaufen. Das ULD setzt in solchen Fällen das eigentliche Auditverfahren aus und geht in die Beratung und Prüfung über. Dies betrifft die Audits in der Kreisverwaltung Segeberg und an der Christian-Albrechts-Universität zu Kiel. Im Folgenden wird beschrieben, welche **Entwicklungen** es im Datenschutzauditbereich gab.

9.2.1 Neue Hinweise zur Durchführung eines Datenschutz-Behördenaudits

In die neuen Hinweise zur Durchführung eines Datenschutz-Behördenaudits sind die Erfahrungen der letzten Jahre eingeflossen. Neu ist das Voraudit, das die Daten verarbeitende Stelle in die Lage versetzt, vor der eigentlichen Begutachtungsphase gemeinsam mit dem ULD die in der Organisation erkannten Schwachstellen zu beseitigen.

Die Hinweise geben interessierten Stellen Informationen über die einzelnen Verfahrensschritte eines Audits. Bei der Überarbeitung wurden besonders die durch das ULD in der Praxis gesammelten Erfahrungen berücksichtigt. Folgende Neuerungen sind von Bedeutung:

- **Abgrenzung des Auditgegenstandes**

Im Rahmen einer Bestandsaufnahme wird der Auditgegenstand von der Daten verarbeitenden Stelle abgegrenzt. Dabei sind folgende Aspekte zu beachten:

- die aufbau- und ablauforganisatorischen Gegebenheiten der Fachabteilungen,
- die eingesetzten IT-Komponenten und -Fachverfahren,
- die Datenverarbeitungs- und Kommunikationswege (Netzplan),
- die Einhaltung der materiellen Zulässigkeitsvoraussetzungen der Datenverarbeitung,
- die festgelegten technischen und organisatorischen Maßnahmen sowie
- die Gewährleistung der Einhaltung der datenschutzrechtlichen und sicherheitstechnischen Vorgaben durch das Datenschutzmanagementsystem.

Bei Verfahren, die sich erst in der Planung oder Entwicklung befinden, können diese Aspekte im Rahmen eines sogenannten **Konzeptaudits** festgelegt werden. Das Konzeptaudit beinhaltet ausschließlich Dokumentationsunterlagen, die den Verfahrensgegenstand in den oben genannten Phasen beschreiben.

- **Voraudit**

In Vorbereitung auf das Datenschutz-Behördenaudit kann die Daten verarbeitende Stelle vom ULD ein Voraudit durchführen lassen. Dabei wird überprüft, ob die Voraussetzungen für das Datenschutz-Behördenaudit von der Daten verarbeitenden Stelle geschaffen wurden. Im Voraudit festgestellte Mängel können gemeinsam mit dem ULD behoben werden. Folgende Schritte werden durchgeführt:

- Abgrenzung des Auditgegenstandes,
- Festlegung der Datenschutzziele,
- Sammlung der zum Auditgegenstand gehörenden Dokumentation,
- Bestandsaufnahme der technischen und organisatorischen Abläufe,
- Erstellung eines Ergebnisberichts mit Projektplan,
- Mängelbeseitigung,
- Einrichtung eines Datenschutzmanagementsystems,
- Erstellung des Datenschutzkonzepts,
- Aufbereitung der für das Datenschutz-Behördenaudit erforderlichen Dokumentation sowie

- abschließende Überprüfung der Erfüllung aller im Voraudit festgelegten und durchzuführenden Aufgaben.

Voraudit und Auditierung werden im ULD **organisatorisch und personell getrennt** behandelt, um die Unabhängigkeit des ULD-Auditors während der Auditierung zu gewährleisten.

- **Begutachtung**

Die vorgelegte Dokumentation für den Auditgegenstand bildet die Grundlage für die Begutachtung vor Ort in der Daten verarbeitenden Stelle durch das ULD. Folgender Ablauf beinhaltet die Begutachtung:

- Überprüfung der Abgrenzung des Auditgegenstandes,
- Analyse der Dokumentation (Datenschutzkonzept),
- Begutachtung der Wirkungsweise des Datenschutzmanagementsystems und der Erreichung der festgelegten Datenschutzziele,
- Hervorhebung von anerkennenswerten und datenschutzfreundlichen Datenverarbeitungsprozessen,
- stichprobenartige Überprüfung der Umsetzung der im Datenschutzkonzept festgelegten Sicherheitsmaßnahmen,
- Überprüfung der Einhaltung datenschutzrechtlicher und bereichsspezifischer Vorschriften in Bezug auf den Auditgegenstand,
- Erstellung eines Gutachtens,
- Verleihung des Datenschutzauditzeichens.

Die Hinweise zur Durchführung eines Datenschutz-Behördenaudits sind im Amtsblatt 2008, S. 1164, Gl.-Nr. 2041.7 sowie im Internet **veröffentlicht**:


www.datenschutzzentrum.de/material/recht/audit.htm

9.2.2 Zahlstellen und InVeKoS-Agrar-Förderprogramm (ZIAF)

Auf Wunsch des Landwirtschaftsministeriums wurde nach der letztjährigen Auditierung der Sicherheitskonzeption des ZIAF-Verfahrens die tatsächliche Umsetzung dieser Konzepte nach dem nationalen Sicherheitsstandard IT-Grundschutz des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) überprüft.

Das „I“ in ZIAF steht für die Abkürzung InVeKoS (Integriertes Verwaltungs- und Kontrollsystem). Mit dem ZIAF-Verfahren zur Agrarförderung werden in Schleswig-Holstein vom Landwirtschaftsministerium (MLUR) finanzielle Fördermaßnahmen verwaltet. Dies geschieht in einer weitverzweigten Infrastruktur auf ca. 350 Arbeitsplätzen in acht verschiedenen Organisationseinheiten an elf Stand-

orten unter Einbeziehung des Dienstleisters Dataport. Dabei werden in unterschiedlichen Förderprogrammen erhebliche Beträge (2006–2007: ca. 2.160 Millionen Euro) ausgezahlt. Die EU hat aus diesem Grund sicherheitstechnische Vorgaben gemacht, um Ausfällen der Informationstechnik und Manipulationen vorzubeugen. Bei der Umsetzung dieser Vorgaben greifen die Bundesländer auf den **Sicherheitsstandard IT-Grundschutz** zurück.

Im Vorjahr waren im MLUR und bei Dataport umfangreiche Sicherheitskonzepte erstellt worden, die sich auf das Management der Informationssicherheit, aber auch die materielle Datensicherheit beziehen (30. TB, Tz. 9.1.3). Die Umsetzung dieser Konzepte werden in einem Auditierungsverfahren gemäß ISO 27001 auf Basis von IT-Grundschutz vom ULD überprüft. Bei dieser Prüfung sind spezifische Vorgaben des BSI zu beachten: Managementaspekte der IT-Sicherheit sind zwingend, einzelne der ca. 5.000 **Sicherheitsmaßnahmen** nach einem Stichprobenprinzip zu überprüfen. Die Prüfung erstreckt sich sowohl auf das MLUR und die beteiligten Organisationseinheiten als auch auf Dataport und hat besonders die Schnittstellen zwischen den Organisationseinheiten zu beleuchten. Gegenwärtig wird der Auditbericht vom BSI überprüft.

> **?** ***ISO 27001: Internationale Norm für das Management von IT-Sicherheit***
>
> *ISO 27001 auf Basis von IT-Grundschutz: Kombination der detaillierten nationalen Vorgaben des IT-Grundschutzes (materielle Sicherheitsmaßnahmen) mit den Vorgaben der Norm ISO 27001 für das Management von IT-Sicherheit.*

Da die Vorgaben der **Datenschutzverordnung** (DSVO) mit dem Standard IT-Grundschutz konform gehen, kann mit der Konformität zu IT-Grundschutz auch die Einhaltung der DSVO nachgewiesen werden.

Um unsere Kompetenzen im Hinblick auf IT-Grundschutz auszubauen, haben sich zwei weitere Mitarbeiter des ULD zu **ISO27001-Auditoren** qualifizieren und vom BSI akkreditieren lassen. Zusammen mit dem BSI und Datenschutzkollegen aus anderen Bundesländern und dem Bund wird an der engen Verzahnung von IT-Sicherheitsmanagement und Datenschutzmanagement im Rahmen des IT-Grundschutzes gearbeitet.

Was ist zu tun?
Das erfolgreich aufgebaute IT-Sicherheitsmanagement im MLUR und bei Dataport muss kontinuierlich weiterentwickelt und angepasst werden, um den künftigen Veränderungen gerecht zu werden.

9.2.3 Ministerium für Bildung und Frauen

Das Ministerium für Bildung und Frauen (MBF) hat sich mit dem Audit seiner IT-Verfahren bei dünner personeller und zeitlicher Ressourcendecke eine große Aufgabe vorgenommen. Die Arbeiten gehen jedoch stetig voran, und die Ergebnisse werden – vor allem bei der Dokumentationssystematik und bei einem neuen (elektronischen) Weg der Berechtigungsdokumentation – voraussichtlich Vorzeigecharakter erlangen.

Die technische und organisatorische Bestandsaufnahme ergab, dass schon viel Dokumentation vorhanden war und Regelungen getroffen wurden. Diese lagen jedoch zum Teil – sowohl elektronisch als auch in Papierform – verstreut vor. Verantwortlichkeiten waren nicht immer eindeutig festgelegt. In einem ersten Schritt musste daher das Ministerium eine **Dokumentationssystematik** festlegen und Verantwortlichkeiten definieren.

Hierzu waren Arbeitsprozesse zu analysieren und zu bewerten sowie Verantwortlichkeiten zu vereinbaren und zu dokumentieren. Es erwies sich als nicht einfach, die zentral vom Finanzministerium zur Verfügung gestellten IT-Komponenten in die eigene Dokumentation zu integrieren. Anschließend musste die übergreifende IT- und Sicherheitskonzeption erstellt werden. Das MBF wählte aufgrund der besseren Übersichtlichkeit und Wartbarkeit der Dokumente einen **modularen Aufbau**.

Hinsichtlich der **Berechtigungsvergabe** entwickelte sich eine lebhafte Diskussion. Bei der Vergabe und Dokumentation der Berechtigungen wurde folgender Ablauf festgelegt:

- Ein Verantwortlicher, z. B. der Leiter eines Referates, erteilt für seine Mitarbeiter Aufträge an die IT, indem er festlegt, welche Berechtigungen ein Mitarbeiter z. B. in der zentralen Datenablage oder in einem Fachverfahren erhalten soll. Dieser Auftrag kann beispielsweise mittels eines Standardlaufzettels oder in einer standardisierten E-Mail erteilt werden.
- Die Administration setzt den Auftrag im IT-System um und gibt eine Rückmeldung an den Auftraggeber, d. h. den Referatsleiter, der das ordnungsgemäße Umsetzen seines Auftrags kontrollieren kann.
- Die durchgeführten Arbeiten – Auftrag, Durchführung und gegebenenfalls Kontrolle – werden elektronisch oder auf Papier so dokumentiert, dass eine Prüfinstanz jederzeit feststellen kann, welche Änderungen wann von welcher Person durchgeführt und von wem beauftragt worden sind und welche Berechtigungen ein einzelnes Benutzerkonto nun effektiv besitzt.

Für das Ministerium war von Anfang an klar, dass sich eine Dokumentation von Hand für diesen Prozess mit den verfügbaren Personalressourcen nicht zufriedenstellend gewährleisten lässt. Zurzeit wird gerade geprüft, inwieweit ein **Ticketsystem zur Berechtigungsdokumentation** eingesetzt werden kann. Diese Lösung hätte den Vorteil, dass

- Berechtigungsvergaben und -änderungen in einem Datenbanksystem erfasst würden,
- daher erkennbar wäre, wer wann welchen Auftrag gegeben hat,
- zu Prüfungszwecken für jedes Benutzerkonto automatisiert eine Berechtigungsabfrage erstellt werden könnte und
- eine zusätzliche Dokumentation der Berechtigungen per Hand entfiele.

Was ist zu tun?
Auch mit knappen Personalressourcen muss das MBF bei diesem Audit am Ball bleiben. Das Ministerium ist auf dem besten Weg zu einer gut strukturierten und transparenten Dokumentation sowie zu einer elektronischen Berechtigungsdokumentation.

9.2.4 Kreis Plön

Nachdem der Kreis Plön sein Kreisnetz durch das ULD hat auditieren lassen, werden nun die Basissysteme für den Betrieb der in der Kreisverwaltung eingesetzten Fachverfahren einem Audit unter Berücksichtigung des Grundschutzstandards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) unterzogen.

Die Kreisverwaltung Plön ist in der kommunalen Verwaltung Schleswig-Holstein weiter Vorreiter in ihrer IT-Sicherheitspolitik (30. TB, Tz. 9.1.6). Als erste Kommunalverwaltung stellt sie sich mit Unterstützung des ULD einer **ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz**. Dieses Zertifikat bietet dem Kreis die Möglichkeit, seine Bemühungen im Bereich der IT-Sicherheit transparent zu machen, was sowohl seinen Kunden, also den nachgeordneten Kommunen, wie den anderen Kreisverwaltungen als Vorbild und den Bürgerinnen und Bürgern als Betroffenen dient.

Bei der Zertifizierung wird neben dem IT-Sicherheitsmanagement die konkrete **Umsetzung von IT-Sicherheitsmaßnahmen** auf der Basis von IT-Grundschutz geprüft. Die Zusammenarbeit mit dem ULD als Prüfinstitution ist bereits weit fortgeschritten. Der sogenannte Basissicherheitscheck ist abgeschlossen, und die Mitarbeiter der IT-Abteilung des Kreises Plön setzen nun die nach dem Grundschutzstandard noch zu bearbeitenden Sicherheitsmaßnahmen um.

Das zur Koordinierung und Überprüfung der Sicherheitsaspekte benötigte IT-Sicherheitsmanagement besteht beim Kreis Plön schon seit längerer Zeit. Insofern hat der Leiter der **IT-Abteilung** frühzeitig die Weichen für die IT-Sicherheitsstrategie richtig gestellt. Hervorzuheben ist, dass das hohe technische Niveau des Rechenzentrums der Kreisverwaltung und der bereitgestellten Dienste auch den nachgeordneten Kommunen zugutekommt. Die IT-Abteilung der Kreisverwaltung Plön nimmt einen Spitzenplatz ein, was Know-how und Professionalität betrifft. Bei der Umsetzung des IT-Grundschutzstandards muss die Kreisverwaltung Plön nach einer festgelegten Methode vorgehen:

Abb.: Grundschutzmethodik / Quelle: www.BSI.de (Webkurs IT-Grundschutz)

Eine IT-Strukturanalyse wurde vollständig durchgeführt. Anschließend wurden der IT-Verbund über die Infrastruktur, die IT-Systeme, Netze und Anwendungen erfasst, der Schutzbedarf festgelegt, die Sicherheitsmaßnahmen bestimmt und umgesetzt sowie eine ergänzende Sicherheitsanalyse durchgeführt. Nach erfolgreichem Abschluss des Verfahrens vergibt das BSI das **ISO 27001-Zertifikat** auf der Basis von IT-Grundschutz und das ULD im Rahmen eines Behördenaudits ein Zertifikat für den datenschutzgerechten Einsatz der Datenverarbeitung an den Landrat des Kreises Plön und seine IT-Abteilung.

Was ist zu tun?
Der von der IT-Abteilung des Kreises Plön eingerichtete IT-Sicherheitsprozess ist dauerhaft auf dem erreichten Niveau zu halten.

9.2.5 Auditverfahren Unfallkasse Nord

Die Unfallkasse Schleswig-Holstein und die Landesunfallkasse Hamburg fusionierten Anfang 2008 zur Unfallkasse Nord. Bei der neuen Unfallkasse Nord wurde eine untere Landesbehörde errichtet, der die Zuständigkeit des staatlichen Arbeitsschutzes zugewiesen wurde. Aus diesen Fusionen ergeben sich zahlreiche Datenschutzfragen. Das ULD wurde mit der Auditierung der Datenverarbeitung der **Versichertendaten sowie der Personalaktenverwaltung** beauftragt. Nach einer kritischen Hinterfragung des Verfahrens zur Einmeldung von Unfällen und der Einbindung der Betroffenen wird hierzu an einer Lösung gearbeitet. Es besteht gute Aussicht, das Audit im ersten Halbjahr 2009 abzuschließen.

Was ist zu tun?
Das Audit bei der Unfallkasse Nord ist erfolgreich zu Ende zu bringen und mit Leben zu füllen.

9.3 Datenschutz-Gütesiegel

9.3.1 Abgeschlossene Gütesiegelverfahren

Zahlreiche Produkte haben vom ULD wieder ein Datenschutz-Gütesiegel erhalten. Zehn Produkte wurden erstmalig zertifiziert, sechs weitere Produkte wurden nach Ablauf der ersten Zertifizierung in einem vereinfachten Verfahren rezertifiziert.

Das **anhaltende Interesse der Hersteller** an Zertifizierungen und Rezertifizierungen zeigt, dass das schleswig-holsteinische Gütesiegel den Herstellern einen echten Wettbewerbsvorteil bietet, der sich lohnt. Erste Hersteller haben von einer Doppelzertifizierung zusammen mit EuroPriSe (Tz. 9.4) Gebrauch gemacht. Auch wenn die Verfahren getrennt durchgeführt werden und unterschiedliche Kriterienkataloge anzuwenden sind, so lassen sich doch merkliche Synergieeffekte nutzen.

Im Einzelnen wurden folgende Produkte **neu zertifiziert**:

- PROSOZ 14plus (Version 5.0.3): softwareunterstützte Bearbeitung der öffentlichen Jugendhilfe in den Bereichen Fallmanagement, Leistungsgewährung und Controlling,
- „wunderloop Integrated Targeting Platform“ in der Anwendung als „wunderloop connect“ und „wunderloop custom“ (Stand: Mai 2008): Verfahren zur gezielten Ansprache von Internetnutzern im Bereich der Online-Werbung auf Basis von deren Nutzerverhalten unter Zwischenschaltung eines Anonymisierungsdienstes,
- FOTOFIX EB digital (Version 1.0): digitale Fotokabine mit integrierter biometrischer Bildbearbeitung zur Nutzung in Meldebehörden,
- PKV-Pseudodatenpool (Version 1.0): Infrastrukturlösung für den gesicherten Austausch von Abrechnungsdaten zwischen Leistungserbringern und Zahlungsstellen im Bereich von Krankenversicherungen,
- TOPqw (Version 4.0.8): Verwaltung von Verträgen zwischen den Sozialämtern/-behörden der Kreise und kreisfreien Städte und den Einrichtungen der Eingliederungshilfe,
- Avan.c (Version 1.0): Internetdienst zur Ermittlung der Rentabilität von medizinischen Einrichtungen,
- digitales Wahlstiftsystem dotVote (Version 1.0): elektronische Abgabe, Speicherung, Bewertung und Auszählung von Stimmen bei Wahlen,

- EUROLabOffice – Fernwartungsverfahren (Stand: November 2008): Fernwartung der Labordiagnostiksoftware EUROLabOffice Version 1.0.8,
- [SPP]: Dienste zur Aktivierung, Lizenzverwaltung und Verhinderung der Umgehung von Sicherheitstechniken im Rahmen von Windows Vista RTM, Windows Vista SP1 und Windows Server 2008 RTM,
- [Fixed IP]: Ermöglichung der IP-basierten Kommunikation zwischen Mobilgeräten über Mobilfunknetze bzw. Kommunikation von stationären Geräten mit einem Mobilgerät über ein Mobilfunknetz auf IP-Basis.

Im **Rezertifizierungsverfahren** wurden folgende Produkte in einem vereinfachten Verfahren (27. TB, Tz. 9.1.4) erneut überprüft und zertifiziert:

- Verfahren der Akten- und Datenträgervernichtung (Stand: Januar 2008): Verfahren zur Vernichtung von Akten und Datenträgern durch die recall Deutschland GmbH (ehemals recall Deutschland GmbH & Co. KG) im Auftrag für öffentliche und nicht öffentliche Stellen,
- SQS-Testsuite für SAP HCM (Version 2.0): Beratungsprodukt zur Qualitätssicherung (Test) von SAP-HCM-Anwendungssystemen in der Praxis,
- Verfahrensregister (Version 2.2): Unterstützung des betrieblichen Datenschutzbeauftragten bei der Erstellung und Verwaltung eines Verfahrensregisters,
- datenschutzkonformes Verfahren zur Vernichtung von Datenträgern aller Art (Stand: September 2008): Vernichtung von Akten, Datenträgern und Mikrofilmen durch die Firma Reisswolf Akten- und Datenvernichtung GmbH & Co. KG, Hamburg, im Auftrag für Auftraggeber aus dem öffentlichen und nicht öffentlichen Bereich,
- Opti.List Professional (Version 7): Archivierung steuerrechtlich relevanter Drucklisten auf Grundlage der Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) sowie der Abgabenordnung,
- Galileo (Version 1.0): klinisches Datenmanagement zur Integration medizinischer IT-Systeme im Krankenhaus und zur Unterstützung des Workflows am klinischen Arbeitsplatz.

Die zahlreichen Datenschutzskandale im Jahr 2008 dürften verstärkt Anlass geben, dass Hersteller nach Lösungen suchen, um Vertrauen bei Verbrauchern und anderen Kunden aufzubauen. Die **auf Qualität ausgerichtete Ausgestaltung** des Gütesiegelverfahrens, bei dem die Gutachten der Sachverständigen von einer unabhängigen staatlichen Stelle auf Plausibilität und Richtigkeit geprüft und dann veröffentlicht werden, wird von allen Beteiligten als wichtig angesehen.

Weitere Informationen für Hersteller befinden sich im Internet unter:

www.datenschutzzentrum.de/guetesiegel/infos_hersteller.htm

Was ist zu tun?
Die Hersteller von Produkten werden weiterhin auf die Vorzüge des Gütesiegels hingewiesen. Dabei findet eine enge Zusammenarbeit mit dem Projekt EuroPriSe statt, um Synergien zu nutzen und Hersteller ziel- und bedarfsgerecht beraten zu können.

9.3.2 Sachverständige

Im vergangenen Jahr konnte das ULD weitere Sachverständige und Prüfstellen für das Gütesiegelverfahren anerkennen.

In den Gütesiegelverfahren erfolgt die Begutachtung der zu zertifizierenden Produkte durch beim ULD anerkannte Datenschutzsachverständige. Wer sich anerkennen lassen möchte, kann dies entweder für den Bereich Recht oder Technik beantragen. Bei entsprechender **Qualifikation** ist eine Doppelzulassung möglich; möglich ist auch die Anerkennung einer ganzen Prüfstelle. Voraussetzungen für eine Anerkennung sind stets neben der Zuverlässigkeit und Unabhängigkeit der Nachweis der erforderlichen Fachkunde. Diese muss sich auf den Datenschutzbereich beziehen.

Hinzugekommen als Sachverständige sind 2008:

- Sachverständiger Michael Bock (Recht und Technik),
- Prüfstelle Mission 100 e.V. (Recht und Technik),
- Sachverständiger Oliver Korth (Recht),
- Prüfstelle Datenschutz cert GmbH (Recht und Technik).

Inzwischen sind beim ULD 31 Einzelsachverständige **registriert**. 14 Sachverständige sind für den Bereich Recht und 11 für den Bereich Technik anerkannt, sechs Sachverständige für beide Bereiche. Hinzu kommen neun Prüfstellen, von denen zwei für Recht, drei für Technik und vier für beide Bereiche bei uns eingetragen sind.

Die Sachverständigen sind verpflichtet, im Abstand von jeweils drei Jahren nach dem Datum der Anerkennung **Nachweise**, vor allem über die Wahrnehmung von Fortbildungen und zum Erfahrungsaustausch, beizubringen. Zahlreiche Sachverständige sind bereits seit mehr als drei Jahren anerkannt und haben die entsprechenden Nachweise vorgelegt.

Im September 2008 fand der jährliche **Gutachterworkshop** in Kiel statt. Von dieser Möglichkeit des Erfahrungsaustausches machten 13 Sachverständige Gebrauch. Diskutiert wurden wieder aktuelle Erfahrungen mit Neu- und Rezertifizierungen, Fragen des Marketings des Gütesiegels wie auch Möglichkeiten der Nationalisierung und Internationalisierung. Ein Schwerpunkt war die Zusammenarbeit mit dem europäischen Gütesiegel EuroPriSe.

Weitere Informationen für Sachverständige befinden sich im Internet unter:

www.datenschutzzentrum.de/guetesiegel/akkreditierung.htm

Was ist zu tun?
Die Sachverständigen sind ein zentraler Baustein und personelle Stütze des Gütesiegelverfahrens. Deren Bestreben, neue Produkte für das Gütesiegelverfahren zu gewinnen, ist daher zu unterstützen.

9.4 EuroPriSe

Das von der Europäischen Union geförderte Projekt des **europäischen Datenschutz-Gütesiegels** – European Privacy Seal (EuroPriSe) – wird in den Wirkbetrieb überführt (Tz. 8.13).

9.4.1 Zertifizierungskriterien

Das europäische Datenschutz-Gütesiegel EuroPriSe 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.

Der EuroPriSe-Kriterienkatalog setzt sich aus vier thematischen Komplexen zusammen: Der erste Komplex befasst sich mit grundlegenden Gesichtspunkten der Funktionsweise des Zertifizierungsgegenstands sowie der Gewährleistung von Datensparsamkeit und Transparenz. Gegenstand des zweiten Komplexes ist die **Rechtmäßigkeit der Datenverarbeitung**. Hier ist insbesondere zu prüfen, ob für die Verarbeitung personenbezogener Daten eine Rechtsgrundlage vorliegt und ob grundsätzliche Prinzipien wie Erforderlichkeit oder Zweckbindung eingehalten werden. Der dritte Komplex betrifft Fragen der Datensicherheit und listet die von der verantwortlichen Stelle zu treffenden technischen und organisatorischen Maßnahmen wie beispielsweise Verschlüsselung oder Verwendung von Passwörtern auf. Der vierte Komplex hat Kriterien zum Inhalt, die die subjektiven Rechte der von der Datenverarbeitung betroffenen Personen betreffen (z. B. Recht auf Auskunft).

Bei der Ableitung der Zertifizierungskriterien wurde nicht nur auf die Vorschriften der EU-Datenschutzrichtlinien zurückgegriffen. Vielmehr wurden auch weitere, diese konkretisierende Quellen wie Rechtsprechung des Europäischen Gerichtshofs (EuGH) und Dokumente der sogenannten **Artikel-29-Datenschutzgruppe**, die sich aus Ver-

? ***Artikel-29-Datenschutzgruppe***

Die Artikel-29-Datenschutzgruppe hat seit 1997 schon mehr als 150 Arbeitsdokumente verabschiedet. Diese können unter

http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs

abgerufen werden.

tretern der nationalen Datenschutzbehörden sowie des Europäischen Datenschutzbeauftragten zusammensetzt, berücksichtigt. Diese Quellen sind bei der Auslegung der Kriterien im konkreten Einzelfall als Hilfsmittel heranzuziehen.

Was ist zu tun?
Der Anforderungskatalog ist kontinuierlich weiterzuentwickeln und an alle wesentlichen Veränderungen und Entwicklungen im Bereich der Gesetzgebung und der Technik anzupassen.

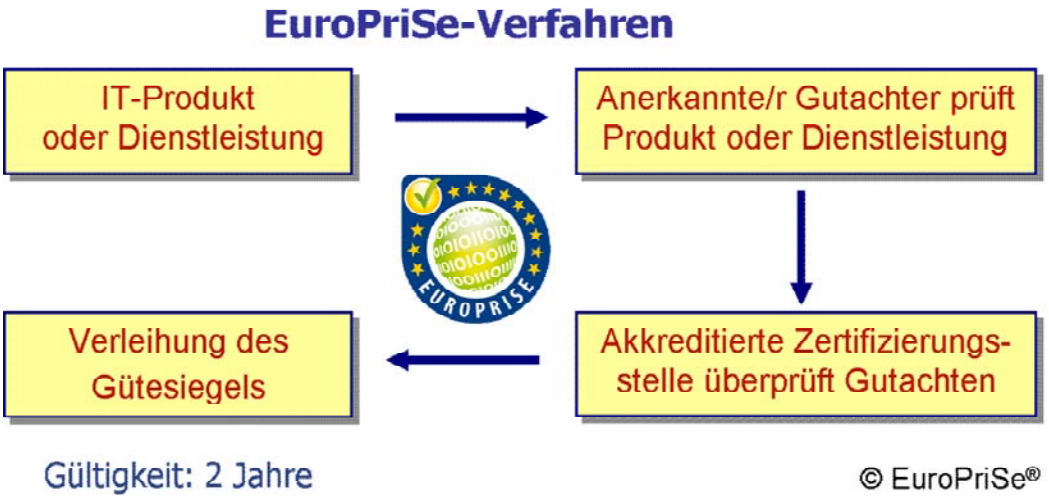
9.4.2 Zertifizierungsverfahren

Voraussetzung für die Auszeichnung eines IT-Produkts oder einer Dienstleistung mit dem EuroPriSe-Zertifikat ist das erfolgreiche Durchlaufen eines qualitätsgesicherten Zertifizierungsverfahrens. Die hohe Qualität dieses Verfahrens wird durch ein Vieraugenprinzip sichergestellt, bei dem die von akkreditierten Sachverständigen verfassten Gutachten von einer kompetenten und unabhängigen Zertifizierungsstelle überprüft werden.

> **?** ***Zertifizierungsgegenstand***
>
> *Der Zertifizierungsgegenstand (engl.: Target of Evaluation – ToE) bestimmt den Umfang des Verfahrens und entscheidet darüber, was genau im Erfolgsfall zertifiziert wird.*

Das Zertifizierungsverfahren beginnt damit, dass ein interessiertes Unternehmen sich mit ihm geeignet erscheinenden, akkreditierten Gutachtern in Verbindung setzt und diese mit der Evaluierung beauftragt. Die **Gutachter** verfassen zunächst eine exakte schriftliche Beschreibung des Zertifizierungsgegenstands, reichen sie bei der Zertifizierungsstelle ein und besprechen die noch offenen Fragestellungen. Sodann erfolgt die Evaluierung des Produkts oder der Dienstleistung durch die Gutachter. Im Anschluss hieran erstellen die Gutachter ein umfassendes Langgutachten und reichen dieses bei der Zertifizierungsstelle ein.

Die **Zertifizierungsstelle prüft** im nächsten Verfahrensabschnitt, ob das Sachverständigengutachten vollständig und nachvollziehbar ist. Bislang gibt es mit dem ULD eine EuroPriSe-Zertifizierungsstelle. Die Einbeziehung weiterer Datenschutzaufsichtsbehörden oder anderer kompetenter und unabhängiger Organisationen als Zertifizierungsstellen ist in Vorbereitung. Identifiziert das ULD inhaltliche Defizite oder Unklarheiten im Gutachten, so informiert es die Gutachter hierüber und fordert sie zur Beantwortung der diesbezüglichen Fragen sowie zur Nachbesserung des Gutachtens auf. Nach Erhalt des Feedbacks seitens der Gutachter prüft das ULD, ob alle offenen Punkte beantwortet worden sind und das Gutachten entsprechend angepasst worden ist. Gegebenenfalls kommuniziert es noch offene Fragen an die Gutachter, welche dann wiederum ihre Antworten beim ULD einreichen.



Sind im Hinblick auf die Gutachten keine Punkte mehr offen und erfüllt das Produkt oder die Dienstleistung alle anwendbaren Zertifizierungskriterien, verleiht die Zertifizierungsstelle das **EuroPriSe-Siegel**. Dies kann auf Wunsch im Rahmen einer öffentlichen Veranstaltung wie etwa einer Messe erfolgen. Um ein Höchstmaß an Transparenz zu gewährleisten, wird eine komprimierte Fassung des Langgutachtens der interessierten Öffentlichkeit auf der EuroPriSe-Website zur Verfügung gestellt. Werden am Zertifizierungsgegenstand keine wesentlichen Änderungen vorgenommen, ist das EuroPriSe-Zertifikat zwei Jahre lang gültig. Nach Ablauf dieser Zeitspanne oder bei wesentlichen Änderungen kann ein vereinfachtes Rezertifizierungsverfahren durchgeführt werden.

9.4.3 Zulassung von Gutachtern

Als EuroPriSe-Gutachter dürfen nur Sachverständige tätig werden, die das strenge EuroPriSe-Akkreditierungsverfahren erfolgreich durchlaufen haben. Während der EuroPriSe-Pilotphase sind über 60 Experten aus zehn verschiedenen EU-Mitgliedstaaten als EuroPriSe-Gutachter zugelassen worden.

Die Evaluierung der zu zertifizierenden IT-Produkte und -Dienstleistungen wird bei EuroPriSe durch akkreditierte Gutachter vorgenommen. Gutachter können für den Bereich Recht und den Bereich Technik akkreditiert werden. Bei einem entsprechenden Maß an **Fachkunde** ist eine Doppelzulassung als rechtlicher und technischer EuroPriSe-Gutachter möglich.

Datenschutzexperten, die als EuroPriSe-Gutachter zugelassen werden wollen, müssen im Rahmen des Akkreditierungsverfahrens neben ihrer Fachkunde auch ihre **Zuverlässigkeit und Unabhängigkeit** nachweisen. Weitere Voraussetzungen für eine Akkreditierung sind die Teilnahme an einem Ausbildungsworkshop für Gutachter und die erfolgreiche Anfertigung eines Trainingsgutachtens zu einem

beim Workshop vorgestellten fiktiven IT-Produkt. Bislang sind im Rahmen von EuroPriSe zwei Ausbildungsworkshops durchgeführt worden, an denen über 100 Datenschutzexperten aus zwölf EU-Mitgliedstaaten teilgenommen haben. Der nächste Workshop wird im Frühjahr 2009 stattfinden.

Insgesamt sind im Jahr 2008 **63 EuroPriSe-Gutachter** akkreditiert worden. 24 Sachverständige haben eine Zulassung als technischer Gutachter erhalten, 34 eine Zulassung als rechtlicher Gutachter. Fünf Datenschutzexperten sind sowohl als rechtlicher als auch als technischer EuroPriSe-Gutachter akkreditiert worden. Die zugelassenen Gutachter verteilen sich auf die folgenden EU-Mitgliedstaaten: Spanien (24), Deutschland (22), Österreich (6), Schweden (3), Kroatien und Niederlande (jeweils 2) sowie Belgien, Frankreich, Großbritannien und Slowakei (jeweils 1 Gutachter).

Eine Liste aller bislang zugelassenen EuroPriSe-Gutachter ist abrufbar unter:


www.european-privacy-seal.eu/experts/pilot-experts/

Was ist zu tun?
Nach der Durchführung der ersten beiden Gutachterworkshops hat eine Vielzahl weiterer Sachverständiger aus verschiedenen EU-Mitgliedstaaten ihr Interesse an einer Zulassung als EuroPriSe-Gutachter bekundet. Deshalb werden 2009 neue Ausbildungsworkshops für Gutachter angeboten werden.

9.4.4 Abgeschlossene EuroPriSe-Verfahren

Im Juli 2008 wurde das erste europäische Datenschutz-Gütesiegel an den Betreiber der Metasuchmaschine Ixquick überreicht. Insgesamt wurden im vergangenen Jahr sechs IT-Produkte bzw. IT-basierte Dienstleistungen mit einem EuroPriSe-Zertifikat ausgezeichnet.

Nachdem die ersten Gutachter akkreditiert waren, konnte ab März 2008 mit den EuroPriSe-Pilotverfahren begonnen werden. Im Januar und Februar 2008 bewarben sich insgesamt 24 Unternehmen um die Teilnahme an den Pilotverfahren. Von den 18 zugelassenen Pilotverfahren wurden bis zum Ende des Jahres sechs Verfahren erfolgreich abgeschlossen.

Im Einzelnen wurden folgende Produkte und Dienstleistungen zertifiziert:

- **Ixquick** (Stand: 28. Januar 2009): Ixquick ist eine Metasuchmaschine, die Suchanfragen von Nutzern an verschiedene Suchmaschinen weiterleitet, die Ergebnisse kombiniert und dem Nutzer bereitstellt, ohne hierbei IP-Adressen zu speichern. Gegenstand der Zertifizierung war die Wortsuche; ausgenommen von der Zertifizierung sind bislang weitere Funktionalitäten von Ixquick wie etwa die Bildersuche.

  
  www.ixquick.com/

- **„wunderloop Integrated Targeting Platform“ (Version 1.13) in der Anwendung als „wunderloop connect“ und „wunderloop custom“**: Verfahren zur gezielten Ansprache von Internetnutzern im Bereich der Online-Werbung („predictive behavioral targeting“). Die Ansprache der Nutzer erfolgt auf der Grundlage ihres Surfverhaltens, welches mit Umfragedaten einer kleinen Zahl zufällig ausgewählter Nutzer kombiniert und mithilfe mathematischer Algorithmen ausgewertet wird.
- **e-pacs Speicherdienst (Version 3.0)**: 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.
- **BGNetPlus** (Stand: 11. November 2008): BGNet Online Banking ist ein Serviceangebot der spanischen Bank Banco Guipuzcoano. Auf der BGNetPlus Online-Plattform werden den Kunden alltägliche Bankdienstleistungen angeboten. Gegenstand der Zertifizierung war das Online-Portal (Webinterface). Nicht von der Zertifizierung umfasst sind die bankinternen Vorgänge zwecks Ausführung der Aufträge des Kunden.
- **DiaDirekt** (Stand: 7. November 2008): Digitalisierungsdienst, der Privat- und Geschäftskunden die Möglichkeit bietet, ihre Fotonegative und Dias in ein digitales Format umwandeln zu lassen. Die digitalisierten Bilder werden auf CD-ROM gebrannt und an den Kunden gesendet. Die Originale werden je nach Wunsch des Kunden entweder an diesen zurückgesendet oder physikalisch zerstört.
- **Microsoft Software Protection Platform – SPP** (Stand: 1. November 2008): SPP ist ein Softwareprodukt, in dem die Dienste Activation, Volume License Management und Security Breach Response für Windows Vista RTM, Windows Vista SP 1 und Windows Server 2008 RTM zusammengefasst sind. Nicht von der Zertifizierung umfasst sind der Echtheitstest im Allgemeinen sowie der Update-Mechanismus.

Die öffentlichen **Kurzgutachten** zu allen verliehenen EuroPriSe-Gütesiegeln sind in englischer Sprache abrufbar unter:

www.european-privacy-seal.eu/awarded-seals/

9.4.5 Laufende EuroPriSe-Verfahren

Die ersten 18 Zertifizierungsverfahren wurden 2008 im Rahmen der EuroPriSe-Pilotphase gestartet. Ein Großteil dieser Verfahren wird im EuroPriSe-Regelbetrieb weitergeführt, einige Verfahren stehen kurz vor dem Abschluss. Zudem ist mit weiteren Zertifizierungsverfahren begonnen worden. Eine Vielzahl von Unternehmen hat ihr Interesse an einer Zertifizierung im Regelbetrieb bekundet.

Von den 18 EuroPriSe-Pilotverfahren aus acht verschiedenen Ländern sind 2008 sechs Verfahren erfolgreich abgeschlossen worden (Tz. 9.4.4). **Elf Pilotverfahren** werden voraussichtlich zum Ende der Pilotphase abgeschlossen oder im Regelbetrieb fortgeführt. Die Zertifizierungsgegenstände entstammen unterschiedlichen Bereichen, etwa dem Gesundheitssektor oder dem Web 2.0.

Neben den Pilotverfahren sind 2008 **weitere Verfahren** gestartet worden, die im Verlauf der ersten Jahreshälfte 2009 abgeschlossen werden sollen.

Was ist zu tun?
Der Bekanntheitsgrad des europäischen Datenschutz-Gütesiegels ist weiter zu steigern. Europäische und internationale Hersteller von IT-Produkten und Anbieter von IT-basierten Dienstleistungen sind auf die Vorzüge des EuroPriSe-Gütesiegels hinzuweisen.

10 Aus dem IT-Labor

10.1 Der mobile Blackberry

Die mobile E-Mail-Lösung „Blackberry“ wird in der Verwaltung verstärkt eingesetzt. Der Hersteller stellt eine umfangreiche Dokumentation bereit und hat ein unabhängiges Gutachten vorgelegt. Aus Sicht des Datenschutzes und der Datensicherheit sind generelle Vorbehalte gegen diese Lösung nicht mehr gerechtfertigt. Gleichzeitig ist klar: Jede Organisation, die diese Lösung einsetzt, muss eigene zusätzliche Sicherheitsmaßnahmen treffen.

Research In Motion (RIM) – eine amerikanische Firma mit Niederlassungen in Europa und Asien – dominiert den Markt für **mobile E-Mail- und Groupware-Lösungen** mit seinem Produkt Blackberry. Blackberry ermöglicht das proaktive Schieben von E-Mails vom Firmen-E-Mail-Server auf das Blackberry-Endgerät per Mobilfunk (Push-Mail). Das häufig teure regelmäßige Abfragen (Polling) des E-Mail-Accounts entfällt. Darüber hinaus können nicht nur E-Mails, sondern z. B. Informationen aus organisationsinternen Systemen – von Kalenderdaten bis zu Datenbankauszügen – auf das mobile Gerät übertragen werden.

So lange wie RIM mit seinen Blackberry-Produkten am Markt ist, gibt es eine immer neue Kritik bezüglich Datensicherheit und Datenschutz. Dies führte nicht selten zu großflächigen Verboten in Landesverwaltungen oder zum Ausstieg großer Firmenkunden. Das ULD wurde häufig um eine Einschätzung gebeten. Wir meinen weiterhin, dass **weder ein generelles Verbot** des Blackberry-Einsatzes **noch eine generelle Freigabe** angemessen sind. In der für den Einsatz in großen Unternehmen oder öffentlichen Verwaltungen bereitgestellten Lösung „Blackberry Enterprise Solution“ wird im internen Netz der jeweiligen Organisation ein Server aufgestellt. Dieser Blackberry Enterprise Server wird so konfiguriert, dass er sich intern mit dem bestehenden Mailserver – z. B. Lotus Notes oder Microsoft Exchange – verbindet. Er leitet neu eintreffende Mails über ein proprietäres, in seinen Grundzügen beschriebenes Protokoll an eine zentrale Vermittlungsstelle weiter. Die Nachrichten werden dabei gemäß RIMs Aussagen so verschlüsselt, dass nur das Zielgerät des Empfängers der Nachricht diese entschlüsseln kann.

Blackberry bündelt nach eigenen Aussagen die Kommunikation zwischen den mobilen Geräte und den Endpunkten in der Infrastruktur des Kunden aus rein wirtschaftlichen Gründen auf wenige Lokationen, die sich derzeit alle außerhalb Deutschlands befinden. Durch diesen „**Flaschenhals**“ werden sämtliche Nachrichten geleitet. Ohne zusätzliche Maßnahmen wäre es RIM möglich, sämtliche Verkehrs- und Inhaltsdaten der Blackberry-Kommunikation einzusehen. Deshalb wird die Kommunikation zwischen dem Blackberry Enterprise Server und dem Endgerät des Nutzers verschlüsselt. RIM fungiert – so die Eigendarstellung – nur als Vermittler und kann keine Kenntnis vom Inhalt der Kommunikation nehmen.

Im November 2008 hat das Fraunhofer-Institut für sichere Informationstechnologie (Fraunhofer-SIT) einen Bericht veröffentlicht, in dem ein Großteil der möglichen Sicherheits- und Datenschutzprobleme beim Blackberry-Einsatz behandelt wird.

Das Fraunhofer SIT bestätigt, dass keine verborgenen Funktionen oder Hintertüren gefunden wurden und weder RIM noch Dritte einen **Zugang zu den Daten innerhalb der Architektur** haben.

Das Restrisiko eines vollständigen **Verlusts der Vertraulichkeit und Integrität** der für die Blackberry-Lösung verfügbaren E-Mail- und Kalenderdaten besteht, wenn z. B. im Blackberry Enterprise Server eine Sicherheitslücke ausgenutzt werden kann. Dieses Restrisiko muss die verantwortliche Organisationsleitung vor dem Einsatz bewerten. Die Bewertung sollte schriftlich festgehalten werden.

Aus dem Bericht des Fraunhofer-Instituts und der von RIM bereitgestellten Dokumentation ergibt sich für die Blackberry-nutzenden Organisationen eine **Liste von Sicherheitsmaßnahmen**, die als Mindestvoraussetzung für einen ordnungsgemäßen Einsatz anzusehen sind. Dazu gehören folgende Punkte:

- Der Blackberry Enterprise Server und einige weitere Komponenten müssen durch eine Firewall von den anderen IT-Systemen der Organisation getrennt werden,
- der Verschlüsselungsalgorithmus muss geeignet gewählt werden (Advanced Encryption Standard, AES),
- spezifische Einstellungen zur Schlüsselverwaltung und -hinterlegung müssen getroffen werden und
- die eingesetzten Komponenten müssen hinreichend aktuell sein (Blackberry Firmware 4.3, Enterprise Server 4.1.6).

Detaillierte Konfigurationshinweise und weitere Maßnahmen finden sich in den unten angegebenen weiterführenden Dokumenten. Das ULD bietet Daten verarbeitenden Stellen in Schleswig-Holstein an, die **korrekte Konfiguration** der eingesetzten Blackberry-Lösung zu überprüfen. Sollten zusätzliche Sicherheitsmaßnahmen notwendig sein, so kann das ULD bei der Konzeption und Umsetzung dieser Maßnahmen beratend und prüfend Hilfestellung geben.

Weiterführende Informationen:

- BlackBerry Enterprise Solution for Microsoft Exchange, Security Analysis, Fraunhofer SIT:
  http://testlab.sit.fraunhofer.de/downloads/certificates/Certification_Report-06-104302.pdf

- Technical Note – Placing the BlackBerry Enterprise Solution in a Segmented Network – Version 4.0 and 4.1:
  http://na.blackberry.com/eng/deliverables/1460/Placing_the_BlackBerry_Enterprise_Solution_in_a_Segmented_Network.pdf

Was ist zu tun?
Organisationen, die eine Blackberry-Lösung einsetzen bzw. einsetzen wollen, müssen die angemessene und wirksame Umsetzung der empfohlenen Sicherheitsmaßnahmen überprüfen und sicherstellen. Ein Einsatz von Blackberry ohne diese Sicherheitsmaßnahmen wird künftig bei Prüfungen des ULD beanstandet werden.

10.2 Virtualisierung

Virtualisieren hilft beim Konsolidieren. Durch Virtualisierung ergeben sich für Datensicherheit und Datenschutz neue Möglichkeiten, um gesetzliche Anforderungen wirtschaftlich und zugleich elegant umzusetzen. Das KomFIT hat hierzu ein richtungsweisendes Grundlagenpapier veröffentlicht.

Seit einigen Jahren ist Virtualisierung ein Thema in der IT-Verwaltung. Da einige Hersteller kostenlose Produkte anbieten, hat so gut wie jeder Administrator schon mit VMware oder Microsoft Betriebssysteme virtualisiert und z. B. in Test- und Freigabeszenarien erfolgreich eingesetzt. Bereits im letzten Jahr hatte das ULD die **Vorteile von Virtualisierung** im Bereich Betriebssysteme und Anwendungen beleuchtet (30. TB, Tz. 10.5). Doch inwieweit lässt sich Anwendungsvirtualisierung im Alltag nutzen?

Dataport hat im Auftrag von KomFIT und unter Beteiligung verschiedener Kommunalverbände, dem Ministerium für Bildung und Frauen sowie dem ULD eine Studie erstellt, die den Bereich Anwendungsvirtualisierung mit Schwerpunkt auf die tatsächliche **Anwendbarkeit auf Fachverfahren** aus dem Bereich der kommunalen Verwaltung behandelt. Dabei werden vor allem die unterschiedlichen Ansätze der Hersteller untersucht und festgestellt, ob die zum Test verwendeten Fachverfahren mit einer virtualisierten Umgebung arbeiten können. Untersucht wurden die aktuellen Produkte der Hersteller Citrix, Microsoft, Thinstall und Landesk. Der Virtualisierungspionier VMware wurde nicht weiter betrachtet, da dieser aktuell nur Produkte listet, um ganze Maschinen und Betriebssysteme zu virtualisieren.

Für die **Tests** wurden das Fachverfahren OK.EWO mit diversen Add-ons sowie Microsoft Word 2003 ausgewählt. Die verschiedenen Hersteller mussten nachweisen, wie viele Schritte nötig sind, um die beiden Produkte zu virtualisieren. Als Nächstes wurde getestet, wie das fertige Paket auf weitere Clients verteilt werden kann, um eine zentrale Softwareverteilung zu gewährleisten. Dabei wurde ebenfalls untersucht, wie sich die virtualisierten Anwendungen im Zusammenhang mit Sicherheitsupdates verhalten und inwieweit die Pakete zu verschiedenen Betriebssystemen und Patchständen kompatibel sind.

Als Fazit legt das fast hundert Seiten starke Konzept keinen Spitzenkandidaten fest. Je nach Infrastruktur und Anwendungsbereich kann sich der Einsatz jedoch lohnen. Durch bessere Datentrennung und Kapselung sowie eine weitestgehende Standardisierung der Pakete lässt sich nicht nur Arbeit sparen, sondern auch die

Datensicherheit und damit auch der **Datenschutz deutlich erhöhen**. Das Konzept Anwendungsvirtualisierung bietet einen guten Überblick und steht den Mitgliedern der kommunalen Landesverbände in Schleswig-Holstein sowie den Dienststellen der Landesverwaltung kostenlos zur Nutzung zur Verfügung.

Was ist zu tun?
Eine Anwendungsvirtualisierung kann viele Probleme lösen und die tägliche Arbeit deutlich vereinfachen, wenn vorher sorgfältig geprüft wird, ob der Hersteller und die Anwendungen richtig zusammenarbeiten.

10.3 Multifunktionsgeräte und Digitalkopierer

Multifunktionsgeräte – also Drucker, Kopierer, Scanner, Fax – haben im modernen Büroalltag Einzug gehalten. Sie sind mit vielfältigen Funktionen und Diensten nicht mehr aus den Arbeitsabläufen wegzudenken.

Zu den Funktionen gehören das Kopieren von Dokumenten in unzähligen Varianten, das Drucken im Netzwerk, das Scannen von Dokumenten mit dem gleichzeitigen Versenden des gescannten Dokuments als E-Mail oder das Versenden von einem Fax direkt vom Arbeitsplatz. Schon die Bedienung der diversen Druckmenüs stellt den Anwender häufig vor eine große Herausforderung. Häufig wird vergessen, dass es sich bei Multifunktionsgeräten um leistungsfähige Server handelt. Das bedeutet, dass nicht nur die reinen Funktionen bedient werden wollen, sondern dass ein **Multifunktionsgerät als Netzwerkgerät** gesehen werden muss.

Es handelt sich um Rechner, die ihre Arbeit im Netzwerk verrichten. Sie sind u. a. mit Prozessor, Arbeitsspeicher, Festplatte, Netzwerkkarte und auch mit einem Betriebssystem ausgerüstet und stellen Dienste für die angeschlossenen Clients (z. B. Arbeitsplatz-PC) zur Verfügung. Aus diesen Gründen sind sie sicherheitstechnisch **als Server zu bewerten**. Dienste werden zur Bereitstellung der vielfältigen Funktionen benötigt und sind in Form von diversen Protokollen im Betriebssystem implementiert.

In Zusammenarbeit mit einer Sicherheitsfirma wurde für eine Fernsehreportage ein professioneller **Penetrationstest** an dem Multifunktionsgerät des ULD durchgeführt. Die Ergebnisse bestätigten die Befürchtungen des ULD. Es war den Angreifern u. a. möglich, die standardmäßig aktivierten Serverdienste anzugreifen, Druckaufträge im Netzwerk abzufangen und zu manipulieren und die Option des vertraulichen Druckens, die den Anwendern das sichere Versenden von Druckaufträgen verspricht, auszuhebeln.

Eine gefährliche Sicherheitslücke stellt auch das **Masteradministratorpasswort** dar. Mit seiner Hilfe können sich Servicetechniker ohne Kenntnis des „normalen“, dem Kunden bekannten Administratorkennwort am Gerät anmelden und sogar das vom Kunden vergebene Administratorpasswort zurücksetzen. Erhält ein Angreifer Zugriff auf das Masteradministratorpasswort, dann kann er das Gerät komplett „übernehmen“. Wie einfach das geht, demonstrierten die Penetrationsprofis: Kein

aufwendiges Sniffen und Knacken von Passwörtern, eine einfache Recherche im Internet genügte zur Beschaffung des Passworts im Klartext.

Das ULD hat eine Informationsschrift mit den **Ergebnissen des Penetrationstests** erarbeitet. Wegen der großen Vielfalt von Gerätetypen und Herstellern ist es unmöglich, eine vollständige Liste der Maßnahmen zur Absicherung von Multifunktionsgeräten bereitzustellen. Folgende allgemeine Hinweise zu Sicherheitsmaßnahmen sollten jedenfalls bei der Planung, Konfiguration und Dokumentation berücksichtigt werden. Ausführlichere Informationen finden sich auf der ULD-Webseite.

- Erstellen Sie vor der Anschaffung eines Multifunktionsgerätes eine Anforderungsanalyse. Berücksichtigen Sie die administrativen Konfigurationsmöglichkeiten.
- Machen Sie sich Gedanken darüber, wie Sie das Multifunktionsgerät an Ihr Netzwerk anschließen möchten. Sichern Sie gegebenenfalls den Netzwerkanschluss ab.
- Bedenken Sie, dass Sie alle Daten auf der Festplatte des Multifunktionsgerätes speichern können. Sie sollten die Möglichkeit zur Verschlüsselung der Festplatte überprüfen (Einsatz eines „Security-Kits“).
- Klären Sie, welche Dienste das Multifunktionsgerät zur Verfügung stellt und welche Protokolle implementiert sind. Sind diese abschaltbar?
- Achten Sie darauf, dass Sie das standardmäßige Administratorpasswort ändern. Denken Sie daran, dass zusätzlich ein Masterpasswort für Techniker existiert.
- Achten Sie beim Einsatz von Boxen, also Speicherbereichen für Dateien, auf Datensparsamkeit. Legen Sie Löschintervalle fest.
- Überprüfen Sie die Notwendigkeit, das Multifunktionsgerät über ein Webinterface zu administrieren. Mit diesem Web-Frontend öffnen Sie auch anderen Benutzern vielfältige Funktionen.
- Achten Sie bei einem Einsatz des Multifunktionsgerätes in einem öffentlich zugänglichen Bereich darauf, dass es ein zeitverzögertes Drucken nach PIN-Eingabe unterstützt.
- Achten Sie auch auf konventionelle Sicherheitsmaßnahmen. Stellen Sie einen Schredder neben das Multifunktionsgerät.
- Regeln Sie in einer Dienstanweisung den Umgang mit dem Multifunktionsgerät.
- Dokumentieren Sie alle Einstellungen in einer Systemakte.
- Definieren und dokumentieren Sie einen Prozess für Wartungen und Reparaturen, u. a. zur Beaufsichtigung des Servicetechnikers.

http://www.datenschutzzentrum.de/kopierer

Was ist zu tun?
Multifunktionsgeräte müssen – genau wie Server – sorgfältig geplant, installiert, konfiguriert, implementiert, gewartet und dokumentiert werden. Es sollte besonders darauf geachtet werden, dass sich ein Multifunktionsgerät in die bestehende Sicherheitskonzeption des Netzes einfügt und nicht zu einem Sicherheitsrisiko wird.

10.4 Systeme ohne Herstellersupport

Alles ist vergänglich. Dies gilt besonders für die schnelllebige Informations- und Kommunikationstechnologie. Wie lange können veraltete Geräte und Programme eingesetzt werden?

Betriebssysteme und Programme haben eine bestimmte Lebensdauer. Innerhalb dieser Zeit veröffentlicht der Hersteller typischerweise Updates, welche kleinere Fehler beseitigen. Entscheidend sind die Updates, die kritische Sicherheitslücken schließen und somit die Sicherheit und Integrität gewährleisten. Wir haben in mehreren Prüfungen festgestellt, dass oft noch Software im Einsatz ist, die nicht mehr vom Hersteller mit Sicherheitsupdates unterstützt wird. Die Daten verarbeitenden Stellen gehen mit dem Einsatz solch **veralteter Programme** erhebliche Risiken ein, da kritische Lücken nicht mehr geschlossen werden.

Am Beispiel der Betriebssysteme der Firma Microsoft lässt sich dies sehr gut darstellen. Microsoft Windows 98 wurde offiziell bis Ende Juni 2006 unterstützt. Wir finden in einzelnen Fällen immer noch vor allem tragbare Geräte mit diesem Betriebssystem. Ähnlich sieht es mit dem Betriebssystem Windows NT in der Version 4.0 aus. Microsoft hat bereits Ende Juni 2004 die Auslieferung von wichtigen Sicherheitsupdates eingestellt. Damit sind die Betriebssysteme teilweise seit über vier Jahren nahezu ungeschützt gegen aktuelle Angriffe und Bedrohungen. Ein Einsatz dieser Systeme in vernetzten IuK-Umgebungen entspricht nicht dem Stand der Technik und ist in vielen Bereichen als grob fahrlässig anzusehen. Das ULD konnte im Test mit gängigen Hackertools die Systeme mit Windows NT oder Windows 98 **innerhalb weniger Sekunden kompromittieren** und manipulieren.

Organisationen, die Windows 2000 einsetzen, befinden sich bereits seit Ende Juni 2005 nicht mehr im vollen **Support durch Microsoft**. Updates und Patches werden noch ausgeliefert, solange das aktuelle Service Pack installiert ist. Microsoft wird den sogenannten „Extended Support“ mit der Auslieferung von kritischen Sicherheitsupdates für Windows 2000 im Juli 2010 einstellen. Spätestens dann ist ein Einsatz von Windows 2000 in vielen Szenarien nicht mehr mit den datenschutzrechtlichen Vorgaben vereinbar. Für die Server Version 2003 werden Sicherheitsupdates bis 2015 und für XP noch bis 2014 entwickelt.

Was ist zu tun?
Veraltete, vom Hersteller nicht oder nur noch unzureichend unterstützte Software darf nicht zur Verarbeitung personenbezogener Daten eingesetzt werden. Ein Einsatz verstößt gegen die datenschutzrechtlichen Bestimmungen und wird vom ULD im Rahmen von Kontrollen beanstandet.

10.5 Google Chrome

Die meisten Internetnutzer waren überrascht: Google, ursprünglich als Anbieter einer Suchmaschine gestartet, veröffentlicht einen eigenen Browser. Programme zur Anzeige von Internetseiten gibt es inzwischen von verschiedenen Anbietern. Neben Microsoft mischt auch Apple im Browsermarkt mit, und die Open-Source-Szene hat mit Firefox eines der populärsten Internetprogramme im Portfolio. Warum nun also ein Browser von Google?

Unter Datenschutzgesichtspunkten ist Google Chrome in mehrfacher Hinsicht auffällig. Es findet eine im Vergleich zu anderen Browsern überaus **rege Kommunikation mit Google-Servern** statt. Chrome sendet jede Eingabe in der Adressleiste in Echtzeit an Google. Auf diese Weise verschmilzt Google die klassische Adressleiste, in der Webadressen eingegeben werden, mit der Suchleiste, die Anfragen an eine Suchmaschine entgegennimmt. In Chrome gibt es nur eine Zeile für Eingaben, die jedes Mal gleichsam als Suchanfrage behandelt werden. So landen nicht nur Suchanfragen, sondern alle aufgerufenen Webseiten bei Google, die der Nutzer ganz ohne Hilfe der Suchmaschine besucht hat.

Bei der Installation pflanzt Google einen **Globally Unique Identifier** (GUID) ins Nutzerkonto des Anwenders, eine weltweit eindeutige Identifikationsnummer. Ein Google Updater sucht fortan nach der Anmeldung am Rechner nach Aktualisierungen für Chrome. Dabei wird besagte Identifikationsnummer an Google übermittelt. Das führt dazu, dass ein Computer unabhängig von IP-Adresse oder vorhandenen Cookies jederzeit für Google wiedererkennbar ist, da die jeweils aktuelle IP-Adresse umgehend bei Google mit der GUID verknüpft werden kann. So ist es technisch möglich, jede Suchanfrage und jede Aktivität eines Nutzers im Einflussbereich von Google über lange Zeit miteinander zu verknüpfen. Das Vorhandensein einer GUID ist speziell bei Google-Produkten keine Neuheit. Auch andere Anwendungen aus dem Hause, z. B. Google Desktop oder Google Toolbar, markieren den Wirtsrechner mit einer weltweit eindeutigen Nummer. Über die Notwendigkeit einer solchen Markierung kann man streiten. Warum die ID im System verbleibt, selbst wenn man Chrome deinstalliert, lässt sich technisch kaum begründen – ebenso wenig wie der Umstand, dass der Updater weiterhin nach Updates sucht (und dabei seine Nummer übermittelt), obwohl der Browser längst entfernt wurde.

Die denkbaren **Gefahren**, die von Chrome für die Privatsphäre der Nutzer ausgehen, sind immens: Theoretisch können alle Suchanfragen seit der Installation von Chrome einem einzelnen Nutzer zugeordnet werden. Entsprechendes gilt für Aufrufe von Diensten wie Google Maps oder YouTube. Ob eine derartige Korre-

lation von Daten von Google durchgeführt wird, lässt sich nicht nachprüfen. Google sollte den Einsatz regelmäßig übertragener GUIDs gründlich überdenken. In Anbetracht der Informationsmenge, über die Google verfügt, sind derlei Identifikatoren schlicht inakzeptabel.

Was ist zu tun?
Der Einsatz von Google Chrome ist derzeit nicht zu empfehlen. Wer sich ein Bild von der Software machen möchte, sollte die portable Version „Portable Chrome" verwenden oder die um datenschutzfeindliche Aspekte beschnittene Chrome-Variante „Iron".

10.6 „Ich weiß, was du gestern gelesen hast!"

Google bietet Zugriffsstatistiken für die eigene Webseite – umfassend, leicht zu implementieren und natürlich gratis. Google Analytics wäre nicht Google, befänden sich nicht handfeste Datenschutzprobleme im Gepäck.

Google Analytics bietet Webseitenbetreibern eine einfache Möglichkeit, **Aufschluss über ihre Besucher** zu erhalten. In umfangreichen Analysen schlüsselt der Dienst neben besuchten Webseiten und Verweildauer auch den vermuteten Wohnort der Besucher auf. Standards wie der eingesetzte Browser, Hostnamen- oder Refereranalyse sind selbstverständlich.

Zum Erheben dieser Daten setzt Google keine Drittanbieter-Cookies ein, wie dies klassischerweise von Analysediensten mithilfe von Blindpixeln getan wird, sondern verwendet **JavaScript-Programme**. Diese baut der Webmaster auf den einzelnen Unterseiten des eigenen Webangebots ein. Der JavaScript-Code wird dann bei der Anzeige der Webseite im Browser des Besuchers ausgeführt und lädt weiteren Code vom Google-Server nach. Durch diesen Kunstgriff kann Google einen Cookie unter der Flagge des aufgerufenen Webservers setzen. Das JavaScript übermittelt die Ergebnisse der Analyse sowie die im Cookie enthaltenen Informationen im Zuge eines klassischen Grafikaufrufs an den Google-Server. Das Ganze bildet somit Drittanbieter-Cookies nach, ohne solche wirklich einzusetzen.

Die wenigsten Internetnutzer sind sich bewusst, dass ihr Surfverhalten beim Besuch von von Analytics unterstützten Webseiten aufgezeichnet und **in die USA übermittelt** wird. Google selbst fordert eigentlich einen prominenten Hinweis auf den Einsatz seiner Analysetechnik. Die Webmaster allerdings scheuen sich vor derlei Informationen und verstecken die Hinweise – wenn sie überhaupt auf ihrer Seite zu finden sind – am liebsten ganz am Ende einer klein gedruckten Datenschutzerklärung. Die Analyse des Nutzerverhaltens auf Webseiten im Internet ist beileibe nichts Neues. Bei Google kommt aber ein erstaunliches Potenzial dazu, nämlich das Nutzerverhalten mit sämtlichen anderen Informationen zu verschneiden, die Google besitzt.

Aus **Sicht des Webseitenbetreibers** stellt sich Google Analytics recht einfach dar: Nutzerdaten des eigenen Webangebots werden zu Google gegeben, eine Auswertung kommt zurück. Das ist im Kern nicht mehr, als eine lokale Analyse mit Statistikprogrammen leisten würde, dafür aber komfortabler. Bei Google laufen zudem die Daten aller Analytics-Kunden auf; eine Verknüpfung der Aktivitäten desselben Nutzers auf verschiedenen Webseiten ist möglich. Nicht zuletzt durch die GUID, die bei jedem Rechnerstart die aktuelle IP-Adresse an Google übermittelt, ist eine Zusammenführung der Analytics-Daten mit jedem anderen genutzten Google-Dienst denkbar. So könnten Suchanfragen, Landkartenaufrufe und Chats, Fotos, Dokumente und das Surfverhalten miteinander verschnitten werden. Der Webseitenbetreiber hat kaum Einflussmöglichkeiten auf die bei Google gespeicherten Logdateien seines Servers. Er kann diese nur komplett löschen lassen, indem er sein Profil bei Google löscht. Einzelne Informationen zu löschen ist nicht möglich. Ebenso kann der Betreiber keinen Einblick in die bei Google gespeicherten Rohdaten nehmen, die Einsicht ist stets auf die fertigen Aggregate beschränkt. Google selbst weist die Vorstellung von sich, Korrelationen zwischen den verschiedenen Daten der einzelnen Dienste herzustellen.

Auf **Nutzerseite** lassen sich Tracking-Dienste wie Google Analytics durch kleinere Eingriffe in die Einstellungen des eigenen Browsers ausschalten. Internetnutzer können sich auf der ULD-Webseite über entsprechende Gegenmaßnahmen informieren.

http://www.datenschutzzentrum.de/tracking/

Was ist zu tun?
Webseitenbetreiber sollten überlegen, ob eine lokale Analyse der eigenen Logdaten mithilfe von Statistikprogrammen ausreichende Ergebnisse liefert. In diesem Falle sollten die Logdaten spätestens nach 24 Stunden ohne Beibehaltung von IP-Adressen aggregiert werden. Die Rohdaten mit IP-Adressen müssen spätestens nach 24 Stunden gelöscht werden. Muss auf externe Dienstleister zurückgegriffen werden, so ist zu beachten, dass kein Datentransfer ins außereuropäische Ausland stattfindet. Webseitenbesucher sind deutlich über die Verwendung externer Dienstleister aufzuklären.

10.7 Personal Firewalls

Personal Firewalls galten lange als Maß der Dinge für die Absicherung eines einzelnen PCs im Internet. Doch wogegen schützen sie wirklich?

Die Idee ist eigentlich einfach: Eine Software auf dem eigenen Rechner überprüft eingehenden wie ausgehenden Datenverkehr und informiert den Nutzer über unbefugte Zugriffe bzw. blockiert diese selbsttätig. **Konventionelle Firewalls** arbeiten als eigenständiges Gerät, das zwischen PC und Netzwerkübergang geschaltet wird. Solche Firewalls können bei ausgehendem Datenverkehr naturgemäß nicht entscheiden, ob dieser legitim ist – schließlich haben sie keine Kenntnis über die auf dem Computer gerade laufenden Anwendungen.

Personal Firewalls sollen diese Lücke schließen, da sie theoretisch alle auf dem Rechner laufenden Prozesse kennen und so bei ausgehenden Datenpaketen die Spreu vom Weizen trennen können. Praktisch hat das Konzept allerdings Schwächen. Das größte Problem stellt die halb automatische Analyse des Datenverkehrs dar. Personal Firewalls können nicht von sich aus erkennen, ob eine spezifische Datenübertragung legitim ist. Daher wird der Nutzer aufgefordert, für eine bestimmte Verbindung eine Entscheidung zu treffen. Die Firewall zeigt dazu bestimmte Informationen wie Quellport, Zieladresse, auslösenden Prozess und verwendete Protokolle an. Der Nutzer muss auf Basis dieser Informationen einstufen, ob er die aktuelle Verbindung genehmigen oder blockieren möchte. Diese Aufgabe ist jedoch selbst mit einiger Fachkenntnis nicht immer zweifelsfrei zu bewältigen. Einerseits suchen viele Anwendungen mit eigenen Prozessen nach Aktualisierungen, andererseits geben sich Schädlinge möglichst unauffällige Programmnamen, um gerade solche Firewallabfragen zu passieren.

Hinzu kommen diverse Möglichkeiten, Informationen an Personal Firewalls vorbeizuschmuggeln. Die einfachste besteht darin, den Browserprozess zu benutzen, um im Schlepptau einer von der Firewall akzeptierten Verbindung Daten nach außen zu transportieren. Die eigentliche Stärke des Konzepts, nämlich die laufenden Anwendungen und damit Ursprünge von Datenpaketen sehen zu können, erweist sich so insgesamt als größte Schwäche. Da die Personal Firewall naturgemäß auf dem zu überwachenden System laufen muss, ist sie automatisch betroffen, wenn dieses System kompromittiert wird. Ein Schädling, der das Betriebssystem befallen hat, wird unter Umständen zuerst versuchen, die Personal Firewall zu beenden oder zu manipulieren. Der Widerspruch, als **Teil eines kompromittierten Systems** genau dieses zu schützen, lässt sich daher nicht ausräumen.

Was ist zu tun?
Personal Firewalls können erfahrenen Anwendern Hilfestellung bei der Analyse ihres Systems geben. Sie können gleichfalls vor den Auswirkungen einiger Schadprogramme schützen. Für unerfahrene Anwender stellen Personal Firewalls keinen wesentlichen Sicherheitsgewinn dar. Durch Fehlbedienung ist unter Umständen sogar eine Verringerung des Sicherheitsniveaus möglich.

11 Europa und Internationales

Die **internationale Dimension personenbezogener** Datenverarbeitung macht es nötig, sich auf europäischer, bilateraler und globaler Ebene um den Schutz informationeller Selbstbestimmung der Bürgerinnen und Bürger Schleswig-Holsteins zu kümmern. Dabei geht es nicht nur, aber auch um die Verarbeitung im Internet (Tz. 2.4).

Im europäischen Rahmen besteht grundsätzlich Konsens über den Schutzbedarf personenbezogener Daten. Die **Europäische Union** (EU) engagiert sich nicht nur für die Förderung der Datenverarbeitung, sondern auch für den damit notwendigen Grundrechtsschutz – mit mehr oder weniger Erfolg. So bleibt der Datenschutz trotz eines umfangreichen Datenaustausches und ehrgeizigen Planungen im Bereich der polizeilichen und justiziellen Zusammenarbeit äußerst notleidend (Tz. 11.1). Nachholbedarf, aber mehr Hoffnung als im Bereich der dritten Säule besteht auch bei der Umsetzung der EU-Dienstleistungsrichtlinie (Tz. 6.3). Positive Signale kommen von der EU-Kommission hinsichtlich der noch nicht abgeschlossenen Planungen zur Überarbeitung der Datenschutzrichtlinie für Telekommunikationsanbieter, der sogenannten ePrivacy-Richtlinie. Innovationsfördernd in Sachen Datenschutz ist die EU durch die Unterstützung von zukunftsweisenden Projekten, an denen das ULD beteiligt ist, so z. B. von PrivacyOS (Tz. 8.2), PrimeLife (Tz. 8.3), FIDIS (Tz. 8.4), PRISE (Tz. 8.6), Malta Twinning Light (Tz. 8.9), EUCoop (Tz. 8.10.2), RISERid (Tz. 8.11) und IM Enabled (Tz. 8.12). Die Förderung des Europäischen Gütesiegels durch EU-Gremien geht über die rein finanzielle Unterstützung hinaus; hier ist die EU Motor einer internationalen Entwicklung (Tz. 9.3).

Eine Besonderheit weist die Beziehung zu den **Vereinigten Staaten von Amerika** auf. In den USA gibt es bisher nur Ansätze für ein Datenschutzrecht, die unseren Anforderungen und Erwartungen nicht genügen. Dies hat direkte negative Auswirkungen auf die Menschen in Schleswig-Holstein, etwa bei Verleumdungsdiensten mit Sitz in den USA (Tz. 7.4). Aber auch der Diskurs mit seriösen Unternehmen wie Google, das ein umfangreiches Internetangebot über Europa und die Welt ausgießt, ist wegen des rudimentären Datenschutzes in den USA schwerfällig (Tz. 7.1 bis Tz. 7.3 und Tz. 10.5).

Große US-Unternehmen sind ebenso wie das ULD einbezogen in **globale Bestrebungen** zur Regulierung der personenbezogenen Datenverarbeitung. Das ULD wirkt im Rahmen seiner Projektarbeit an der Entwicklung internationaler Datenschutzstandards mit. Es stellt den Sekretär der Arbeitsgruppe 5 „Identity Management and Privacy Technologies“ des ISO/IEC JTC 1/SC 27. Schwerpunkt war insofern die Entwicklung und Kommentierung von Standards zu einem „Privacy Framework“, einer „Privacy Reference Architecture“ und eines „Identity Framework“. Zudem nahm das ULD an der Erarbeitung von Policystandards beim

W3C, dem World Wide Web Consortium, teil und bringt seine Erfahrungen in den internationalen Diskurs ein, der von der nationalen spanischen Datenschutzbehörde zur Vorbereitung der kommenden Internationalen Datenschutzkonferenz koordiniert wird.

11.1 Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit

Nach der lang erwarteten Verabschiedung des Rahmenbeschlusses für den Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit ist ein einheitliches hohes Datenschutzniveau in der EU nicht in Sicht.

Der Rahmenbeschluss über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, der sogenannten dritten Säule, verarbeitet werden, ist vom Rat der Europäischen Union (EU) verabschiedet worden. Ziel des Rahmenbeschlusses war die Herstellung eines **gleichwertigen hohen Datenschutzniveaus** innerhalb der EU im Bereich der dritten Säule. Innerhalb der ersten Säule, den europäischen Gemeinschaften, ist dieses Ziel erreicht. Die Datenschutzrichtlinie aus dem Jahr 1995 ist in allen Mitgliedstaaten umgesetzt.

Leider bleibt der verabschiedete Rahmenbeschluss weit hinter den Erwartungen und dem Erforderlichen zurück. Weder ein gleichwertiges noch ein hohes, ja **nicht einmal ein angemessenes Datenschutzniveau** wurde für die dritte Säule erreicht. Der Anwendungsbereich des Rahmenbeschlusses ist auf die reine grenzüberschreitende Kommunikation beschränkt geblieben. Die hierfür festgelegten Regelungen bleiben hinter dem nationalen, z. B. dem deutschen, und auch dem europäischen Datenschutzniveau aus der ersten Säule weit zurück (30. TB, Tz. 11.2).

Der Rahmenbeschluss findet nur auf diejenigen personenbezogenen Daten Anwendung, die zwischen den Mitgliedstaaten ausgetauscht werden. Für die rein innerstaatliche Datenverarbeitung gelten die Vorgaben des Rahmenbeschlusses – anders als die Datenschutzrichtlinie der ersten Säule – dagegen nicht. Es kann so nicht gewährleistet werden, dass die von anderen Mitgliedstaaten an deutsche Behörden übermittelten Daten in einer Weise erlangt und verarbeitet wurden, die einem Mindeststandard genügt. Dies ist nicht nur im Hinblick auf den Grundrechtsschutz der Betroffenen unbefriedigend, auch die Qualität der Daten ist nicht ausreichend gewährleistet. Außerdem wird ein erheblicher **Mehraufwand bei der anschließenden Verarbeitung** der zwischen den Mitgliedstaaten übermittelten Daten entstehen, da für die übermittelten Daten andere Anforderungen gelten als für die nationalen Daten, die der Empfänger ebenfalls verarbeitet.

Auch die inhaltlichen Vorgaben des Rahmenbeschlusses sind unzureichend; die letztjährige Kritik gilt weiterhin (30. TB, Tz. 11.2). Besonders defizitär ist das **Recht der Betroffenen auf Auskunft** geregelt. Das deutsche Recht räumt den Betroffenen grundsätzlich einen eigenen umfassenden Auskunftsanspruch über die zur Person bei einer Stelle gespeicherten Daten ein. Dies ist nach deutschem Verfassungsrecht geboten. Der Rahmenbeschluss dagegen reduziert den Anspruch

des Betroffenen auf die Bestätigung der nationalen Kontrollstelle, dass alle erforderlichen Prüfungen durchgeführt wurden.

Von einem gleichwertigen hohen Datenschutzniveau sind Polizei und Justiz in Europa nach Verabschiedung des Rahmenbeschlusses weit entfernt. Ein solches Niveau ist aber seit Jahren überfällig, da ungeachtet der datenschutzrechtlichen Defizite der **Informationsaustausch zwischen den Mitgliedstaaten** und den Einrichtungen der EU wie Europol und Eurojust immer mehr ausgebaut wird. Es gibt Informationssysteme wie das Schengener Informationssystem und das Visa-Informationssystem, die ständig erweitert werden. Der durch den Prümer Vertrag ermöglichte Zugriff der Behörden der Vertragsstaaten auf DNA-, Fingerabdruck- und Kfz-Daten wird durch Überführung in den Rechtsrahmen der EU auf die anderen EU-Mitgliedstaaten ausgedehnt. Zu der Vielzahl der Maßnahmen hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Entschließung gefasst:

www.bfdi.bund.de/cln_027/nn_1207020/DE/Oeffentlichkeitsarbeit/Entschliessungssammlung/DSBundLaender/76DSK__ZusammenarbeitEuropa.html

Im Rahmenbeschluss zur sogenannten **Schwedischen Initiative** wird den Mitgliedstaaten sogar auferlegt, für die Übermittlung personenbezogener Daten an Stellen anderer Mitgliedstaaten und Einrichtungen der EU dieselben Maßstäbe anzulegen wie für die Übermittlung an nationale Stellen (Tz. 11.2). Nach geltendem Recht unterliegt die Datenübermittlung an Polizei- und Justizbehörden anderer Mitgliedstaaten oder der EU in Deutschland strengeren Voraussetzungen als die Übermittlung an deutsche Polizei- und Justizbehörden. Der Grund ist, dass ein Datenschutzniveau nach nationalem Recht im Empfängerstaat nicht sichergestellt ist. Eine solche Garantie ist nach Verabschiedung des Rahmenbeschlusses für den Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit nicht in Sicht. Dennoch werden die Mitgliedstaaten gezwungen, die gesetzlichen Voraussetzungen für einen erleichterten innereuropäischen Datenaustausch zu schaffen.

Welche Konsequenzen das für die Betroffenen hat, wird am **Beispiel des Auskunftsanspruchs** deutlich: Übermittelt eine deutsche Polizei- oder Justizbehörde personenbezogene Daten an eine Stelle eines anderen Mitgliedstaates, so kann der Betroffene von der deutschen Stelle grundsätzlich Auskunft über die dort zu seiner Person gespeicherten Daten und auch über die Empfänger verlangen, an welche die Daten übermittelt wurden. Möchte er darüber hinaus erfahren, wie seine Daten vom Empfänger weiterverarbeitet wurden, dann richtet sich der Auskunftsanspruch nach dem Recht des Empfängerstaats. Der Rahmenbeschluss für den Datenschutz in der dritten Säule gewährleistet nicht, dass die Auskunftserteilung durch den Empfänger angemessenen Datenschutzstandards genügt.

Was ist zu tun?
Der Rahmenbeschluss für den Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit bedarf hinsichtlich seines Anwendungsbereichs, der vorgesehenen Datenschutzstandards und der Datenschutzkontrolle einer massiven Verbesserung.

11.2 Innereuropäischer Datenaustausch à la „Schwedische Initiative“

Das Fehlen eines einheitlichen und angemessenen Datenschutzniveaus in Europa hindert den Rat der Europäischen Union nicht an der Intensivierung des personenbezogenen Informationsaustausches der Strafverfolgungsbehörden. Die fehlenden Datenschutzvorkehrungen müssen daher auf nationaler Ebene nachgerüstet werden.

Der Rat der Europäischen Union hat im Jahr 2006 einen Rahmenbeschluss zur Vereinfachung des Informationsaustausches zwischen den Strafverfolgungsbehörden der EU-Mitgliedstaaten verabschiedet – die „Schwedische Initiative“. Der Informationsaustausch soll dadurch erleichtert werden, dass für innereuropäische grenzüberschreitende Datenübermittlungen dieselben Voraussetzungen gelten sollen wie für solche innerhalb eines Mitgliedstaates. Die Umsetzung wird zu einem deutlichen quantitativen **Anstieg und zur Beschleunigung** des Informationsaustausches zwischen Polizeien und Justizbehörden in Europa führen. Da es nach Verabschiedung des Rahmenbeschlusses für den Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit (Tz. 11.1) weiterhin kein einheitliches und angemessenes Datenschutzniveau in Europa gibt, sind die vorgesehenen Erleichterungen des Datenaustausches persönlichkeitsrechtlich hochgefährlich.

Der Rahmenbeschluss zur Vereinfachung des Informationsaustausches zwischen den europäischen Strafverfolgungsbehörden muss national umgesetzt werden. Die Frist hierfür ist mittlerweile verstrichen; dem ULD sind aber noch keine Entwürfe bekannt. Dabei sind die **verbleibenden Spielräume** zur normenklaren und verhältnismäßigen Gestaltung der Befugnisse zum Informationsaustausch **zu nutzen**. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu eine Entschließung gefasst. Die Voraussetzungen für die Übermittlung, also die Anforderungen an ein entsprechendes Ersuchen, den Umfang der zu übermittelnden Daten, die zuständigen Stellen und die weitere Verwendung der Daten sind zu regeln.

www.bfdi.bund.de/cln_027/nn_1207020/Oeffentlichkeitsarbeit/Entschliessungssammlung/DSBundLaender/76DSK__SchwedischeInitiative.html

Was ist zu tun?
Die Gesetze zur Umsetzung des Rahmenbeschlusses müssen die europäischen Defizite zur Sicherung des Datenschutzes beim polizeilichen und justiziellen Austausch kompensieren.

12 Informationsfreiheit

12.1 EU-Transparenzinitiative und das Agrar- und Fischereifonds-Informationen-Gesetz

Der Bundesgesetzgeber hat ein Agrar- und Fischereifonds-Informationen-Gesetz verabschiedet, dessen Ziel es ist, mehr Transparenz bei der Verwendung europäischer Subventionen zu schaffen. Dabei ist der Gesetzgeber jedoch hinter den Erwartungen zurückgeblieben.

Mit dem Bundesgesetz werden die gemeinschaftsrechtlichen Vorgaben zum Europäischen Fischereifonds (EFF), zum Europäischen Garantiefonds für die Landwirtschaft (EGFL) und dem Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raumes (ELER) umgesetzt, wonach Informationen zu den **gezahlten Subventionen veröffentlicht** werden sollen. Bei Subventionen im Bereich des EGFL und des ELER werden zu den Empfängern insbesondere die folgenden Informationen veröffentlicht: Vorname und Name, die Gemeinde, in der der Empfänger wohnt oder eingetragen ist, sowie gegebenenfalls die Postleitzahl, die Höhe der gezahlten Beträge, die im Haushaltsjahr zugeflossen sind, sowie Angaben zur Währung. Bei Subventionen im Bereich des EFF wird ein Verzeichnis der Begünstigten, die Bezeichnung der Operationen und des Betrags der für die Vorhaben bereitgestellten öffentlichen Mittel veröffentlicht.

Die mit dem Agrar- und Fischereifonds-Informationen-Gesetz geschaffene Transparenz stellt einen Schritt in die richtige Richtung dar. Für die Öffentlichkeit wird so prüfbar, welche Beträge im Einzelnen ausgezahlt wurden. Ferner wirkt die Veröffentlichung der Angaben auf eine wirtschaftliche Haushaltsführung hin. Doch wurde dem Transparenzgedanken nicht ausreichend Rechnung getragen, da bei Zahlungen aus den verschiedenen Fonds nicht der jeweilige **Förderungszweck** benannt wird. Diese Veröffentlichung wäre nach den gemeinschaftsrechtlichen Vorgaben möglich. Eine Prüfung, inwieweit die Fördermittel an die einzelnen Empfänger ordnungsgemäß vergeben wurden, kann nicht stattfinden, da z. B. verborgen bleibt, ob sich die Förderung auf einen materiellen Gegenstand, auf die Finanzierung einer Infrastrukturmaßnahme oder auf eine Baumaßnahme bezog.

Aus Datenschutzsicht kritisch ist, dass bereits in den europäischen wie auch den deutschen Regelungen den Empfängern keine Widerspruchsrechte gegen die Veröffentlichung eingeräumt werden; für den EFF werden diese sogar nach EU-Recht ausdrücklich relativiert. Nach allgemeinem Datenschutzrecht muss aus überwiegenden schutzwürdigen, sich aus ihrer besonderen Situation ergebenden Gründen von einer Veröffentlichung abgesehen werden. Dies kann vor allem bei **Kleinunternehmern mit geringen Förderhöhen** der Fall sein (30. TB, Tz. 12.1). Das ULD unterstützt die Forderung des Europäischen Datenschutzbeauftragten, dass Widerspruchsrechte berücksichtigt werden. Auf nationaler Ebene kann im Rahmen des Verordnungserlasses der Datenschutz zumindest teilweise noch zur Geltung gebracht werden.

Was ist zu tun?
Alle Beteiligten müssen darauf hinwirken, dass der Transparenzgedanke und der Datenschutz bei der EU-Subventionskontrolle in ein ausgewogenes Verhältnis gebracht werden.

12.2 Was kostet die Sanierung des Holstentores?

Die Vergabe öffentlicher Aufträge unterliegt im Rahmen der vergaberechtlichen Vorschriften der Informationsfreiheit.

Eine Antragstellerin begehrte von der Stadt Lübeck Einsicht in diverse **Kostenabrechnungen** zur Sanierung des Holstentores. Die Stadt verweigerte dies und berief sich insbesondere auf vergaberechtliche Vorschriften, wonach Angebote und ihre Anlagen zu verwahren und geheim zu halten sind.

Zwar sind die begehrten Kostenabrechnungen keine **Angebotsunterlagen**, doch muss für Informationen, welche Rückschlüsse auf diese zulassen, ein vergleichbarer Geheimnisschutz gelten. Das ULD hat sich zur näheren Prüfung exemplarisch zu einem Angebot die Unterlagen und die dazugehörigen Schlussrechnungen vorlegen lassen. Der Vergleich ergab, dass die Rechnungen derart detailliert aufgeschlüsselt sind, dass sie bis in die einzelnen Positionen den Punkten des Angebotes entsprechen. Da pro Gewerk für die Sanierung jeweils nur ein einziges Unternehmen beauftragt wurde und die beauftragten Unternehmen auf einer am Holstentor angebrachten Tafel eingesehen werden konnten, war es möglich, aus der Schlussrechnung die Bieterunterlagen zu rekonstruieren. Selbst bei einer Anonymisierung des Bieters wäre aufgrund der spezifischen Angaben in der Schlussrechnung in Verbindung mit den Angaben auf der am Holstentor angebrachten Tafel erkennbar gewesen, welches Unternehmen die Schlussrechnung erstellt hat. Die Stadt Lübeck hatte das spezifische Informationsbegehren daher zu Recht abgelehnt.

Was ist zu tun?
Das Vergaberecht steht einem Informationszugang entgegen, wenn aus den begehrten Unterlagen detaillierte Rückschlüsse auf die Angebotsunterlagen und deren Anlagen gezogen werden können.

12.3 Ein gesunder Insolvenzverwalter wendet sich an eine Krankenkasse

Das Informationsfreiheitsgesetz Schleswig-Holstein findet neben den gesetzlichen Bestimmungen zum Insolvenzrecht Anwendung.

Ein Insolvenzverwalter begehrte von einer gesetzlichen Krankenkasse im Hinblick auf die versicherte Insolvenzschuldnerin Auskünfte zu **eingegangenen Beträgen und Nebenforderungen** sowie zur Höhe der Rückstände zu den jeweiligen Zahlungseingängen. Die Krankenkasse bat das ULD um Prüfung, ob das Informationsfreiheitsgesetz Schleswig-Holstein (IFG-SH) überhaupt zur Anwendung kommt.

Nach dem Insolvenzrecht ist der Insolvenzschuldner verpflichtet, dem Insolvenzverwalter über alle das Insolvenzverfahren betreffenden Verhältnisse Auskunft zu geben. Diese Auskunftspflicht erstreckt sich auf alle vermögensrelevanten Umstände, die eine Bestimmung der Vermögensmasse zulassen. Hierzu gehören bestehende Forderungen oder Angaben, die für eine Betriebsfortführung von Bedeutung sein können. Das Insolvenzrecht begründet keinen Auskunftsanspruch des Insolvenzverwalters gegenüber einer gesetzlichen Krankenkasse. Nach dem IFG-SH bleiben Zugangsrechte in „anderen Vorschriften", die einen weitergehenden Zugang ermöglichen, allerdings unberührt. Hierzu gehören die Bestimmungen des Insolvenzrechtes. Der Gesetzgeber hat mit dem Insolvenzrecht auch **keine abschließende Regelung** getroffen, sodass das IFG-SH parallel Anwendung findet.

Der Insolvenzschuldner konnte sich bezüglich der bei der Krankenkasse vorhandenen Unterlagen nicht auf den Schutz von **Betriebs- und Geschäftsgeheimnissen** berufen. Diese setzen ein berechtigtes Geheimhaltungsinteresse des Insolvenzschuldners voraus. Gegenüber dem Insolvenzverwalter besteht ein solcher Diskretionsanspruch nicht; der Insolvenzschuldner wäre diesem nach Insolvenzrecht auskunftspflichtig.

Was ist zu tun?
Die gesetzlichen Krankenkassen müssen nach dem Informationsfreiheitsgesetz Schleswig-Holstein den Insolvenzverwaltern vermögensrelevante Auskünfte zu den Insolvenzschuldnern erteilen. Das Insolvenzrecht steht dem nicht entgegen.

12.4 Keine Wahl bei der Wahlkreiseinteilung?

Die Vorschriften des Gemeinde- und Kreiswahlgesetzes sind neben dem Informationsfreiheitsgesetz Schleswig-Holstein anwendbar.

Ein Bürger wandte sich an einen Landkreis und erbat die Bereitstellung von Unterlagen über die Wahlkreiseinteilung zur Kreistagswahl 2008. Der Kreis lehnte einen Informationszugang ab und berief sich dabei auf das Gemeinde- und Kreiswahlgesetz. Die Einsicht könne dazu führen, dass die **unabhängige Tätigkeit der Wahlorgane** unzulässig beeinflusst werde. Zudem stehe einer Offenlegung der Informationen das Wahlgeheimnis entgegen.

Nach dem Wahlrecht sind Personen, die bei Wahlen eine ehrenamtliche Tätigkeit übernehmen, zur unparteiischen Wahrnehmung ihres Amtes und zur **Verschwiegenheit** über die ihnen bei ihrer Tätigkeit bekannt gewordenen Tatsachen, insbesondere über alle dem Wahlgeheimnis unterliegenden Angelegenheiten, zu verpflichten. Dies schließt jedoch die Anwendung des IFG-SH nicht aus. Ein Anspruch auf Informationszugang bezüglich der Unterlagen zur Wahlkreiseinteilung ist wohl möglich. Das IFG-SH enthält ja Vorschriften, die den behördlichen Entscheidungsprozess und personenbezogene Daten hinreichend schützen.

Die Einteilung der Wahlkreise berührt nicht das **Wahlgeheimnis**. Dieses zielt darauf ab, dass die Wählerin oder der Wähler den Stimmzettel unbeobachtet kennzeichnen kann und deren individuelles Wahlverhalten nicht bekannt wird. Die Einteilung der Wahlkreise hat damit nichts zu tun.

Was ist zu tun?
Die Behörden müssen auch bei Wahlunterlagen im Einzelfall prüfen, ob ein Informationszugang nach dem Informationsfreiheitsgesetz in Betracht kommt.

12.5 Die Geschäftsgeheimnisse des Bundes

Die Bundesanstalt für Immobilienaufgaben kann sich nicht auf eigene Betriebs- und Geschäftsgeheimnisse berufen. Einem Informationszugang können jedoch öffentliche Belange entgegenstehen.

Ein Bürger beantragte bei einer Behörde des Landes die Einsichtnahme in ein Bodenwertgutachten, welches im Auftrag der **Bundesanstalt für Immobilienaufgaben** (BImA) erstellt wurde. Bei der BImA handelt es sich um eine Anstalt öffentlichen Rechts, die der Aufsicht des Bundesministeriums der Finanzen unterliegt. Sie vermarktet Liegenschaften (Vermietung, Verkauf, forstliche Bewirtschaftung), die der Bund nicht mehr zur Erfüllung seiner Aufgaben braucht. Die schleswig-holsteinische Behörde bat das ULD um Beratung.

Die BImA als Anstalt öffentlichen Rechts konnte sich im vorliegenden Fall nicht auf den Schutz von **Betriebs- und Geschäftsgeheimnissen** berufen. Dieser Schutz dient der Sicherung privatwirtschaftlicher Positionen und basiert auf den Grundrechten des Unternehmers. Daher können sich öffentliche Stellen grundsätzlich nicht auf den Schutz von Betriebs- und Geschäftsgeheimnissen berufen.

Der Offenlegung des Gutachtens standen auch keine **öffentlichen Belange** entgegen. Solche können vorliegen, wenn das Bekanntwerden der Informationen die Beziehungen zwischen dem Bund und Schleswig-Holstein schädigen würde. Bei einer Schädigungsprognose wird insbesondere darauf abgestellt, ob der Informationszugang bestehende Geheimhaltungsvereinbarungen verletzen würde, die einem berechtigten und zu akzeptierenden Willen der jeweiligen Stelle entsprechen. Schließlich wird geprüft, ob mit der Offenlegung die beim Bund bestehende Rechtslage im Informationszugangsbereich unterlaufen würde. Beides traf überwiegend nicht zu: Anhaltspunkte für einen berechtigten Willen zur Geheimhaltung waren nicht feststellbar. Die beim Bund bestehende Rechtslage wurde nicht unterlaufen, da im Rahmen einer hypothetischen Anwendung des Informationsfreiheitsgesetzes des Bundes (IFG-Bund) einem Informationszugang ebenfalls keine öffentlichen Belange entgegengestanden hätten. Zwar schützt das IFG-Bund auch fiskalische Interessen von Bundesbehörden, doch hatten die Angaben im begehrten Bodenwertgutachten keinen wesentlichen Einfluss auf laufende Verkaufsverhandlungen. Der Informationszugang unterlag insoweit keiner Beschränkung.

Was ist zu tun?
Verfügt eine schleswig-holsteinische Behörde über Informationen, die von einer öffentlichen Stelle des Bundes stammen, so muss stets geprüft werden, ob der Informationszugang die Beziehungen zwischen dem Bund und Schleswig-Holstein schädigen würde.

12.6 Informationsfreiheit auf dem Friedhof

Eine Anstalt öffentlichen Rechts kann sich nicht auf den Schutz von Betriebs- und Geschäftsgeheimnissen berufen, soweit diese öffentliche Aufgaben wahrnimmt.

Der Antragsteller interessierte sich für die Aufstellung über die erzielten Einnahmen einer für die Bewirtschaftung von Friedhöfen zuständigen Anstalt öffentlichen Rechts. Die Anstalt lehnte den Antrag unter Hinweis auf den Schutz von Betriebs- und Geschäftsgeheimnissen ab. Sie wies den Antragsteller darauf hin, dass neben den städtischen Friedhöfen ein Krematorium betrieben werde, das im Wettbewerb zu anderen privat oder öffentlich betriebenen Krematorien steht. Die Liberalisierung im Bestattungswesen habe zu einem wirtschaftlichen Wettbewerb geführt, es würden insoweit **keine öffentlichen Aufgaben** wahrgenommen.

Im vorliegenden Fall nahm die Anstalt eine öffentliche Aufgabe wahr. Dies ergab sich bereits aus der bestehenden Friedhofssatzung. Die Aufgabe der Anstalt besteht darin, die Bevölkerung mit **Bestattungs- und Grabpflegeleistungen** zu versorgen, ein Krematorium und eine Leichenhalle zu betreiben und für die Unterhaltung des öffentlichen Grüns auf den Friedhöfen zu sorgen. Für die Anstalt besteht die Verpflichtung, die übertragenen Aufgaben sparsam, wirtschaftlich und unter Beachtung des öffentlichen Zwecks zu führen. Unter diesen Voraussetzungen war die Anstalt verpflichtet, einen Informationszugang zu gewähren. Da die Anstalt weiterhin eine Offenlegung der erzielten Einnahmen ablehnte, musste das ULD dies förmlich beanstanden.

Was ist zu tun?
Bei der Beurteilung, ob sich öffentliche Stellen ausnahmsweise auf den Schutz von Betriebs- und Geschäftsgeheimnissen berufen können, ist zu prüfen, ob öffentliche Aufgaben wahrgenommen werden oder ein rein privates Handeln vorliegt.

12.7 Wer hat mich verraten?

Die Offenlegung der Identität von Behördeninformanten kommt nur in Betracht, wenn ausreichende Anhaltspunkte dafür vorliegen, dass der Informant seine Angaben wider besseres Wissen oder zumindest leichtfertig gemacht hat.

Die zuständigen Mitarbeiter der Bauaufsicht eines Kreises erhielten von einer Person den Hinweis, dass bei den Aufgängen eines bestimmten Gebäudes eine erhöhte Absturzgefahr bestehe und keine ausreichenden **Sicherheitsvorkehrungen** getroffen seien. Die behördlichen Mitarbeiter prüften den Sachverhalt vor Ort und sahen keine übermäßigen Sicherheitsrisiken. Der Eigentümer des Gebäudes stellte daraufhin beim Kreis einen Antrag nach dem Informationsfreiheitsgesetz, um die Identität des Behördeninformanten zu erfahren.

Der Name des Behördeninformanten ist ein personenbezogenes Datum. Der Offenbarung standen hier überwiegende schutzwürdige Belange des Informanten entgegen. Die Behörden sind zur Erfüllung ihrer Aufgaben auf die Hinweise von Informanten angewiesen, wobei deren Identität grundsätzlich geheim zu halten ist, wenn diese der Offenlegung nicht zustimmen. Eine andere Beurteilung kommt nur in Betracht, wenn genügend Anhaltspunkte dafür vorliegen, dass der Informant **wider besseres Wissen oder leichtfertig**, d. h. entgegen jeder Logik, falsche Informationen gegeben hat. Konkret waren hier für eine Beurteilung der Sicherheitsvorkehrungen fachliche und rechtliche Kenntnisse erforderlich, die einem Informanten nicht ohne Weiteres zur Verfügung stehen. Die falsche Einschätzung führte nicht zum Schluss leichtfertiger Datenweitergaben durch den Informanten. Die Preisgabe des Namens des Informanten musste daher unterbleiben.

Was ist zu tun?
Die Behörden müssen prüfen, ob konkrete Anhaltspunkte dafür vorliegen, dass der Informant vorsätzlich oder leichtfertig falsche Informationen weitergegeben hat.

12.8 Informationsfreiheit für 1-Euro-Jobber

Der Prüfbericht einer ARGE zu einem Maßnahmeträger enthält nicht zwingend Betriebs- und Geschäftsgeheimnisse.

Eine Antragstellerin begehrte gegenüber einer ARGE Einsicht in einen Ergebnisbericht, der im Rahmen der Prüfung eines Maßnahmeträgers für 1-Euro-Jobber erstellt wurde. Die ARGE gab zu bedenken, dass hier Betriebs- und Geschäftsgeheimnisse des **Maßnahmeträgers** zu beachten seien, da der Träger in der Form einer privatrechtlichen Gesellschaft, einer GmbH, organisiert war.

Ein Betriebs- und Geschäftsgeheimnis setzt voraus, dass die geheim zu haltenden Tatsachen Gegenstand eines berechtigten wirtschaftlichen Interesses sind. Der Bericht, den sich das ULD für Prüfzwecke vorlegen ließ, enthielt allerdings keine Angaben z. B. zur Projektidee oder Projektumsetzung, deren Offenlegung den Wettbewerb um künftige **Projekte negativ beeinflussen** konnte. Die bloße Beschreibung von Räumlichkeiten, Sachmitteln und Arbeitsabläufen bildete ebenso wenig den Gegenstand eines berechtigten wirtschaftlichen Interesses, da damit nicht gleichzeitig schutzwürdige Rechnungsunterlagen, Kalkulationsgrundlagen, Produktionsabläufe, Konditionen oder Marktstrategien verbunden waren. Im Ergebnis enthielt der Prüfbericht damit keine Betriebs- und Geschäftsgeheimnisse. Der Informationszugang musste gewährt werden.

Was ist zu tun?
Betriebs- und Geschäftsgeheimnisse müssen als Begründung einer Auskunftsverweigerung tatsächlich festgestellt werden.

12.9 „Vorhandene“ Informationen im Internet

Informationen, die nicht einer Behörde zurechenbar und im Internet frei abrufbar sind, unterfallen nicht dem Informationsfreiheitsgesetz.

Ein Antragsteller bat eine ARGE um Zusendung von Kopien zu Handlungsempfehlungen, Arbeits- und Dienstanweisungen sowie Bearbeiterhinweisen, soweit diese für die Bearbeitung von Anträgen nach dem zweiten Sozialgesetzbuch von Bedeutung sind. Die ARGE kam dem Antragsbegehren nach, führte im Hinblick auf die **Bearbeiterhinweise** jedoch aus, dass solche nicht vorhanden seien. Zur Wahrnehmung von Aufgaben werde vonseiten des Leistungszentrums (ARGE) vielmehr auf die Empfehlungen und Hinweise der Bundesagentur für Arbeit zurückgegriffen, welche im Internet frei abrufbar sind.

Ein Antrag nach dem IFG-SH kann sich immer nur auf bei den Behörden „vorhandene“ Informationen beziehen, d. h., diese müssen in Schrift-, Bild-, Ton- oder elektronischer Form vorliegen oder auf sonstigen Informationsträgern gespeichert sein. Sind Bearbeiterhinweise, etwa als PDF-Datei, auf dem behördlichen Computersystem gespeichert, so sind sie vorhanden. Dies war vorliegend jedoch nicht der Fall. Die Behörde nutzte nur das **Internetangebot der Bundesagentur für Arbeit**, aus dem die Bearbeiterhinweise bei Bedarf am Computerbildschirm per Internet abgerufen wurden.

Was ist zu tun?
Sobald die per Internet recherchierten Informationen im behördlichen Computersystem gespeichert werden, gelten diese als vorhandene Informationen. Dann muss den Antragstellern ein Informationszugang gewährt werden.

13 DATENSCHUTZAKADEMIE – Nie war sie so wertvoll wie heute!

Datenklau spukt in Presse, Funk und Fernsehen. Die Sorge um den sorgfältigen Umgang mit persönlichen Daten ist vehement ins öffentliche Bewusstsein gerückt. Die Notwendigkeit für den einzelnen Bürger sowie für Institutionen und Firmen, Personaldaten professionell – also datenschutzgerecht – zu verarbeiten, weiterzugeben und zu sichern, wird verstärkt erkannt.

Datenschutzbeauftragte in Verwaltung und Wirtschaft, IT-Sicherheitsbeauftragte, Beschäftigte, die Personendaten verarbeiten, Administratoren, interessierte Bürgerinnen und Bürger – alle erhalten in der DATENSCHUTZAKADEMIE Schleswig-Holstein ein hochqualifiziertes und preisgünstiges Fortbildungsangebot.

- **Schulungsbetrieb 2008**

Über mangelnde Auslastung konnte sich die DATENSCHUTZAKADEMIE im Jahr 2008 nicht beklagen. Waren im Jahr 2007 insgesamt 766 **Teilnehmerinnen und Teilnehmer** zu verzeichnen (2006: 616), so nahmen im letzten Jahr 936 Menschen an Fortbildungsmaßnahmen der Akademie teil. Mit den 502 Besuchern der Sommerakademie „Internet 2008 – Alles möglich, nichts privat?“ hatten somit 1.438 Personen die Möglichkeit, sich live mit aktuellen und grundsätzlichen Fragen von Datenschutz und Datensicherheit auseinanderzusetzen. 14 Mitarbeiterinnen und Mitarbeiter des ULD vermittelten ihr Wissen in 32 regulären Kursen und 17 Sonderkursen über einen Zeitraum von insgesamt 111 Schulungstagen.

Damit kommt das ULD seiner **gesetzlichen Aufgabe** nach, Bürgerinnen und Bürger zu beraten und informieren sowie Fortbildungsveranstaltungen zu den Themen Datenschutz und Datensicherheit durchzuführen.

Die Dozentinnen und Dozenten der DATENSCHUTZAKADEMIE sind alle im ULD beschäftigt. Sie sorgen gemeinsam mit den Mitarbeitern der Nordsee Akademie und des Grenzvereins seit vielen Jahren mit ihrem Engagement für den guten Ruf der Akademie. Die Gemeinde der treuen Kursteilnehmer wächst stetig: Eine Teilnehmerin besuchte schon 23 Kurse. Beim 25. Kurs ist eine Ehrung fällig.

- **Sonderkurse**

Das Angebot der DATENSCHUTZAKADEMIE an kundenorientiert maßgeschneiderten Schulungsangeboten wurde verstärkt genutzt. Das **Ministerium für Umwelt, Landwirtschaft und ländliche Räume** (MLUR) legte gemäß der Anforderungen des Gutachtens zur „Sicherheit der ZIAF-Informationssysteme der Zahlstelle“ einen Schulungsplan vor, aus dem sich bedarfsgerechte Maßnahmen zur Sensibilisierung der Mitarbeiter ergaben (Tz. 9.2.2). In enger inhaltlicher Abstim-

mung zwischen MLUR und ULD wurden, aufbauend auf den BSI-Grundschutzkatalogen, 13 verschiedene Schulungsmodule den Zielgruppen

- Vorgesetzte,
- IT-Sicherheitsmanagement,
- Datenschutzbeauftragte,
- Infrastrukturverantwortliche,
- Benutzer und
- Administratoren

zugeordnet. In verschiedenen Kursen – von großen Einführungsveranstaltungen für alle Mitarbeiter bis zu Spezialistenworkshops – wurden von den Grundlagen der IT-Sicherheit über Sicherheitsmanagement/BSI-Grundschutz bis zu Windows-Betriebssystemen alle Themen erarbeitet, die für eine gelungene Durchführung des ZIAF-Auditprozesses im Ministerium notwendig sind.

Eine weitere umfangreiche, erst nach langen organisatorischen Vorbereitungen realisierbare Sonderkursreihe fand unter dem Thema „Datenschutz und Datensicherheit für Systemadministratoren“ im Auftrag der **Landeshauptstadt Kiel** statt. Die Stadt kam mit dieser Schulungsmaßnahme einer Aufforderung des Landesrechnungshofes nach. An 16 Schulungstagen sowie zwei Prüfungstagen bekamen 40 mit administrativen Tätigkeiten betraute Mitarbeiterinnen und Mitarbeiter der Stadt Kiel Kenntnisse vermittelt in

- datenschutzrechtlichen und -technischen Grundlagen,
- IT-Dokumentation und -Konzeption,
- Datenschutzmanagement, Netzwerken und Angriffen,
- Windows 2003.

Neun Teilnehmer der groß angelegten Schulung konnten ihre neu erlangte Sachkenntnis in der erfolgreichen Prüfung zum **„Systemadministrator mit Datenschutzzertifikat“** unter Beweis stellen. Zusammen mit drei weiteren Systemadministratoren, die im November 2008 die eintägige theoretische und praktische Prüfung erfolgreich absolvierten, erhielten damit in diesem Jahr insgesamt 12 Ausgebildete ihr Datenschutzzertifikat.

Weitere Sonderkurse wurden beispielsweise durchgeführt

- beim Kommunalen Forum für Informationstechnik (KomFit e.V.), „Sicherheitsmanagement auf Basis von IT-Grundschutz“,
- beim Zweckverband Kommunale Datenverarbeitung Oldenburg (KDO), „Datenschutzgerechter Einsatz von Linux“,
- in den Mürwiker Werkstätten, „Datenschutz in Werkstätten für Menschen mit Behinderungen unter Berücksichtigung der besonderen Berufsgeheimnisse“,

- gemeinsam mit dem IQSH, „Datenschutzrecht für Schulleiter“,
- bei der ARGE Mölln, „SGB-II Fallmanagement“,
- an der TU Harburg, „Einführung in das Datenschutzrecht“,
- beim Landesbetrieb für Straßenbau und Verkehr, „Grundschutz für Systemadministratoren“,
- beim Landesamt für soziale Dienste (LAsD), „Sozialdatenschutzrecht und Informationsfreiheitsgesetz SH“,
- beim Landesamt für Natur und Umwelt (LANU), „Rechtsfragen des LDSG“,
- beim Amt für ländliche Räume (ALR), „Einführung in das LDSG“,
- bei der Beschäftigungsgesellschaft Flensburg (bequa), „Sozialdatenschutz“,
- bei der ARGE Bad Segeberg, „Datenschutz im SGB-II-Bereich“.

- **Reguläre Kurse**

Erstmals fanden folgende Kurse statt:

- „Sicherheitsmanagement auf Basis von IT-Grundschutz“ (ITS-II),
- „Mit dem BSI-Grundschutztool zum IT-Sicherheitskonzept“ (BSI-GST) und
- „Von der Bedrohung zum Restrisiko“ (RISK).

Sie erfüllten die Erwartungen und werden fortgeführt.

Die Kurse „Test und Freigabe“ (TEST), „Firewalls: Theorie und Praxis“ (FW), „Datensicherheit und Datenschutz für Systemadministratoren“ (DS), „Vista und Longhorn für erfahrene Administratoren“ (WIN-NG) und „Windows 2003 Terminal Server mit Citrix Metaframe 4.0“ (WIN-TS) wurden 2008 nicht durchgeführt, werden aber 2009 erneut angeboten.

Im Jahresprogramm 2009 werden folgende Kurse neu aufgenommen:

- **„Wie schütze ich meine Daten im Alltag?“ (ALL)**: Der halbtägige Kurs findet im ULD statt und richtet sich an Privatpersonen (auch Gruppen oder Schulklassen). Dem eigenverantwortlichen Bürger werden Wege aufgezeigt, wie er Datenmissbrauch verhindern, Internet und elektronische Geschäfte sicher(er) nutzen und sich vor Computerviren usw. schützen kann.
- **„Was gibt’s Neues? – Aktuelle Entwicklungen im Bereich der Datensicherheit“ (AKT)**: Der Kurs für alle, die eigentlich schon alle Kurse absolviert haben, sich aber als erfahrene Datenschutzbeauftragte oder Systemadministratoren über den jeweils aktuellsten Stand der Technik und Neuerungen bei der Datensicherheit austauschen wollen.
- **„Arbeitnehmerdatenschutz“ (AND)**: Dieser Kurs wendet sich an Mitarbeiterinnen und Mitarbeiter der Personalabteilung und Personaleinsatzplanung, an betriebliche Datenschutzbeauftragte und Betriebsräte. Datenschutzrechtliche

Rahmenbedingungen für Leistungs- und Verhaltenskontrolle der Mitarbeiterinnen und Mitarbeiter stehen im Fokus dieses wichtigen Kurses.

Die seit vielen Jahren angebotenen Grundlagenkurse der DATENSCHUTZAKADEMIE erfreuen sich traditionell großer Beliebtheit:

- **„Datenschutzrecht" und „Datensicherheitsrecht" (DR/DT)** befähigen die Datenschutzbeauftragten der schleswig-holsteinischen Behörden nun schon seit 15 Jahren, ihre verantwortungsvolle Aufgabe fachkompetent wahrzunehmen.
- Die **„Einführung Datenschutz im Schulsekretariat" (ES)**, die in Zusammenarbeit mit Komma (Kompetenzzentrum für Verwaltungsmanagement) in Bordesholm stattfindet, wurde wegen des großen Interesses als Workshop im ULD fortgeführt.
- Der Kurs **„Führung von Personalakten" (PA)** wurde aus demselben Grund ein zweites Mal ausgeschrieben.
- Die Kurse im Sozial- und Medizinbereich bilden ebenfalls von jeher fundierte Grundlagen des Schulungsbetriebs: **„Datenschutz in der Arztpraxis" (AR)** und **„Datenschutz im Krankenhaus" (DK)** verzeichnen aufgrund vieler Unklarheiten im Zusammenhang mit der geplanten Einführung der elektronischen Gesundheitskarte und anderer Veränderungen im Rahmen der Gesundheitsreform regen Zuspruch. Sie werden im kommenden Jahr jeweils zwei-, statt bislang einmal angeboten. Der dreitägige Kurs **„Sozialdatenschutzrecht" (S)**, der ebenso wie andere Mehrtageskurse in der Nordsee Akademie Leck stattfindet, bildet in vielen Fällen die Initialzündung für die Buchung von Sonderkursen beispielsweise bei ARGEn und in Werkstätten für Menschen mit Behinderungen (siehe oben).

Was sagen unsere Kursteilnehmer?

„Ich hätte vorher nicht geglaubt, dass man den Stoff so interessant vermitteln kann."

„Sehr positiv überrascht."

„Angenehmer, lockerer Stil."

„Topdozent mit viel Humor und dennoch sehr sachlich."

„Praxisnahe Beispiele."

„Kompetent und informativ."

„Sehr zu empfehlen."

„Ich habe viele Anregungen für die Arbeit bekommen."

„Sehr gute Vorbereitung für die Tätigkeit behördlicher Datenschutzbeauftragter."

„Referent ist ausgezeichnet."

„Dröges Thema sehr lebhaft dargeboten!"

„Sehr gut – weiter so!"

- Datenschutz im privatwirtschaftlichen Bereich ist Thema in den Kursen zum „**Bundesdatenschutzgesetz" (BDSG I & II)** , dem **„Workshop für betriebliche Datenschutzbeauftragte" (DWBT)** und dem Kurs **„Technischer Datenschutz, Systemdatenschutz" (SIB)**. Diese Kurse stellen mit jeweils drei ausgebuchten Terminen pro Jahr einen wesentlichen Teil des Schulungsprogramms.

- Das Angebot im Bereich der Technikkurse konnte qualitativ konsolidiert werden. **„IT-Sicherheitsmanagement“ (ITS)** und **„Sicherheitsmanagement auf Basis von IT-Grundschutz“ (ITS-II)** sowie **„Mit dem BSI-Grundschutztool zum IT-Sicherheitskonzept“ (BSI-GST)** befähigen die Absolventen, die Sicherheit von Verfahren oder Geschäftsprozessen und die Verwaltung der IT-Verbünde von Organisationen mithilfe der IT-Grundschutzmethode umzusetzen. Diese Kursinhalte werden zunehmend von öffentlichen Stellen des Landes Schleswig-Holstein nachgefragt. Die Kurse **„Windows 2003 Sicherheit I und II“ (WIN I & II)** versetzen die Teilnehmerinnen und Teilnehmer in die Lage, eine Client/Server-Umgebung einzurichten, zu analysieren und eventuelle Schwachstellen abzubauen.
- Das **Praxisforum**, ein kostenlos angebotener Beratungsworkshop für behördliche Mitarbeiterinnen und Mitarbeiter, fand 2008 in den Räumen des ULD zu den Themen **„Test & Freigabe“** und **„Dokumentation nach LDSG und DSVO“** statt. 2009 wird zusätzlich das Thema **„Datenschutzpraxis für die Internetnutzung“** angeboten.

Praxisforum

Wir möchten gern mit Ihnen –

Datenschutz- und IT-Sicherheitsbeauftragten, IT-Revisoren/Prüferinnen und Prüfern, Fachverfahrensverantwortlichen, Administratorinnen und Administratoren –

Fragen aus der Praxis für die Praxis diskutieren, Erfahrungen austauschen, Neues dazulernen, Wissenswertes erarbeiten …

Das Praxisforum ist ein kostenfreies Beratungsangebot im Rahmen der DATENSCHUTZAKADEMIE Schleswig-Holstein, ULD, Holstenstraße 98, 24103 Kiel.

Info und Anmeldung: akademie@datenschutzzentrum.de, Tel. 0431/988-1281

- **Jahresprogramm 2009 der DATENSCHUTZAKADEMIE**

März	11.03.-13.03.	ITS	IT-Sicherheitsmanagement
	16.03.-18.03.	ITS-II	Sicherheitsmanagement auf Basis von IT-Grundschutz
	19.03.	ALL	Wie schütze ich meine persönlichen Daten im Alltag? **(NEU)**
	23.03.	BDSG-I	Grundkurs Bundesdatenschutzgesetz
	23.03.-25.03	WIN-I	Windows 2003 Sicherheit I
	24.03.	BDSG-II	Betriebliches Datenschutzmanagement
	25.03.	DWBT	Workshop für betriebliche Datenschutzbeauftragte
	26.03	SIB	Technischer Datenschutz/ Systemdatenschutz nach BDSG
	27.03.	AND	Arbeitnehmerdatenschutz (**NEU)**
April	27.04.-29.04.	BSI-GST	Mit dem BSI-Grundschutztool zum IT-Sicherheitskonzept
	23.04.	PD	Datenschutzgerechtes Produktdesign
Mai	04.05.-05.05.	RISK	Risikoanalyse und Risikomanagement
	05.05.	IFG	Das neue Informationsfreiheitsgesetz Schleswig-Holstein
	06.05.	AR	Datenschutz in der Arztpraxis
	07.05.	DK	Datenschutz im Krankenhaus
	11.05.-12.05.	DR	Datenschutzrecht für behördliche Datenschutzbeauftragte
	13.05.-15.05	DT	Datensicherheitsrecht für behördliche Datenschutzbeauftragte
	19.05.-20.05	TEST	Test und Freigabe
	26.05.-27.05	SiKo	Sicherheitskonzepte erstellen
Juni	03.06.	ES	Datenschutz im Schulsekretariat
	18.06.	LDSG-R	Rechtsfragen des Landesdatenschutzgesetzes
	22.06.-23.06.	PA	Führung von Personalakten
Juli	01.07.-03.07.	WIN-TS	Windows 2003 Terminal Server mit CitrixXenApp
	07.07.	BDSG-I	Grundkurs Bundesdatenschutzgesetz
	08.07.	BDSG-II	Betriebliches Datenschutzmanagement
	09.07.	SIB	Technischer Datenschutz/ Systemdatenschutz nach BDSG
August	31.08.	Sommerakademie: „Arbeitnehmer – Freiwild der Überwachung?“	

September	07.09.- 08.09.	DR	Datenschutzrecht für behördliche Datenschutzbeauftragte
	10.09.	ALL	Wie schütze ich meine persönlichen Daten im Alltag? **(NEU)**
	09.09.- 11.09	DT	Datensicherheitsrecht für behördliche Datenschutzbeauftragte
	15.09.	ES (WS)	Datenschutz im Schulsekretariat
	16.09.- 17.09.	AKT	Was gibt's Neues? Aktuelle Entwicklungen im Bereich der Datensicherheit **(NEU)**
	21.09.- 23.09.	S	Sozialdatenschutzrecht
	21.09.- 23.09.	WIN-I	Windows 2003 Sicherheit I
	28.09.- 29.09.	DS	Datensicherheit und Datenschutz für SystemadministratorInnen
Oktober	01.10.	AND	Arbeitnehmerdatenschutz **(NEU)**
	13.10.	BDSG I	Grundkurs Bundesdatenschutzgesetz
	14.10.	BDSG-II	Betriebliches Datenschutzmanagement
	15.10.	SIB	Technischer Datenschutz/ Systemdatenschutz nach BDSG
	26.10.- 28.10.	WIN-II	Windows 2003 Sicherheit II
November	03.11.- 04.11.	FW	Firewalls: Theorie & Praxis
	10.11.	AR	Datenschutz in der Arztpraxis
	11.11.	DK	Datenschutz im Krankenhaus
	10.11.- 11.11.	WIN- NG	Vista und Longhorn für erfahrene AdministratorInnen **(NEU)**
	18.11.- 20.11.	ITS	IT-Sicherheitsmanagement
	23.11.- 25.11.	ITS-II	Sicherheitsmanagement auf Basis von IT-Grundschutz
Dezember	01.12.	SDZ	Prüfung zum Systemadministrator mit Datenschutzzertifikat

Übrigens ...

ULD-Ausbildungsangebote gibt es bei uns nicht nur in der DATENSCHUTZ-AKADEMIE!

In der seit 2005 praktizierten Kooperation mit der Fachhochschule Kiel werden in jedem Wintersemester ca. 30 Bachelor- und Masterstudenten der Informatik und Wirtschaftsinformatik in Datenschutzrecht und -technik sowie IT-Recht unterrichtet.

Die Vorlesungen finden in den Räumen des ULD statt.

Sommerakademie 2009 * Sommerakademie 2009 * Sommerakademie 2009

Arbeitnehmer – Freiwild der Überwachung?

Das technische Überwachungs- und Kontrollpotenzial im Arbeitsleben beeinträchtigt zunehmend die Persönlichkeitsrechte von Beschäftigten:

- Betriebe werden videoüberwacht.
- Personalinformationssysteme erstellen Persönlichkeitsprofile.
- Telekommunikation und Internetnutzung werden protokolliert.
- Multifunktionale Mobilsysteme garantieren Totalüberwachung auch im Außendienst.
- Gesundheits- und Drogentests greifen in die Privatsphäre ein.
- Gentests bergen das Potenzial beruflicher Diskriminierung.
- Beschäftigte in internationalen Unternehmen arbeiten unter rechtsunsicheren Bedingungen.

Die Erkenntnis mancher Arbeitgeber, dass unkontrollierte Arbeit die Produktivität steigert, hat sich bisher wenig durchgesetzt.

Die Sommerakademie 2009 bietet eine Bestandsaufnahme der technischen Überwachungsmöglichkeiten, der Rechtslage und der Praxis und Lösungen für einen besseren technischen, organisatorischen und rechtlichen Arbeitnehmerdatenschutz.

Montag, 31. August 2009,
Maritim Hotel Bellevue, Kiel

Die Teilnahme ist kostenlos. Bitte melden Sie sich an unter

www.datenschutzzentrum.de/sommerakademie

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstr. 98, 24103 Kiel
Tel.: 0431/988-1200
Fax: 0431/988-1223
E-Mail: akademie@datenschutzzentrum.de

Index

A

Adressdaten **57**, **93**
Agrar- und Fischereifonds-Informationen-Gesetz **189**
Aktenvernichtung **94**
AN.ON **145**
Anonymisierung **77**, **105**, **118**, **137**, **190**
Anonymität im Internet **145**
Antiterrordatei **38**
Antiterrordateigesetz (ATDG) **38**
Arbeitnehmer **12**, **65**, **66**
Arbeitnehmerdatenschutz **12**
Arbeitsgemeinschaft (ARGE) **51**, **53**, **194**, **195**
Arbeitslosengeld **50**, **51**, **53**
Arbeitszeiterfassung **28**
@rtus **30**
Auftragsdatenverarbeitung **88**, **97**, **153**
Auskunft **21**, **30**, **53**, **61**, **108**, **186**, **191**
Auskunfteien **13**, **73**, **87**, **99**
Auskunftssperre **22**
Authentifizierung **19**, **116**, **154**
Authentisierung **110**, **128**
Authentizität **111**
automatisierte Verfahren **20**, **116**

B

Banken **13**, **81**
bdc\Audit **151**
Beratung **60**, **65**, **94**, **159**
Bestattungsgesetz **62**
Bewerber **93**
Bewerberdaten **94**
Bilddaten **137**
Biometrie **144**
Blackberry **175**
Bluetooth **131**
BMB-EUCoop **152**
Browser **181**
Bundesagentur für Arbeit (BA) **51**, **53**, **195**
Bundesauditgesetz **158**
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI) **38**
Bundesdatenschutzgesetz (BDSG) **13**, **73**, **79**, **84**
Bundeskriminalamt (BKA) **31**, **38**
Bundesverfassungsgericht **14**, **29**, **31**, **37**, **40**, **41**
Bürgerbüro **26**
Bußgeld **78**, **81**, **90**

D

Dataport **10**, **123**, **124**, **132**, **162**, **177**
Datenerhebung **27**, **34**, **47**, **63**, **94**, **100**, **118**
Datenerhebungsbefugnis **63**
DATENSCHUTZAKADEMIE Schleswig-Holstein **196**
Datenschutz-Audit **13**, **15**, **159**
  Kreis Plön **164**
  Ministerium für Bildung und Frauen **163**
  Unfallkasse Nord **165**
  ZIAF **161**
Datenschutzbeauftragter **115**
  behördlicher **105**, **114**, **116**
  betrieblicher **74**
Datenschutz-Behördenaudit **159**
Datenschutzgremium **17**
Datenschutz-Gütesiegel **15**, **155**, **159**, **166**, **169**
  Anerkennung von Sachverständigen **168**
  EuroPriSe (European Privacy Seal) **169**, **172**
  Rezertifizierung **167**, **171**
Datenschutzmanagement **107**, **162**
Datenschutzverordnung (DSVO) **103**, **107**, **162**
Datensicherheit **17**, **26**, **28**, **48**, **101**, **105**, **107**, **121**, **140**, **169**, **175**
Datensparsamkeit **18**, **36**, **111**, **117**
Datenspeicherung **22**, **82**
Datenübermittlung **22**, **57**, **95**, **112**, **187**
Datenvermeidung **36**
Deutsche Bundesbank **33**
DIANA **40**
DNA **187**
Dokumentation **17**, **63**, **103**, **108**, **120**, **121**, **122**, **131**, **161**, **163**, **175**

E

E-Government **14**, **110**, **112**, **120**, **152**
Einheitlicher Ansprechpartner (EAP) **109**, **110**

Einwilligung **47**, **56**, **69**, **71**, **74**, **82**, **84**, **88**, **93**, **97**, **98**, **127**, **136**
elektronische Gesundheitskarte **54**
elektronische Signatur **24**, **144**
elektronischer Einkommensnachweis (ELENA) **64**
elektronischer Personalausweis **25**
elektronischer Personalausweis (ePA) **143**
E-Mail **128**, **175**, **203**
ePass **26**, **143**
EU-Datenschutzrichtlinie **169**
EU-Dienstleistungsrichtlinie **109**, **112**, **185**
Europa **153**, **185**
Europäische Kommission **142**
Europäische Union (EU) **146**, **185**
European Privacy Seal (EuroPriSe) **155**, **166**, **169**, **170**, **171**, **172**, **174**

F

Fernmeldegeheimnis **31**, **41**, **102**, **126**
Finanzamt **69**, **70**, **71**
Finanzministerium **109**
Firewall **131**, **176**, **183**
Freigabe **22**, **103**, **106**, **107**, **108**, **175**
Future of Identity in the Information Society (FIDIS) **143**, **185**

G

genetische Daten **66**
Geodaten **75**, **120**
Geschäftsgeheimnis **195**
Globally Unique Identifier (GUID) **181**, **183**
Google **133**, **185**
Google Analytics **134**, **182**
Google Chrome **181**
Google Desktop **181**
Google Maps **135**, **137**, **181**
Google Street View **135**
Google Toolbar **181**
Gütesiegel **158**, **166**, **168**
  Anerkennung von Sachverständigen **168**

H

Handel **80**
Hartz IV **52**
Hinweis- und Informationssystem (HIS) **85**

I

Identitätsmanagement **142**, **143**, **144**
Industrie **142**
Informationsfreiheitsgesetz **190**, **191**, **195**
Informationsgesellschaft **62**
Informationssicherheitsmanagementsystem (ISMS) **123**
Instant Messaging Enabled E-Government Services (IM Enabled) **154**, **185**
Internet **32**, **90**, **97**, **100**, **128**, **133**, **149**, **150**, **185**, **195**
  Anonymität im **145**
IP-Adresse **19**, **117**, **119**, **172**, **181**, **183**
ISO 27001 **162**, **164**, **165**
ISSH **35**, **36**
IT-Konzept **106**, **120**, **122**
IT-Labor **175**
IT-Produkt **155**, **169**, **170**, **171**
IT-Sicherheit **48**, **162**, **164**
IT-Verfahren **29**, **108**, **163**

J

Jugendamt **58**, **60**, **61**
Justizverwaltung **40**
Justizvollzugsanstalten **42**, **43**

K

Kfz-Kennzeichenerfassung **29**
Kfz-Zulassungsbehörde **48**, **50**
Kieler Sicherheitskonzept Sexualstraftäter (KSKS) **44**
Kirchensteuergesetz **69**
Kommunalverwaltung **128**, **164**
Konferenz der Datenschutzbeauftragten des Bundes und der Länder **29**, **34**, **187**, **188**
Kontendaten **115**
Kontrollen **39**, **48**, **127**, **131**
Kontrollkompetenz **101**
Kraftfahrt-Bundesamt (KBA) **48**, **49**
Krankenkassen **190**
Krankenversicherung **56**
Krebsregister **55**
Kreditinstitute **68**, **83**
Kredit-Scoring **13**
Kundendaten **80**, **133**

L

Landesdatenschutzgesetz (LDSG) **28**
Landeskriminalamt (LKA) **29**, **33**, **35**
Landesverwaltungsgesetz **29**
Landtag **17**, **37**, **69**, **83**, **156**
Landwirtschaftsministerium **161**
Listenprivileg **75**, **81**, **99**
Löschung **24**, **27**, **71**, **108**, **118**, **135**, **138**

M

Mammografie-Screening **55**
Mandatsgeheimnis **101**
Meldebehörde **19**, **20**, **153**
Meldedaten **19**, **20**, **22**, **23**, **60**
Melderecht **18**, **20**, **23**
Melderegister **21**, **23**
Meldewesen **59**
Mitarbeiterbespitzelung **77**
Mobilfunk **175**

N

Normenklarheit **29**
Nutzerdaten **134**, **154**, **183**
Nutzungsdaten **134**

O

Online-Durchsuchung **14**, **31**, **37**
Online-Spiele **142**, **148**
OSCI-Transport **112**

P

Passwort **114**
Patientendaten **58**
Permission Marketing **13**, **14**, **74**, **82**
Personalakten **28**, **39**
Personalaktendaten **28**
Personendaten **14**, **74**, **149**
Personenüberprüfungsverfahren **33**
Pflegeheime **63**
Polizei **29**, **30**, **31**, **34**, **44**, **47**, **187**
Polizeirecht **29**
Privacy and Identity Management for Europe (PRIME) **142**
Privacy and Identity Management in Europe for Life (PrimeLife) **142**, **185**
Privacy Enhancing Shaping of Security Research and Technology (PRISE) **146**, **147**, **185**
Privacy Open Space (PrivacyOS) **140**
Protokolldaten **38**, **48**, **108**, **117**, **126**
Protokollierung **23**, **36**, **39**, **108**, **112**, **122**, **124**, **127**, **129**, **130**
Prüfungen **34**, **45**, **47**, **63**, **69**, **119**, **131**, **158**
Pseudonymisierung **56**, **118**
Public Key Infrastructures (PKI) **143**

R

Registry Information Service on European Residents (RISER) **152**, **153**

S

Schwedische Initiative **188**
Schweigepflicht **58**, **61**, **67**, **84**
Scoring **13**, **73**, **87**
Secure Access to Federated E-Justice/ E-Government (SAFE) **110**, **112**
Sicherheitskonzept **17**, **106**, **120**, **122**, **131**
Sicherheitsüberprüfungen **39**
Signatur **25**, **112**
Sommerakademie **13**, **196**, **203**
Sozialgesetzbuch **195**
Sozialhilfe **50**
Sparkassen **94**
Speicherung **35**, **41**, **54**, **72**, **118**, **134**
Staatsanwaltschaft **47**
Steuergeheimnis **69**
Steueridentifikationsnummer (Steuer-ID) **68**
Steuerverwaltung **68**
Strafvollzug **42**
Systemadministration **122**
Systemdatenschutz **103**

T

Telekom **12**
Telekommunikation **37**, **41**, **42**, **80**
Telekommunikationsdaten **73**
Telekommunikationsgeheimnis **128**
Telekommunikationsgesetz (TKG) **125**
Telemediengesetz (TMG) **125**
Transparenz **13**, **77**, **85**, **86**, **100**, **107**, **113**, **171**, **189**
Twinning Light **150**, **185**

U

Überwachung **32**, **55**, **78**, **89**, **93**, **111**, **113**, **122**, **128**
ULD-Innovationszentrum (ULD-i) **140**

V

Verbunddateien **33**
Verfahren **23**, **40**, **60**, **64**, **79**, **87**, **93**, **103**, **104**, **108**, **109**, **116**, **123**, **128**, **130**, **174**
Verfassungsschutz **29**, **31**, **40**
Verfügbarkeit **133**
Verhaltenskontrolle **79**, **93**, **121**
Verhältnismäßigkeit **29**, **32**, **35**, **45**, **47**
Verkehr **48**
Verschlüsselung **22**, **64**, **108**, **116**, **154**, **169**, **179**
Versicherungen **53**, **85**
Verwaltung **18**, **25**, **111**, **144**, **150**, **164**, **175**
Videoüberwachung **12**, **79**, **89**, **91**, **92**
Virtualisierung **177**
Virtuelles Datenschutzbüro **149**
Volkszählungsurteil **12**
Vorratsdatenspeicherung **37**, **40**, **41**, **64**, **145**

W

Warndatei **35**, **36**
Webcam **89**
Werbesendungen **96**
Werbezwecke **14**, **22**, **74**, **81**
Wirtschaft **73**
World Wide Web **117**, **186**

Z

Zahlungsinformationssystem für Agrarfördermittel (ZIAF) **123**, **161**, **196**
Zeitschriftenabonnements **88**
Zertifizierung **123**, **156**, **158**, **164**, **166**, **169**, **172**, **174**
Zugriffsrechte **113**
Zweckbindung **21**, **64**, **95**, **107**, **111**, **113**, **117**, **119**, **169**