DATENSCHUTZ
TÄTIGKEITSBERICHT
2012 / 2013

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

HmbBfDI

Hamburg

24. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit 2012 / 2013

Diesen Tätigkeitsbericht können Sie abrufen unter
www.datenschutz-hamburg.de

Vorgelegt im Februar 2014
Prof. Dr. Johannes Caspar
(Redaktionsschluss: 31. Dezember 2013)

Herausgegeben vom
Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit
Klosterwall 6 (Block C)
20095 Hamburg

Tel. 040-428 54 40 40
Fax 040-428 54 40 00
mailbox@datenschutz.hamburg.de

Auflage: 1.300 Exemplare
Layout: Kameko Design GbR, Fotos [redacted] Druck: Lütcke & Wulff, 20097 Hamburg

INHALTSVERZEICHNIS

VORWORT 8

I. EINLEITUNG – NEUE UND ALTE HERAUSFORDERUNGEN DES DATENSCHUTZES

1. Der Entwurf der EU-Datenschutzverordnung 13
2. Die Dialektik der Ausspähung 14
3. Die Entwicklung des Datenschutzes in Hamburg 17
   - 3.1 Eingabenzahlen 17
   - 3.2 Präventiv-Beratung 18
   - 3.3 Verwaltungsverfahren mit überregionaler Bedeutung 19
   - 3.4 Personelle Situation der Dienststelle – Im Norden nichts Neues 20
   - 3.5 Umstrukturierung der Dienststelle 21

II. INFORMATIONS- UND KOMMUNIKATIONSTECHNIK

1. Was heißt „Mandantenfähigkeit"? – eine Orientierungshilfe 26
2. Bring your own device (BYOD) - Outlook für mobile Geräte (DME Excitor) 28
3. Zugang über das Internet: Bereitstehende Sicherheitsmechanismen werden nicht genutzt 31
4. Keine Ende-zu-Ende-Verschlüsselung mehr bei E-Mails in der Hamburgischen Verwaltung 33
5. Einführung NGN in der FHH 34
6. Smart TV / HbbTV 37
7. Migration Datennetz und Anwendungen - Verfahrenskataster Polizei 39
8. Prüfung von Smartphone Apps 40
9. Speicherung von WLAN-Passwörtern bei Android Geräten 42

III. DATENSCHUTZ IM ÖFFENTLICHEN BEREICH

1. Polizei 46
   - 1.1 Auswertung der Protokolle von Zugriffen auf polizeiliche Dateien 46
   - 1.2 Ergänzung des PolDVG um Bestandsdatenabfrage 47
   - 1.3 Videoüberwachung der Polizeikommissariate nach Hausrecht 49
   - 1.4 Videoüberwachung von Fußballstadien durch die Polizei 50
   - 1.5 Eingaben zur Löschung von Daten in polizeilichen Dateien 52
   - 1.6 Ausländervereine 53
   - 1.7 Funkzellenabfragen 54
   - 1.8 Sicherheitsüberprüfungen bei Abschleppunternehmen 55
2. Verfassungsschutz 57
   - 2.1 Verdeckte Ortung über Mobilfunkeinrichtungen im Ausland 57
   - 2.2 BVerfG-Urteil zur Antiterrordatei und die Folgen 59
   - 2.3 Datenerfassung zur Werbung von V-Leuten 61
3. Justiz 62
   - 3.1 Übersendung von Anklageschriften an die Ausländerbehörde 62
   - 3.2 Auskunft an Betroffene über Ermittlungsdaten der Staatsanwaltschaft 63

III.

4. Strafvollzug 65
4.1 Neue Strafvollzugsgesetze 65
4.2 Beschwerden und Eingaben 66
5. Gesundheitswesen 68
5.1 Bußgeld wegen Altakten-Entsorgung durch Asklepios-Klinik 68
5.2 Neuer Behandlungsvertrag für die Asklepios-Kliniken 69
5.3 Beanstandung des UKE wegen Not-Zugriffsberechtigung 71
5.4 Änderungen der Gesetze zu psychischen Krankheiten und zum Maßregelvollzug 73
5.5 Mitteilung von Gutachten durch den MDK an die Krankenkassen 74
5.6 Externe Abrechnung und Bonitätsprüfung für Zahnärzte 76
5.7 Vereinbarung des HmbBfDI mit der Ethikkommission der Ärztekammer 78
5.8 Klinisches Krebsregister 79
5.9 Tierhalterregister 81
5.10 Veröffentlichung von Patientendaten im Internet (UKE) 82
5.11 Geburtsdaten-Übermittlung vom Standesamt an das Gesundheitsamt 83
5.12 Zugriff Kosmetikinstitut auf Arztpraxis-Software 84
5.13 Faxen von Arztbriefen 85
6. Sozialwesen 86
6.1 Frühe Hilfen – Babylotse 86
6.2 Obachtverfahren Gewalt u21 läuft ohne erforderliche Mandantentrennung 88
6.3 SDZ Harburg – „baulicher" Datenschutz 91
6.4 Datenerhebung durch Betreuungsbehörde 92
6.5 JUS-IT: Daten der Jugendämter wurden erneut nicht gelöscht 93
7. Schulwesen 96
7.1 Statistik in der Behörde für Schule und Berufsbildung 96
7.2 Nutzung sozialer Netzwerke zu schulischen Zwecken 99
7.3 IServ 100
7.4 Medienkompetenz – Hamburger Medienpass 101
7.5 Jugendberufsagentur - Datenschutzgerecht soll niemand verloren gehen 102
7.6 Landesmusikakademie Hamburg – Seminarverwaltung 104
7.7 Bildungs- und Betreuungsangebote an Schulen 105
7.8 Mittagessen, Biometrie und Einwilligungserklärung 107
7.9 Protokollierung der Abrufe aus dem ZSR 109
7.10 ichblickdurch.de 110
7.11 HBSC-Kids-Studie (UKE) 111
7.12 Hamburger Schulinspektion 112
7.13 Kommunikation bei Schulkonflikten 113
8. Forschung 114
8.1 Überblick über beratene Forschungsprojekte 114
9. Bauen, Wohnen, Umwelt 116
9.1 Luftbilder: Vereinbarung mit dem Landesbetrieb Geoinformation und Vermessung 116
9.2 Kamerafahrten durch Hamburgs Straßen 117

III.

10. Finanzwesen 119
10.1 Kultur- und Tourismustaxe 119
10.2 Ein Korruptionsregister zum Schutz des fairen Wettbewerbs 120
10.3 VoSystem zur Organisation der Vollstreckung in der Steuerverwaltung 122
10.4 Technische Überwachung der Spielbank Hamburg 124
11. Behördliche Datenschutzbeauftragte 126
11.1 Entwicklung 126
12. Verkehr 127
12.1 Projekt Deutschland online KFZ 127
12.2 Handyparken 129
12.3 Verkehrslenkung durch Videoüberwachung 131
12.4 Kamerafahrten zu Zwecken der Straßenunterhaltung 134
12.5 Videoüberwachung des Schiffsverkehrs 136
13. Hochschulwesen 137
13.1 Novellierung des Hamburgischen Hochschulgesetzes 137
13.2 Projekt Hochschulübergreifendes Identitätsmanagementsystem eCampus-IDMS 138
14. Wirtschaftsverwaltung 139
14.1 Videoüberwachung im Jagdwesen 139
15. Parlamentsangelegenheiten, Wahlen und Volksabstimmungen 141
15.1 Änderungen des Volksabstimmungsrechts 141
15.2 Vordrucke für die Beantragung von Briefwahlunterlagen 142
16. Bezirke 143
16.1 Datenverarbeitung bei der Ausschussarbeit der Bezirksversammlungen 143
16.1.1 Öffentliche Behandlung von Eingaben 143
16.1.2 Weitergabe personenbezogener Daten an Ausschüsse 145
16.1.3 Personenbeziehbarkeit bei der Beantwortung Großer und Kleiner Anfragen 146
16.2 Online-Übertragungen aus Sitzungen der Bezirksversammlungen 148
16.3 Videoüberwachung in öffentlichen Toiletten 151
17. Statistik 153
17.1 Registergestützte Volkszählung – Zensus 2011 153
17.2 Landesinformationssystem (LIS) 155
18. Personenstandswesen 157
18.1 Elektronisches Personenstandsregister 157
18.2 Prüfung der Standesamtlichen Registerstelle mit dem Generalregister der Hamburgischen Standesämter 159
19. Meldewesen 163
19.1 Was bringt das neue Bundesmeldegesetz? 163
20. Personalausweis- und Passwesen 165
20.1 Antragsverfahren für ePass und neuen Personalausweis endlich datenschutzgerecht 165
20.2 Dauerbrenner: Anforderung von Personalausweiskopien und Hinterlegungsverbot 167

IV. BESCHÄFTIGTENDATENSCHUTZ

1. Das ausgefallene Gesetzgebungsverfahren 172
2. Arbeitskreis Beschäftigtendatenschutz 173
3. Prüfung der Beschäftigtendatenverarbeitung mit SAP beim UKE 173
4. KoPers/ePers - Sachstand 174

V. TELEMEDIEN

1. Orientierungshilfe Soziale Netzwerke 178
2. Umsetzung der Cookie-Richtlinie 179
3. Do Not Track 182
4. Nutzung sozialer Netzwerke durch öffentliche Stellen 183
5. Nutzung Sozialer Netzwerke insbesondere Facebook durch die Polizei Hamburg 185
6. Google 187
   - 6.1 Verfahren gegen die Google Datenschutzbestimmungen 188
   - 6.2 Google WLAN Bußgeldverfahren 190
   - 6.3 Google Analytics 191
   - 6.4 Löschung von Suchergebnissen aus der Google Suchmaschine 193
7. Facebook 194
   - 7.1 Facebook Gesichtserkennung 195
   - 7.2 Fanpages und Social Plugins 196
   - 7.3 Graph Search 198
8. Xing – Auftragsdatenverarbeitung und CDN 199
9. Datenschutz und Online-Dating 200
10. Abgeordnetenwatch.de 201
11. Private Fahndung in Sozialen Netzwerken 203
12. Das Ausspähprogramm PRISM und die US-Diensteanbieter 205

VI. DATENSCHUTZ IM NICHT-ÖFFENTLICHEN BEREICH

1. Die Europäische Datenschutz-Grundverordnung 210
   - 1.1 Überblick 210
2. Internationaler Datenverkehr 214
   - 2.1 Auswirkungen von Prism 214
   - 2.1.1 Safe Harbor 215
   - 2.1.2 Standardvertragsklauseln 216
   - 2.1.3 Unternehmensregelungen 216
   - 2.2 Cloud Computing weltweit 217
   - 2.3 Fluggastdatenübermittlung 218
3. Kreditwirtschaft 218
   - 3.1 Kontaktloses Bezahlen mit Near Field Communikation (NFC) 218
4. Versicherungswirtschaft 220
   - 4.1 Bonitätsabfrage bei Krankenversicherungen 220
   - 4.2 Schadenklassedatei 222

VI.
4.3 Einwilligungs- und Schweigepflichtentbindungserklärung 223
4.4 Verhaltensregeln 224
5. Handel 225
5.1 Unzulässige Datenverarbeitung durch Versandhändler 225
5.2 Kundenkarte für Kinder und Jugendliche 228
6. Auskunfteien 229
6.1 Stichprobenverfahren 229
6.2 Umgang mit Schätzdaten 230
6.3 Hinweis auf Auskunfteimeldung 231
6.4 Benachrichtigung bei Übermittlung von Scorewerten 232
7. Transport und Verkehr 233
7.1 Ortungssysteme in Mietwagen 233
7.2 Datenverarbeitung durch Taxizentralen 234
7.3 Datenerhebung bei Ausgabe verbilligter Zeitkarten durch die Hamburger Hochbahn 236
8. Videoüberwachung 238
8.1 Videoüberwachung des öffentlichen Straßenraums 238
8.2 Videoüberwachung in und an Taxis 240
8.3 Videoüberwachung in einem Medizinischen Versorgungszentrum 241
9. Wohnungswirtschaft 242
9.1 Datenerhebung bei der Vermietung von Wohnraum – Informationsschrift für Vermieter und Mietinteressenten 242
9.2 Veröffentlichung von personenbezogenen Daten im Internet 244
9.3 Übermittlung von Kündigungsschreiben an öffentliche Stellen 245
10. Werbung 247
10.1 Der große E-Mail-Verteiler 247
10.2 Anwendungshinweise 248
11. Bußgeldfälle und Anordnungen 249
11.1 Übersicht 249
12. Meldepflicht und Prüftätigkeit 250
12.1 Bericht über durchgeführte Prüfungen 250
12.2 Meldepflicht nach § 42a BDSG 252
12.3 Register 253

VII. INFORMATIONEN ZUR DIENSTSTELLE
1. Eingabenstatistik 256
2. Presse- und Öffentlichkeitsarbeit beim HmbBfDI 257
3. Aufgabenverteilung 260

STICHWORTVERZEICHNIS 264

Vorwort

Der Berichtszeitraum 2012/2013 war geprägt von zwei grundlegenden Diskussionen, die gegenwärtig noch andauern und die vermutlich auch das nächste Jahr - wenn nicht sogar die nächsten Jahre - bestimmen werden.

Gemeint ist zum einen die Debatte um eine Neustrukturierung des Datenschutzes auf europäischer Ebene. Ausgehend von den Kommissionsentwürfen einer Europäischen Grundverordnung sowie einer Richtlinie zur Datenverarbeitung von Polizei und Justiz, die die Mitgliedstaaten zur Einhaltung bestimmter Mindestvorgaben in diesem Bereich verpflichten sollte, hat sich eine breite und äußerst vielschichtige Diskussion über die künftigen Grundlagen des Datenschutzes in Europa entwickelt.

Zum anderen geht es um die notwendigen Konsequenzen, die aus den Erkenntnissen einer millionenfachen und systematischen Überwachung der digitalen Kommunikation durch die Geheimdienste gezogen werden sollten. Auch hier ist kein Ende der Diskussion abzusehen, stehen doch Antworten auf drängende Fragen, die durch die Enthüllungen des ehemaligen US-Geheimdienstmitarbeiters Edward Snowden seit Juni 2013 offenbar wurden, nach wie vor aus.

Welche Regelungen künftig für den Schutz des informationellen Selbstbestimmungsrechts gegenüber privaten wie auch öffentlichen verantwortlichen Stellen gelten, hat ebenso wie die Frage nach Ausmaß und Grenzen einer nachrichtendienstlichen Überwachung direkten Einfluss auf die datenschutzrechtliche Situation für die Bürgerinnen und Bürger vor Ort. Die Welt der globalen Kommunikation rückt die Menschen immer enger zusammen. Sie eröffnet Chancen, aber auch Risiken: Dem Einzelnen ist die Teilhabe an der scheinbar grenzenlosen Welt der Kommunikation und des Wissens jederzeit möglich, während die rasante technologische Entwicklung und die Ökonomisierung von personenbezogenen Daten die digitalen Grundrechte des Individuums immer verletzlicher werden lassen. Fragen des Datenschutzes und der Datensicherheit

greifen auf weitere Anwendungsfelder des täglichen Lebens über. Die Komplexität steigt ständig. Dies ist auch der Grund dafür, dass der aktuelle Tätigkeitsbericht gegenüber dem Berichtszeitraum 2010/11 im Umfang erneut wesentlich zugelegt hat.

Mit der Abfassung von Berichten allein ist es jedoch nicht getan: Das Datenschutzrecht muss auch beachtet und durchgesetzt werden. Die Datenverarbeitung privater und staatlicher Stellen fordert daher einen immer größeren Aufwand nicht nur an datenschutzrechtlicher Kontrolle, sondern gerade auch an einer möglichst früh ansetzenden Beratung und Information sowohl der verantwortlichen Stellen als auch der betroffenen Bürgerinnen und Bürger.
Wir haben uns auch in diesem Berichtszeitraum bemüht, allen Anforderungen eines modernen Datenschutzes und allen Erwartungen, die nicht zuletzt von den vielen Bürgerinnen und Bürgern, die sich auch in diesem Zweijahreszeitraum hilfesuchend an uns gewendet haben, gerecht zu werden. Insoweit gilt mein besonderer Dank allen Mitarbeiterinnen und Mitarbeitern, die sich trotz steigender Anforderungen bei gleichzeitig defizitärer Personalausstattung diesen Aufgaben immer wieder aufs Neue gestellt haben.

Johannes Caspar
Februar 2014

I. EINLEITUNG NEUE UND ALTE HERAUSFORDERUNGEN DES DATENSCHUTZES

1. Der Entwurf der EU-Datenschutzverordnung 13
2. Die Dialektik der Ausspähung 14
3. Die Entwicklung des Datenschutzes in Hamburg 17

Die vergangenen beiden Jahre haben fundamentale Fragestellungen im Bereich des Datenschutzes aufgeworfen und das Verständnis über die Anforderungen an den Datenschutz tiefgreifend verändert. In den Berichtszeitraum 2012-2013 fällt zunächst die grundlegende Diskussion um die Schaffung eines neuen einheitlichen und kohärenten Datenschutzrechts innerhalb der EU. Braucht es eine einheitliche Datenschutzregelung, die in allen Mitgliedstaaten gleichermaßen gilt? Wie soll diese zentrale Regelung für einen Einzugsbereich von ca. einer halben Milliarde Menschen im Einzelnen aussehen? Hier geht es um die autonome Gestaltung des eigenen Rechtskreises, die angesichts einer rasanten Digitalisierung der Lebenswelt zum wirksamen Schutz der informationellen Selbstbestimmungsrechte von Bürgerinnen und Bürgern von zentraler Bedeutung ist.

Eher reaktiv sind die sich aus den seit Juni 2013 veröffentlichten Erkenntnissen des Whistleblowers und ehemaligen NSA-Mitarbeiters Edward Snowden ergebenden Handlungsfolgen. Die dokumentierte flächendeckende Ausspähung durch Nachrichtendienste westlicher Staaten stellt ein millionenfaches Außerkraftsetzen von Grundrechten dar – von Grundrechten, die eigentlich einen privaten Raum der freien Kommunikation der Bürgerinnen und Bürger garantieren sollten. Die Erkenntnisse erschüttern die Grundfeste des Systems demokratischer Rechts- und Verfassungsstaaten und stellen eine Zäsur dar, die zentrale Fragen aufwirft: Welche Reaktionen, welche politischen und rechtlichen Konsequenzen müssen ergriffen werden, um die digitalen Grundrechte des Einzelnen vor einem anlasslosen Zugriff durch Nachrichtendienste zu schützen? Wie kann die staatliche Schutzpflicht, Bürger nicht zu passiven Subjekten einer unkontrollierten und unverhältnismäßigen Ausspähung werden zu lassen, umgesetzt werden? Es bedarf hierauf schneller und konkreter Antworten, um die Glaubwürdigkeit rechtstaatlicher Garantien nicht auf Dauer zu beschädigen.

1. Der Entwurf der EU-Datenschutzverordnung

Seit die EU-Kommission im Januar 2012 den Entwurf einer Datenschutzgrundverordnung vorgelegt hat, wird über die Berechtigung einer künftigen Zentralisierung der Regelung im Umgang mit den persönlichen Daten durch private und öffentliche Stellen in der EU kontrovers diskutiert. Hierbei geht es um das derzeit wohl ambitionierteste Regelungsprojekt der Europäischen Union. Es enthält grundlegende Antworten auf die Frage, in welcher Weise europaweit künftig mit den wichtigsten Ressourcen der digitalen Gesellschaft – den personenbezogenen Daten der Bürgerinnen und Bürger – umgegangen werden darf. Das Grundverständnis der neuen unmittelbar geltenden Regelung zielt auf eine für alle Mitgliedstaaten einheitlich konzipierte Lösung. Im Grundsatz beabsichtigt die Neuregelung, die im nationalen Recht angelegte Trennung von Datenschutz im öffentlichen und im nicht-öffentlichen Bereich, für die in Deutschland sowohl das Bundesdatenschutzgesetz als auch die jeweiligen Landesdatenschutzgesetze gelten, künftig weitgehend aufzulösen.

Dass diese Vorschläge zunächst nicht nur Anhänger fanden, mag angesichts der großen praktischen Tragweite eines europaweiten Regelungsrahmens zum Umgang mit personenbezogenen Daten kaum überraschen. So kreiste die Diskussion im zurückliegenden Berichtszeitraum zunächst um grundsätzliche Fragestellungen wie die Einhaltung des Grundsatzes der Subsidiarität, die Folgen einer Zentralisierung des Datenschutzes für die deutschen Grundrechte sowie die Konsequenzen für den künftigen Rechtsschutz vor dem Bundesverfassungsgericht. Später verdichtete sie sich dann zusehends auf praktische Fragen: etwa auf die inhaltliche Ausgestaltung neuer Datenschutzregelungen auf EU-Ebene zur Verbesserung des Schutzes der Daten im Internet („Recht auf Vergessenwerden", „Privacy by Default" und „Privacy by Design") oder auf die neue Gestaltung des Zusammenwirkens der Aufsichtsbehörden als Voraussetzung dafür, dass die Regelungen von den Aufsichtsbehörden der Mitgliedstaaten auch einheitlich vollzogen werden („One-Stop-Shop"). Auf Kritik stieß insbesondere die Möglichkeit der Kommission, durch die Einfügung zahlreicher delegierter Rechtsakte die sehr allgemein gehaltenen Regelungen der Grundverordnung näher auszuformen. Die Steuerung wesentlicher, für das Grundrecht der informationellen Selbstbestimmung zentraler Fragestellungen – wie etwa der Einsatz von Videoüberwachung oder der Bereich des Scoring – durch Rechtsakte der Kommission würde, so die Befürchtung, den rechtsstaatlichen Legislativvorbehalt außer Kraft setzen (zu Einzelheiten s. VI 1.).

Nachdem der zuständige Ausschuss im Europäischen Parlament sich im Oktober 2013 nach mehreren tausend Änderungsvorschlägen unter dem Eindruck des Geheimdienstskandals und insbesondere der Erkenntnisse über die Ausspähung von Internet-Dienstanbietern (dazu noch im Folgenden unter 2.) auf eine gemeinsame Regelung verständigt hat, liegt die Verantwortung für den Fortgang des Verfahrens nun im Rat und damit bei den Mitgliedstaaten. Ob es gelingt, die intensiv geführte Diskussion auf den Weg zu einer künftigen EU-Datenschutzgrundverordnung im Verlauf der nächsten

Monate abzuschließen und damit noch vor der Wahl zum Europäischen Parlament Ende Mai 2014 eine Regelung zu verabschieden, erscheint derzeit überaus fraglich. Ein Grund hierfür ist sicherlich auch die nach wie vor abwartende Haltung der Bundesregierung. Trotz der hohen nationalen Bedeutung des Datenschutzes – jüngst wurde durch eine Studie ausgewiesen, dass knapp 70 % der Deutschen sich um den Schutz ihrer persönlichen Daten sorgen (GfK-Verein, Pressemitteilung vom 21. November 2013) – gehörte die deutsche Seite im Ministerrat eher zu den Kritikern der EU-Datenschutznovelle.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) hat sich in dem vergangenen Berichtszeitraum für eine moderne EU-Datenschutzverordnung eingesetzt, die an einem hohen Schutzstandard für den Datenschutz in der digitalen Gesellschaft ausgerichtet ist. Besonderes Augenmerk gilt dabei einem einheitlichen Vollzug des Rechts durch die unabhängigen Aufsichtsbehörden. Insbesondere wurde gefordert sicherzustellen, dass die Vereinheitlichung der Zuständigkeit auf die Behörde am Ort der Hauptniederlassung eines Unternehmens („One-Stop-Shop") nicht dazu führen darf, dass große Internetdienste in Mitgliedstaaten ausweichen, in denen die Behörden weniger streng über die Einhaltung der Datenschutzstandards wachen. Die wenig erfreulichen Erfahrungen, die im Berichtszeitraum gerade bei der unterschiedlichen Auslegung des EU-Rechts im Zusammenhang mit der Einführung der automatischen Gesichtserkennung durch Facebook gesammelt wurden (s. dazu unter V 7.1), gaben Anlass, entsprechende Verfahrensreglungen im Aufsichtsbereich zu fordern, damit sich künftig keine „Datenschutzwüsten" für datenverarbeitende Unternehmen in Europa ergeben. Ein Selbsteintrittsrecht der Datenschutzaufsichtsbehörden ist für den Fall erforderlich, dass die zuständige federführende Behörde am Ort der Niederlassung nicht oder nicht hinreichende Maßnahmen zur Kontrolle und Überwachung der verantwortlichen Stellen erlässt.

Im Rahmen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich der HmbBfDI im Berichtszeitraum in drei Entschließungen für einen starken Datenschutz auf europäischer Ebene mit eingebracht (Entschließung vom 21./22. März 2012, „Ein hohes Datenschutzniveau für Europa"; Entschließung vom 7./8 März 2012, „Europäische Datenschutzreform konstruktiv und zügig voranbringen!"; Entschließung vom 13. März 2013, „Europa muss den Datenschutz stärken").

2. Die Dialektik der Ausspähung

Die Veröffentlichung der Dokumente des damaligen Geheimdienstmitarbeiters und Whistleblowers Edward Snowden haben seit Juni 2013 immer wieder neue Facetten von Überwachungspraktiken durch westliche Nachrichtendienste aufgedeckt, die im Maßstab moderner Rechts- und Verfassungsstaaten sowohl qualitativ als auch quantitativ nicht vorstellbar waren. Die aufgezeigte Dimension der Überwachung leitet für

den Datenschutz einen erneuten Paradigmenwechsel ein. Dieser kann mit einer Entwicklung vom Überwachungsstaat zur Überwachungsgesellschaft hin zur internationalen entgrenzten Überwachung durch Geheimdienste im Rahmen eines dialektischen Prozesses beschrieben werden.

Die 1980er Jahre waren im Wesentlichen vom Misstrauen gegenüber einem Nationalstaat geprägt, der seine Bürgerinnen und Bürger vermehrt durch staatliche Datensammlung ausspähte, was sich paradigmatisch an der Diskussion um die aus der heutigen Perspektive doch vergleichsweise eher harmlose Volkszählung entzündete. Das Volkszählungsurteil von 1983, das in 2014 nunmehr 30 Jahre Bestand hat, war Geburtsstunde einer verfassungsrechtlichen Entfaltung des Datenschutzes in der nationalen Rechtsordnung. Im Urteil zur Volkszählung liegt letztlich der Identitätskern aller datenschutzrechtlichen wirksamen Ansätze – selbst gegen in Gesetzesform gegossene Überwachungsregelungen und -praktiken einer staatlichen Datenverarbeitung. Das Grundrecht der informationellen Selbstbestimmung hat gerade auch durch die technisch-organisatorische Implementierung datenschutzrechtlicher Verfahren seinen Siegeszug in die Verwaltung in Bund und Ländern angetreten.

Seit Beginn der 2000er Jahre setzt dann eine unübersehbare Entwicklung hin zur Überwachungsgesellschaft ein. Ursache hierfür ist zum einen eine massive Digitalisierung der Lebenswelt, die die Möglichkeiten des Speicherns und Übermittelns von Daten exponentiell ansteigen ließ. Die neuen Möglichkeiten der Informations- und Kommunikationstechnologie sind wohl Katalysatoren für eine Form der kommunikativen Freiheit des Individuums. Gleichzeitig erweist sich der digitale Fortschritt aber auch als Entstehungsgrund von Risikotechnologien für die Privatsphäre. Zum anderen ergibt sich seither ein klarer Trend hin zu einer Ökonomisierung von personenbezogenen Daten. Daten werden mittlerweile als Eintrittskarten in der Welt der vermeintlichen Gratiskultur im Internet zu immer wichtigeren ökonomischen Ressourcen. Der Datenschutz gerät dadurch stärker in die Defensive. Die umfassende wirtschaftliche Nutzung von personenbezogenen Daten führt wiederum zu einer weiteren Beschleunigung der technischen Innovationen und verstärkt damit die Dynamik der Entwicklung hin zu einer Überwachungsgesellschaft.

All dies dokumentiert sich spürbar in den Eingaben von Bürgerinnen und Bürgern, die sich seit einigen Jahren in der Masse nicht mehr gegen öffentliche, sondern vermehrt gegen private Akteure als verantwortliche Stellen richten. Ausführlich wurde diese Entwicklung bereits im 22. Tätigkeitsbericht dargestellt (TB 2008/2009, S. 2). Sie war Anlass für den damals vom HmbBfDI entwickelten Entwurf eines modernen, auf drei Module gestützten Datenschutzkonzepts (unmittelbare sowie mittelbare Steuerung und Förderung der individuellen Datenschutzkompetenz). Der derzeitige Berichtszeitraum unterstreicht erneut, dass der Trend zur Überwachungsgesellschaft nach wie vor ungebrochen ist (dazu VII 1.).

Die jüngst bekannt gewordene Internationalisierung des Überwachungszusammenhangs durch Geheimdienste stellt eine Synthese der vorangegangenen Entwicklungslinien dar: Zum einen bleibt auch die nachrichtendienstliche Überwachung im Kern eine staatliche Überwachung. Diese ist jedoch ihrer Ausrichtung nach entgrenzt und ihrer Struktur nach einer demokratisch-transparenten Kontrolle nur noch bedingt zugänglich. Die Spionagetätigkeit in der digitalen Welt wird durch die technische Infrastruktur begünstigt, mit der die Privatsphäre der Individuen immer verletzlicher geworden ist. Gegenstand der Überwachung sind die unbescholtenen Bürgerinnen und Bürger selbst geworden, deren Kommunikation verdachtsunabhängig und anlasslos einer gigantischen Rasterfahndung unterschiedlicher Geheimdienste unterzogen wird, die ihre Daten gegenseitig austauschen. Die Zugriffe auf den digitalen Datenstrom durch Programme wie X-Keyscore und Tempora machen es möglich, Daten an Internetknotenpunkten in Echtzeit zu erfassen. Darüber hinaus eröffnet das Programm Prism den US-Geheimdiensten die Möglichkeit, auf die gesammelten Nutzerdaten der US-Internetdienste zurückzugreifen und damit auch in tiefer liegende Schichten der Vergangenheit der Nutzer durch Auswertung der Datenmengen bei den Providern selbst vorzudringen.

Das Ergebnis der Entwicklung muss zu einer politischen Auseinandersetzung mit dem gegenwärtigen System flächendeckender anlassloser Überwachung und zu einer Neubewertung aller Bemühungen um einen künftig effizienten Schutz der Daten und der Privatsphäre führen. Das Telekommunikationsgeheimnis gewährleistet nach Auffassung des Bundesverfassungsgerichts die freie Entfaltung der Persönlichkeit durch einen „privaten, vor den Augen der Öffentlichkeit verborgenen Austausch von Nachrichten, Gedanken und Meinungen (Informationen) und wahrt damit die Würde des denkenden und freiheitlich handelnden Menschen." (Beschluss vom 20. Juni 1984, 1 BvR 1494/78, Rn 43). Diese zentrale Freiheitsgewährleistung ist derzeit unter massiven Druck geraten.

Hier hat sich eine Entwicklung vollzogen, die eine enorme Herausforderung an den Datenschutz stellt. Um künftig die Bürgerinnen und Bürger vor einer unverhältnismäßigen massenhaften Ausspähung – und damit auch die digitalen Grundrechte – zu schützen, sind mehrstufige Handlungsebenen zu betreten: Es gilt, die Datensicherheit zu verbessern, um Zugriffen von außen zu begegnen; ein Trend, der leider an der FHH gegenwärtig vorbeizulaufen scheint (dazu s. noch unter II.). Die Diskussion sollte sich aber nicht nur auf die sicherheitstechnische Verbesserung von IT beziehen, sondern auch auf die Entwicklung von Alternativ-Angeboten wie den Aufbau eines datenschutzfreundlichen Internetangebots, wie Suchmaschinen und soziale Netzwerke auf nationaler bzw. europäischer Ebene. Insbesondere sollte geprüft werden, ob nicht auch die Angebotspalette öffentlich-rechtlicher Rundfunkanstalten in diese Richtung zu stärken ist.

Daneben bedarf es eines Zusammenwirkens von politischen Initiativen in Richtung auf

essentielle Verbesserungen des Datenschutzes auf nationaler, EU- sowie auf internationaler Ebene. Neben einer Reform der Kontrollverfahren, einer stärkeren Transparenz sowie einer rechtsstaatlichen Überprüfung der nationalen Nachrichtendienste, dem Abschluss von internationalen Abkommen sowie völkerrechtlichen Regelungen für einen verbesserten Datenschutz gehört schließlich auch das Projekt einer gemeinsamen Datenschutzordnung Europas zu einer Kernforderung gerade für den Schutz von europäischen Nutzern der US-Internetdienste. Nur wenn die EU als einheitlicher Datenschutzakteur auftritt, lässt sich ein Gegengewicht aufbauen, mit dem erfolgreich einem anlasslosen und massenhaften Ausspähen durch die US-Regierung entgegengetreten werden kann.

Die Datenschutzbeauftragten des Bundes und der Länder haben jüngst in drei Entschließungen auf die Probleme der internationalen Dimension der Überwachung aufmerksam gemacht, auf eine bestehende Schutzpflicht des Staates für die digitalen Grundrechte seiner Bürgerinnen und Bürger hingewiesen und auf Aufklärung und notwendige Konsequenzen hingewiesen (Entschließung vom 5. September 2013, „Keine umfassende und anlasslose Überwachung durch Nachrichtendienste; Entschließung vom 1. Oktober 2013, „Handlungsbedarf zum Datenschutz im Bereich der öffentlichen Sicherheit in der 18. Legislaturperiode des Deutschen Bundestags"; „Forderungen für die neue Legislaturperiode: Die Datenschutzgrundrechte stärken!"). Der HmbBfDI unterstützt mit Nachdruck den Kurs der Datenschutzkonferenz und setzt sich für eine nachhaltige Stärkung der digitalen Grundrechte auf allen politischen Ebenen ein.

3. Die Entwicklung des Datenschutzes in Hamburg

3.1 Eingabenzahlen

Im Verlauf des Berichtszeitraums hat sich eine Konsolidierung der Eingabenzahlen auf einem recht hohen Niveau von über 1000 Eingaben pro Jahr ergeben. Als Eingaben werden alle schriftlich per Post, E-Mail oder Telefax eingehenden, nicht dagegen mündliche Beschwerden von Bürgerinnen und Bürgern gewertet. Im Jahr 2012 waren 1.098 schriftliche Eingaben bei der Dienststelle zu verzeichnen, 2013 waren es 1.047.

Im Vergleich zum Referenzzeitraum des 23. Tätigkeitsberichts, insbesondere für das Jahr 2010, ist die Zahl der Eingaben allerdings rückläufig. Der signifikante Anstieg im Jahr 2010 auf 1687 Eingaben war jedoch im Wesentlichen darauf zurückzuführen, dass bundesweit Beschwerden zum Widerspruchsverfahren der Bürgerinnen und Bürger gegenüber Abbildungen bei Google Street View eingingen. Der HmbBfDI war hierfür zuständige Stelle, da Google seine deutsche Hauptniederlassung in Hamburg hat.

Die Arbeitslast der Dienststelle liegt auf einem für alle Mitarbeiter dauerhaft nur schwer leistbaren Niveau. Das ist letztlich auch darauf zurückzuführen, dass sich die gestiegenen Komplexitätsanforderungen des Datenschutzes gerade im qualitativen

Bereich der Bearbeitung auswirken. Zudem haben sich Anforderungen an die datenschutzgerechte Begleitung von IT-Projekten öffentlicher Stellen in den letzten Jahren wesentlich erhöht. Gleiches gilt für die zahlreichen datenschutzrechtlichen Beratungen im Bereich der Abstimmung von Senatsdrucksachen sowie im Zuge von geplanten Gesetzesänderungen.

3.2 Präventiv-Beratung

Eine möglichst frühzeitige Beteiligung des HmbBfDI ist nicht nur für die Datenschutzbehörde, sondern auch für die kontrollierten verantwortlichen Stellen anzustreben. Eine präventiv ansetzende Beratung macht es möglich, wesentliche Defizite bereits auf einer ersten Verfahrensstufe festzustellen und Umsteuerungsmaßnahmen zu ergreifen, bevor Beanstandungen ausgesprochen, Anordnungen erlassen oder Bußgeldverfahren eingeleitet werden. Gleichzeitig wird auf Seiten der verantwortlichen Stelle eine stärkere Vertrauensbasis für die Umsetzung der jeweiligen Projekte und damit auch mehr Rechtssicherheit geschaffen.

Die Begleitung von IT-Projekten und Vorhaben öffentlicher Stellen anlässlich von Lenkungsgruppensitzungen oder anderweitiger pro-aktiver Einbindung hat sich im Zuständigkeitsbereich des HmbBfDI in der Vergangenheit bewährt. Diese Erfahrungen sollten künftig auch in stärkerem Maße für nicht-öffentliche Stellen nutzbar werden. Der HmbBfDI unterstützt daher nachdrücklich das aktuelle Forschungsvorhaben des Hans-Bredow-Instituts unter Beteiligung des Amts für Medien der Senatskanzlei. Dessen Ziel ist es u.a., neue Wege der mittelbaren Steuerung vor dem Hintergrund eines regulatorischen Dialogs zwischen Datenschutzaufsicht und den nicht-öffentlichen verantwortlichen Stellen am Beispiel der Unternehmen der Internetbranche auszuloten.

Im Rahmen eines an alle Akteure versandten Fragebogens und eines danach durchgeführten Praktiker-Workshops „Dialog zwischen Datenschutzaufsicht und Unternehmen der Internet-Branchen" fand eine umfassende empirische Bestandsaufnahme über Kommunikationsstrukturen zwischen Vertretern der Internetunternehmen, u.a. Google und Facebook, AOL, Xing sowie Beratern und Rechtsanwälten einerseits und den Vertretern der Aufsichtsbehörden andererseits statt. Hier wurde aus den unterschiedlichen Perspektiven erörtert, wie Verbesserungen im Bereich der Datenschutzaufsicht durch eine stärkere begleitende Beratung bei Projektentwicklungen erreicht werden können. Die Ergebnisse über die Befragungen zur gegenseitigen Wahrnehmung der teilnehmenden Organisationen waren durchweg interessant und fielen z.T. auch überraschend aus. Die wissenschaftliche Auswertung der Ergebnisse durch das Hans-Bredow–Institut wird mit Spannung erwartet.

Das bereits im Rahmen des 22. Tätigkeitsberichts entwickelte Konzept „Hamburger Datenschutz 2010" weist drei Module einer modernen Datenschutzaufsicht auf: Neben der unmittelbaren behördlichen Steuerung und dem Selbstdatenschutz Betroffe-

ner gehört die Weiterentwicklung und Optimierung des Instruments der mittelbaren Steuerung zum Gegenstand moderner Rechtskultur. Durch eine selbstverantwortliche Beteiligung von datenverarbeitenden Unternehmen sollen Reibungsverluste vermieden werden, die sich durch ein ausschließlich auf ordnungsrechtliche Maßnahmen und ein auf nachfolgende gerichtliche Klärung verwiesenes Modul der hierarchischen Steuerung häufig ergeben.

Insoweit könnte die Stärkung der Möglichkeiten einer aktiven Beratung von verantwortlichen Stellen durch die Aufsichtsbehörden durchaus Win-Win-Effekte herbeiführen. Dies gilt umso mehr, als gerade im zurückliegenden Berichtszeitraum Maßnahmen und Projekte verantwortlicher Stellen ohne hinreichende Kommunikation mit den Aufsichtsbehörden eingeführt wurden, was dann im weiteren Verlauf zu langwierigen Prüfverfahren mit Beanstandungen führte und in aufsichtsbehördliche Verfahren mündete.

3.3 Verwaltungsverfahren mit überregionaler Bedeutung

Als besonders arbeitsintensiv erwies sich im Berichtszeitraum die Kontrolle von global agierenden Internetkonzernen, deren deutscher Hauptsitz sich in Hamburg befindet. Ein umfangreiches Verwaltungsverfahren hatte die Einführung der automatischen Gesichtserkennung durch Facebook ohne ausdrückliche Zustimmung der Nutzer zum Gegenstand. Dieses bereits im Jahr 2011 eingeleitete Verfahren führte zu dem Erlass einer verwaltungsrechtlichen Anordnung sowie entsprechender Aktivitäten anderer nationaler Aufsichtsbehörden, die zum Teil mit entsprechenden Anhörungsschreiben ebenfalls selbstständige Verwaltungsverfahren gegen Facebook eröffneten (dazu ausführlich unter V. 7.1).

Umfänglich und komplex gestaltete sich ebenfalls das Verwaltungsverfahren gegen die Google Inc. wegen der von Google im März 2012 in Kraft gesetzten neuen Privatsphärebestimmungen. Diese berechtigen Google zu einer umfassenden Zusammenführung der von Nutzern bei den einzelnen Diensten hinterlassenen Daten und ermöglichen die Erstellung von Megaprofilen (näher zum Verfahren unter V 6.1). In der hierfür durch die Artikel 29 Datenschutzgruppe der EU gebildeten Task Force ist neben den Aufsichtsbehörden aus Frankreich, England, den Niederlanden, Spanien und Italien der HmbBfDI als zuständige nationale Aufsichtsbehörde vertreten und übernimmt die erforderliche Koordination mit den Aufsichtsbehörden der Länder. Die Gespräche mit Vertretern von Google sowie den anderen Aufsichtsbehörden haben im Verlauf der letzten Monate erhebliche personelle Ressourcen gebunden.

Beide Verfahren zeigen, dass eine vorgeschaltete Kommunikation mit den Aufsichtsbehörden die Unternehmen in die Lage versetzt hätte, die geplanten Maßnahmen einer realistischen datenschutzrechtlichen Risikoeinschätzung zu unterziehen. Soweit die Unternehmen daher nicht bereits von Anfang an entschlossen waren, die Neuerungen auch gegen den Widerstand der europäischen bzw. nationalen Aufsichtsbehörden

durchzusetzen, hätte ein kooperativ gestaltetes Verfahren hier durchaus dazu beitragen können, förmliche Verwaltungsverfahren zu verhindern.

3.4 Personelle Situation der Dienststelle – Im Norden nichts Neues

Im Wesentlichen hat sich in den letzten Jahren an der Personalausstattung des HmbBfDI leider wenig geändert. Die personelle Situation der Dienststelle ist seit 2002 trotz eines enormen Bedeutungszuwachses des Datenschutzes in Staat und Gesellschaft und eines stetig ansteigenden Arbeitsaufwands rückläufig (siehe Anlage zum 23. Tätigkeitsbericht, Datenschutz, Fakten, Zahlen, Daten, Abbildung 2). Die befristete Beschäftigung von vier externen Mitarbeitern mit insgesamt 3,1 Stellenanteilen (davon zwei Stellen durch Rückkehr von Asklepios) konnte die Personalengpässe etwas abmildern, aber nichts an dem strukturellen Ausstattungsdefizit ändern.

Dass mittlerweile 2,0 Stellenanteile von diesen externen Stellen in den eigenen Stellenplan aufgenommen wurden, ist bestenfalls eine kosmetische Korrektur: Eine Stelle wird Ende 2013, die andere Stelle im Verlauf von 2014 wegen Eintritts in den Ruhestand ersatzlos wegfallen. Gleichzeitig wurde für den Doppelhaushalt 2013/2014 dem HmbBfDI eine Sparquote von 15.000 Euro auferlegt, die jährlich aus dem Personalhaushalt zu erbringen ist.

Unter dem Strich wurden dem HmbBfDI 14,7 Stellen für den Bereich des Datenschutzes zugewiesen. Weitere 2,0 Stellen stehen ihm für den Bereich der Informationsfreiheit zur Verfügung. Die Personalengpässe im Bereich des Datenschutzes wurden dadurch etwas kompensiert, dass in den vergangenen Jahren Stellenanteile aus dem Bereich der Informationsfreiheit insbesondere zur Behandlung der komplexen Internet- und Social Media-Fragestellungen zum Datenschutz verlagert wurden. Parallel zu den höheren Anforderungen im Datenschutzbereich ergibt sich seit der Verabschiedung des Hamburgischen Transparenzgesetzes Mitte 2012 gleichzeitig eine Verschärfung der Arbeitsbelastung im Bereich der Informationsfreiheit: Hamburg ist mit dem neuen Transparenzgesetz im Informationsfreiheitsbereich Vorreiter unter den Bundesländern. Die steigende Bedeutung der Transparenz für die öffentliche Verwaltung hat sich im letzten Jahr deutlich in den Eingaben nach dem Hamburgischen Transparenzgesetz niedergeschlagen: Auf diesem Gebiet sind mittlerweile die Eingaben durch Bürgerinnen und Bürger um 350 % gestiegen (vgl. Informationsfreiheitsbericht 2012/2013).

Die Personalengpässe im Datenschutzbereich werden immer stärker auch bei der täglichen Arbeit bemerkbar: So ist mittlerweile ein Rückgang der anlassunabhängigen Prüfungen verantwortlicher Stellen im nicht-öffentlichen Bereich, aber auch im öffentlichen Bereich, wo diese ebenfalls kaum stattfanden, zu verzeichnen. Gleichzeitig wurde das Vorhaben einer flächendeckenden Befassung und nachträglichen Auswertung der von öffentlichen Stellen betriebenen Videoüberwachungsanlagen nach § 30 HmbDSG eingestellt und stattdessen eine Prüfung nur noch in besonderen Bereichen durchgeführt. Für

die private Videoüberwachung fällt es zunehmend schwer, den zahlreichen Anzeigen von Bürgerinnen und Bürgern nachzukommen. Die notwendigen Vorortkontrollen, rechtlichen Bewertungen und der Vollzug durch Bußgeld- und Verwaltungsverfahren sind überaus arbeitsintensiv und mit dem gegenwärtigen Personalbestand in der Menge der Fälle kaum mehr zu leisten. Dies zeigt auch die Tatsache, dass es immer schwerer fällt, komplexere Bußgeldverfahren zu einem Abschluss zu bringen. Zwar ist die Eingabenzahl gegenüber dem Zeitraum 2010-2011 rückläufig, komplexe IT-Verfahren, die wir z.T. über Jahre begleiten, binden jedoch in erheblichem Maße personelle Kapazitäten.

Es wird darauf hingewiesen, dass zur Wahrung der Unabhängigkeit des Datenschutzbeauftragten, die nach der Rechtsprechung des EuGH gemäß der EU-Datenschutzrichtlinie sicherzustellen ist, auch eine für die Aufgabenerfüllung angemessene personelle und sachliche Ausstattung erforderlich ist. Der Hamburgische Beauftragte hat in der Vergangenheit wiederholt auf Personaldefizite hingewiesen. Dies hat leider keinen Erfolg gehabt. Für den Doppelhaushalt 2015/2016 wird der HmbBfDI daher die aus seiner Sicht mindestens erforderlichen Personalbedarfe Anfang 2014 im Haushaltsverfahren anmelden.

3.5 Umstrukturierung der Dienststelle

Um die Nutzung der knappen personellen Ressourcen künftig zu optimieren, aber auch um die Organisation der Dienststelle den Praxisbedürfnissen anzupassen und eine effizientere Struktur einzuführen, wird ab 1.1.2014 ein veränderter Zuschnitt der Referate in der Dienststelle umgesetzt. Die ohnehin kaum trennscharfe formelle Unterscheidung zwischen einer Zuständigkeit für öffentliche Stellen (bisher Referat D 4) und einer Aufsichtsbehörde, die nach § 38 BDSG für nicht-öffentliche Stellen zuständig ist (Referat D 5), wird aufgegeben. Eine Zuordnung unter der Kategorie öffentlich/privat war bereits in der Vergangenheit etwa im Bereich des Gesundheitswesens (bisher ausschließlich D 4), aber auch im Bereich des Beschäftigtendatenschutzes (bisher ausschließlich D 5), letztlich ohnehin nicht konsequent durchzuhalten. Die Referate werden daher nach Maßgabe sachlicher Gesichtspunkte in die Referate Sicherheit, Demokratie und Daseinsvorsorge (künftig D 4) und Wirtschaft und Finanzen (künftig D 5) integriert.

Dem Gebot einer effizienteren Arbeitsorganisation folgend, die künftig auch eine interne Vertretungssituation ermöglicht, wurde der Bereich Informationsfreiheit mit der Videoüberwachung zusammengelegt (Referat D3). Damit ist sichergestellt, dass es eine zentrale Kompetenz für den gesamten Bereich der Videoüberwachung gibt, für den bisher eine wenig überzeugende Zuständigkeitstrennung in öffentliche und nichtöffentliche verantwortliche Stellen zugrunde lag.

Eine besondere Herausforderung des Datenschutzes stellt seit einigen Jahren der Bereich der Telemediendienste dar, die immer stärker den Alltag prägen und immer größere Nutzerzahlen an sich binden. Hamburg ist als moderner Medienstandort nicht

nur Standort für bekannte Internetdienste wie z.B. Google, Facebook, AOL und Xing, sondern auch für viele innovative Start-Up-Unternehmen, die ihre Dienstleistungen über das Internet anbieten. Bereits in der Vergangenheit hat sich ein hoher Arbeits- und Beratungsaufwand für sowohl technische als auch juristische Grundsatzfragen ergeben, die immer wieder den bisherigen Zuschnitt der Referate durchbrachen. Gerade die Nutzung von Telemedien durch öffentliche Stellen brachte es mit sich, dass die bisherige Zuständigkeitstrennung sehr komplexe, allerdings einheitlich zu beantwortende Fragen aufwarf, die durch zwei unterschiedliche Referate zu beantworten waren. Um die damit verbundenen Reibungsverluste aufzufangen, wird künftig für alle Fragestellungen mit dem Schwerpunkt „Telemedien" ein neues Referat, in dem juristischer und technischer Sachverstand gebündelt sind, geschaffen. Das bisherige Technikreferat wird jedoch nicht aufgelöst und in die anderen Referate integriert, sondern bleibt in zunächst verkleinerter Form bestehen und soll auch künftig in die Beratung und Prüfung eingebunden werden.

Unter dem Strich soll die Organisationsveränderung mit einem zusätzlichen Referat eine Verkleinerung der Verwaltungseinheiten bringen, die damit flexibler auf die unterschiedlichen datenschutzrechtlichen Herausforderungen reagieren können. Dies kann allerdings insbesondere dort Schwierigkeiten verursachen, wo der Aufgabenumfang bereits durch die mangelnde personelle Ausstattung derzeit kaum bewältigt werden kann. Im Sinne einer Abwägung der für und gegen eine Umstrukturierung sprechenden Argumente hat schließlich der Gesichtspunkt eines effizienten und den Datenschutzherausforderungen angemessenen Organisationsaufbaus einer modernen Datenschutzbehörde den Ausschlag gegeben.

I.

INFORMATIONS- UND KOMMUNIKATIONSTECHNIK II.

1. Was heißt „Mandantenfähigkeit"? – eine Orientierungshilfe 26
2. Bring your own device (BYOD) - Outlook für mobile Geräte (DME Excitor) 28
3. Zugang über das Internet: Bereitstehende Sicherheitsmechanismen werden nicht genutzt 31
4. Keine Ende-zu-Ende-Verschlüsselung mehr bei E-Mails in der Hamburgischen Verwaltung 33
5. Einführung NGN in der FHH 34
6. Smart TV / HbbTV 37
7. Migration Datennetz und Anwendungen - Verfahrenskataster Polizei 39
8. Prüfung von Smartphone Apps 40
9. Speicherung von WLAN-Passwörtern bei Android Geräten 42

1. Was heißt „Mandantenfähigkeit"? – eine Orientierungshilfe

Die Datenschutzbeauftragten des Bundes und der Länder haben datenschutzrechtliche Anforderungen bei der Nutzung gemeinsamer IT-Infrastrukturen fixiert.

Zur Zentralisierung und Konsolidierung verteilter Datenverarbeitung sowie aus Kostengründen greifen Daten verarbeitende Stellen zunehmend auf kooperative Betriebsmodelle zurück, die die gemeinsame Nutzung von Systemen und Programmen zur automatisierten Verarbeitung personenbezogener Daten vorsehen. Die gemeinsame Nutzung einer solchen Infrastruktur unterliegt erhöhten Anforderungen an die Trennung der personenbezogenen Daten, um die aus der gemeinsamen Nutzung entstehenden Risiken für die informationelle Gewaltenteilung, die Zweckbindung und Vertraulichkeit hinreichend zu reduzieren. Die Datenschutzgesetze der Länder und des Bundes fordern, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben worden sind, getrennt voneinander verarbeitet werden. Die getrennte Verarbeitung betrifft sowohl die Speicherung als auch die Verarbeitungsfunktionen wie etwa Datenbanktransaktionen oder Datensatzbuchungen.

Aus wirtschaftlichen oder praktikablen Gründen kann es aber sinnvoll sein, dass Ressourcen wie Hard- und Software, also IT-Infrastrukturen, für verschiedene voneinander zu trennende Datenbestände gemeinsam genutzt werden. In begründeten Fällen kann auch eine gemeinsame Speicherung mit mandantenbezogener Kennzeichnung der Daten zulässig sein. Voraussetzung hierfür ist, dass die Daten mandantenbezogen geführt und Verarbeitungsfunktionen, Zugriffsberechtigungen und Konfigurationseinstellungen je Mandant eigenständig festgelegt werden können. Die Datenverarbeitung muss dabei zwingend durch technische Maßnahmen getrennt voneinander erfolgen. Insbesondere gilt das auch dann, wenn für die jeweiligen Daten unterschiedliche Stellen verantwortlich sind oder es sich bei den personenbezogenen Daten um besondere Arten personenbezogener Daten handelt.

Da der Begriff des „Mandanten" schillernd ist und weder eine allgemein anerkannte Definition noch eine detaillierte Festlegung der datenschutzrechtlichen Anforderung vorlag, die bei der Nutzung gemeinsamer IT-Infrastrukturen einzuhalten sind, um ein Verfahren rechtskonform zu betreiben, haben die Datenschutzbeauftragten des Bundes und der Länder die „Orientierungshilfe Mandantenfähigkeit" erarbeitet, die im Oktober 2012 vom Arbeitskreis Technik einstimmig verabschiedet und im November 2012 von der Datenschutzkonferenz zustimmend zur Kenntnis genommen wurde.
In dieser Orientierungshilfe, die in unserem Internetangebot unter www.datenschutz-hamburg.de abrufbar ist, werden fünf Prüfschritte benannt, die bei einer Mandantentrennung zu beachten sind:

▶ Prüfschritt 1: Rechtliche Grundlagen

Auf der Grundlage insbesondere der jeweiligen spezialgesetzlichen Regelungen muss in diesem Prüfschritt geklärt werden, ob es eine Ermächtigungsbefugnis gibt, durch welche ggf. auch eine gemeinsame Verarbeitung (gemeinsame und verbundene automatisierte Dateien) zugelassen werden dürfte, ob von dieser Gebrauch gemacht wurde oder ob gar eine Nutzung gemeinsamer Infrastrukturen explizit ausgeschlossen ist.

▶ Prüfschritt 2: Ausgestaltung von Übermittlungen zwischen Mandanten

Die rechtlichen Grundlagen und Anforderungen an die Zulässigkeit der Übermittlung und die Form ihrer Durchführung sind vorab zu prüfen. Wenn die Übermittlung von Daten eines Mandanten an einen anderen zulässig ist, muss diese Übermittlung technisch über definierte Schnittstellen zwischen diesen Mandanten umgesetzt werden.

▶ Prüfschritt 3: Abgeschlossenheit der Transaktionen innerhalb eines Mandanten

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

▶ Prüfschritt 4: Unabhängigkeit der Konfiguration

Eine ausreichende Mandantentrennung setzt voraus, dass die Zugriffsberechtigungen, die Verarbeitungsfunktionen und die Konfigurationseinstellungen je Mandant eigenständig festgelegt werden.
Die Berechtigungsvergabe muss über ein auf Ebene des einzelnen Mandanten abgeschlossenes Berechtigungssystem erfolgen. Hierzu ist sicherzustellen, dass eine mandantenübergreifende Berechtigungsvergabe auf Anwendungsebene weder aus den einzelnen Mandanten heraus noch durch die mandantenübergreifenden Funktionen zur Verwaltung der einzelnen Mandanten möglich ist. Ein Nutzer muss somit zu genau einem Mandanten und darf nicht zu mehreren zugeordnet sein.

▶ Prüfschritt 5: Beschränkung der mandantenübergreifenden Verwaltung der Datenverarbeitung

Mandantenübergreifende Funktionen zur Verwaltung der Mandanten und der gemeinsam genutzten Infrastruktur dürfen grundsätzlich keine Verarbeitung personenbezogener Daten eines Mandanten ermöglichen. Die mandantenübergreifende Verwaltung muss revisionssicher protokolliert werden. Diese Protokolle müssen auch bei einer Prüfung einzelner Mandanten genutzt werden können. Mandantenübergreifende Datenzugriffe sind nur in begründeten Ausnahmefällen zulässig und nur im für die jeweilige Aufgabenstellung erforderlichen Umfang, insbesondere für die mandantenübergreifende Verwaltung und zur Beseitigung von Notfallsituationen, wenn andere

Maßnahmen mit geringeren Zugriffsrechten nicht ausreichend sind. Die Vergabe der hierfür vorgehaltenen Rollen ist sehr restriktiv zu handhaben, und diese Rollen dürfen nicht Nutzern auf Anwendungsebene zugeordnet werden.

Diese Anforderungen an die Mandantenfähigkeit sind regelhaft bei Prüfungen und Beratungen als Bewertungsmaßstab zugrunde zu legen. Es ist zu erwarten, dass diese Thematik gerade bei einem IT-Dienstleister wie Dataport, der von mehreren Bundesländern getragen wird, eine verstärkte Bedeutung erlangen wird. Wenn vergleichbare Anforderungen von verschiedenen Daten verarbeitenden Stellen, auch solcher aus verschiedenen Bundesländern, an Dataport herangetragen werden, ist der Ansatz naheliegend, dafür eine gemeinsame IT-Infrastruktur zu nutzen. Datenschutzgerecht kann dieses nur erfolgen, wenn die aufgezeigten Prüfschritte von den Daten verarbeitenden Stellen detailliert berücksichtigt werden.

2. Bring your own device (BYOD) - Outlook für mobile Geräte (DME Excitor)

Auch die Stadt möchte sich dem Trend der Zeit nicht verschließen. Mobile Geräte, bei denen Sicherheit nicht erstes Designprinzip ist, werden zur Datenverarbeitung auch bei hohem Schutzbedarf genutzt.

Eher beiläufig erfuhren wir von den ersten Versuchen, die seit 2007 in der hamburgischen Verwaltung zur Verfügung stehende Möglichkeit E-Mails, Termine und elektronischen Dokumente auf ein dienstliches BlackBerry-Gerät weiterzuleiten, zu ergänzen. Von einer „App" für das iPhone war die Rede, von Zugriffen auf dienstliche Daten wie mit der BlackBerry-Lösung, aber eben auf einem Gerät, das primär für den Consumer-Markt konzipiert ist.

Die neue Umsetzung des „Outlook für mobile Geräte" in der FHH mit der aus Dänemark stammenden Lösung „DME Excitor" wird durch den Dienstleister Dataport realisiert. Technisch betrachtet werden die Daten in einem verschlüsselten Container auf dem Smartphone oder Tablet gehalten. Das genutzte Gerät kann ein dienstliches oder auch ein privates sein.

Diese neue technische Lösung greift den BYOD-Trend auf. „Bring your own device" bedeutet das private Gerät für dienstliche Aufgaben zu nutzen. Der Mitarbeiter nutzt sein vertrautes Smartphone und kann jederzeit an dienstlichen Themen teilhaben, ohne dafür ein zweites Gerät dabei haben zu müssen. Der Arbeitgeber muss keine Hardware stellen. Ein Gewinn für Alle?

Die Befassung mit dem Thema machte schnell klar, dass dieses Verfahren viele Aspekte hat. Die Datenschutzbeauftragten des Bundes und der Länder haben zu diesem Trend in einem Workshop rechtliche wie technische Aspekte erörtert und verfolgen das Ziel, zu einer abgestimmten Wertung zu kommen.

Ein gravierender Aspekt bei der Nutzung privater Geräte ist es, dass eine Beschränkung der installierten Anwendungen sichergestellt werden kann, so wie dies bei der BlackBerry-Lösung der Fall war. Dort konnten nur explizit von der Finanzbehörde freigegebene Apps genutzt werden. Nun stehen unzählige Apps der bekannten App-Stores mit den damit verbundenen Sicherheitsrisiken zur Verfügung (vgl. II. 9). Auch ist eine Trennung von Administration und Nutzung bei privaten Geräten nicht realisiert.

Seit Juli 2012 wird diese Lösung zunächst für iPhones genutzt. Obwohl mit dieser neuen Lösung zahlreiche datenschutzrechtliche Risiken verbunden sind, wurden wir erst kurz vor dem Produktionsstart eingebunden. Zentrale Unterlagen bekamen wir erst kurz nach Produktionsstart und selbst das Sicherheitskonzept befand sich noch in der Abstimmung innerhalb der Finanzbehörde.

Seit April 2013 bietet die FHH diese Lösung auch für androidbasierte Geräte an. Die bestehende Blackberry-Lösung für den Betrieb dienstlicher Geräte wird es ab 2014 nicht mehr geben. Ein Übergang der Nutzer auf DME Excitor ist vorgesehen, der parallele Betrieb der BlackBerry-Server wäre nicht wirtschaftlich. Ob es dann noch viele dienstliche Geräte geben wird, bleibt abzuwarten.

Die DME-Lösung stellt sicher, dass die Daten, die immer als Kopie aus der Exchange-Installation auf das mobile Gerät übertragen werden, auf dem gesamten Weg verschlüsselt sind und auch auf dem mobilen Gerät verschlüsselt gespeichert werden. Wir konnten erreichen, dass die Finanzbehörde klare Regeln für die Nutzung durch die Mitarbeiter festlegt.

Leider gibt es verschiedene offene Punkte, die sicherheitskritisch sind:

- In der Risikoanalyse wird der Schutzbedarf zu niedrig angesetzt. Da innerhalb der hamburgischen Verwaltung auch E-Mails mit hohem Schutzbedarf verschickt werden, gelangen diese auch auf die privaten Geräte. Die technischen und organisatorischen Maßnahmen müssen sich daran ausrichten.

- Zentrale Schutzmaßnahme der DME-Lösung ist die Nutzung eines Containers, der die dienstlichen Daten von den anderen Nutzungen, die auf dem Smartphone laufen, isolieren soll. Wie sicher diese Trennung in der Praxis ist, lässt sich nur in einem Penetrationstest (Praxistest der Verfahrenssicherheit mit realen Angriffsszenarien durch ein beauftragtes IT-Sicherheitsunternehmen) feststellen. Schon bei erster Nutzung wurde zumindest deutlich, dass auch Daten aus dem privaten

Telefonbuch des Smartphones in den Container hineingelangen. Ein solcher Datenfluss sollte nach der Beschreibung jedoch gar nicht möglich sein. In unserer Stellungnahme haben wir gegenüber der Finanzbehörde deutlich gemacht, dass ein solcher Penetrationstest aufgrund des hohen Schutzbedarfs gerade bei dieser Lösung durchgeführt werden sollte.

- Bei Smartphone-Nutzung ist es weit verbreitet, dass Backup- oder Cloudservices genutzt werden. Auf diesem Weg könnten Unberechtigte Zugriff auf dienstliche Daten nehmen (vgl. II. 9). Eine Überprüfung der Wirksamkeit von Maßnahmen zur Verhinderung von solchen Datenabflüssen ist dringend geboten.

- Die Nutzung eines Mobile Device Management (MDM) zur zentralen Kontrolle der Endgeräte für dienstliche Geräte zur Sicherstellung der Richtlinien-Konformität entspricht nach Ansicht des Bundesamtes für Sicherheit in der Informationstechnik dem Stand der Technik. Es ist nicht nachvollziehbar, warum dieses nicht bei der FHH zum Einsatz kommt.

- Insbesondere für Wartung der Geräte durch externe Dritte bedarf es einer festgelegten Regelung, damit auf diesem Weg der Dienstleister keinen Zugriff auf die dienstlichen Daten nehmen kann. Eine Löschung der Daten des Containers sollte daher erfolgen, bevor das Gerät zur Wartung oder Reparatur aus der Hand gegeben wird.

- Um die DME-App für Android-basierten Geräte aus dem App-Store beziehen zu können, muss ein Account bei Google angelegt werden. Auch bei der Nutzung von dienstlichen Geräten könnten auf diese Weise Mitarbeiter-Daten bei der Registrierung diesem Dienstleister übermittelt werden. Es sollte umgehend eine Registrierung ohne Nutzung persönlicher Daten des Mitarbeiters vorgesehen werden.

Grundsätzlich schätzt der HmbBfDI den Einsatz von privaten Geräten für dienstliche Aufgaben unter den heutigen besonderen Gefahren für mobile Endgeräte als sehr risikoreich ein.

Die Nutzung in der FHH stellt hohe Anforderungen an den verantwortungsvollen Umgang mit Daten und Geräten durch die Beschäftigten und die Dienststellen als Daten verarbeitende Stellen.

Die Verarbeitung von Daten mit möglicherweise hohem Schutzbedarf nach dem realisierten Konzept erfordert umfangreiche technisch-organisatorische Maßnahmen.

Auf den Endgeräten erfolgt eine Verarbeitung von Daten mit normalem und hohem Schutzbedarf. Die eingesetzten Geräte unterliegen einer Vielzahl von Angriffsvektoren, sind von der Architektur nicht für das Business-Segment konstruiert und als handlicher

Freizeitbegleiter einem erhöhten Verlustrisiko ausgesetzt. Nach Ansicht des HmbBfDI ist mit den bisher dokumentierten Betrachtungen des Risikos und den vorgesehenen technischen und organisatorischen Maßnahmen das IT-Verfahren nicht datenschutzgerecht zu betreiben. Die Restrisiken überschreiten das tolerierbare Maß bei weitem. Insbesondere sollte ein umfassender Penetrationstest durchgeführt werden. Von den dabei erzielten Ergebnissen wäre auch abzuleiten, ob über die Nutzung des MDM und der weiteren vom HmbBfDI aufgezeigten Maßnahmen hinaus noch zusätzliche Maßnahmen erforderlich sind, um zu einer datenschutzgerechten Lösung zu gelangen.

3. Zugang über das Internet: Bereitstehende Sicherheitsmechanismen werden nicht genutzt

Ein Penetrationstest zeigt serverseitig zwar keine gravierenden Mängel auf. Schwachstelle bleibt jedoch das private Endgerät, auf dem dienstliche Daten verarbeitet werden.

Mit dem IT-Verfahren Zugang von extern (Zuvex) wird eine Infrastrukturkomponente bereitgestellt, mit der ein Zugriff auf IT-Verfahren im FHH-Netz über das Internet ermöglicht wird (vgl. 23. TB II. 2.). Für diesen Zugriff können sowohl dienstliche als auch private Endgeräte eingesetzt werden. Zuvex soll zwei Nutzergruppen zur Verfügung stehen: Mitarbeitern der FHH, die bereits über einen FHHNET Account verfügen und Mitarbeitern bzw. Dritten, die einen Zugriff aus dienstlichem Interesse der FHH oder zur Erfüllung dienstlicher Aufgaben der FHH aufgrund von Rechtsvorschriften benötigen und noch kein Zugangskonto besitzen.

Der Zugriff erfolgt über ein Sicherheitsgateway, das Microsoft Forefront Unified Access Gateway (UAG). Als erste Anwendung wurde der Zugriff auf die FHHportal-Infrastruktur (SharePoint 2010) ermöglicht. Die Finanzbehörde hat in der Risikoanalyse dargelegt, dass Zuvex für die Nutzung von Daten mit normalem und mit hohem Schutzbedarf ausgelegt ist. Bevor jedoch mit Zuvex ein Zugriff auf Anwendungen mit Daten mit „hohem" Schutzbedarf ermöglicht wird, ist zu prüfen, ob die bereits getroffenen Maßnahmen ausreichend oder ggf. weitere zu ergreifen sind. Für Anwendungen mit Daten mit „sehr hohem" Schutzbedarf ist ein Zugriff über Zuvex nicht vorgesehen.

Da mit Zuvex ein weiterer Zugang zum FHH-Netz geschaffen wurde, haben wir uns dafür eingesetzt, vor der Einführung von Zuvex mit einem Penetrationstest das Sicherheitsniveau der eingesetzten Systeme zu bestimmen und Schwachstellen zu identifizieren. Wir begrüßen es ausdrücklich, dass ein externer Sicherheitsdienstleister diese Tests im Auftrag der Finanzbehörde durchgeführt hat. Auch das Ergebnis ist erfreulich,

da beim Zielsystem aus UAG und FHHPortal insgesamt nur wenige und davon keine hoch-kritischen Schwachstellen gefunden wurden.

Als Schwachpunkt der realisierten Lösung verbleibt jedoch das Gerät, mit dem über das Internet zugegriffen wird. Dieser Aspekt war nicht Gegenstand des durchgeführten Penetrationstests. Es werden von der Finanzbehörde keine technischen Vorgaben für das zugreifende Medium gemacht. Da alleine Benutzerkennung und Passwort zur Authentisierung herangezogen werden, kann ein Zugriff mit allen internetfähigen Geräten erfolgen. Neben PC und Laptop kann somit auch ein Zugriff über Smartphones erfolgen. Da auch explizit private Geräte zulässig sind, kann nicht von einer bestimmten Konfiguration und einem Mindeststand an vorhandenen Sicherheitsmaßnahmen ausgegangen werden. Um die Risiken zu verringern, dass die Daten, die im Zuge eines Zugriffes auf diesem Gerät verarbeitet werden, von unberechtigten Dritten missbraucht werden, hat Microsoft für solche UAG-Lösungen mit dem Modul „Endgerätekontrolle" eine technische Lösung bereitgestellt, mit der vor einer Übertragung von Inhaltsdaten automatisiert geprüft werden kann, ob auf diesem Gerät wenigstens eine Firewall und ein aktuelles Virenschutzprogramm läuft. Die Finanzbehörde hat jedoch entgegen ersten Planungen insbesondere aus Performancegründen entschieden, auf eine technische Endgerätekontrolle völlig zu verzichten. Stattdessen muss sich der Nutzer nur verpflichten, entsprechende Sicherheitsmaßnahme zu treffen. Ob dies geschieht, kann so in keiner Weise kontrolliert werden. Da wir eine erhebliche Gefahr sehen, dass durch unerkannte Schadsoftware auf dem privaten Gerät dienstliche Daten kompromittiert werden können, halten wir zumindest die Nutzung einer solchen Endgerätekontrolle für erforderlich. Gerade vor dem Hintergrund, dass Zuvex auch für Daten mit hohem Schutzbedarf genutzt werden kann, sollten aber auch am Markt verfügbare technische Alternativen geprüft werden, mit denen etwa ein Zugriff von einem privaten Gerät nur aus einer gesicherten und abgeschotteten Umgebung heraus erfolgen kann.

Zur Authentisierung werden alleine Benutzerkennung und Passwort benötigt. Eine starke Authentisierung, wie sie insbesondere bei Daten mit hohem Schutzbedarf gefordert wird, kann mit diesen Mechanismen nicht erreicht werden. Dafür wäre eine Zwei-Faktor-Authentisierung mit Besitz und Wissen z.B. mit einer Chipkarte eine anforderungsgerechte Umsetzung: man könnte sich am PC dann nur anmelden, wenn man sowohl eine entsprechende Chipkarte in den Kartenleser am PC einsteckt als auch sein Passwort eingibt. Bei Zuvex wird nicht nur auf die Zwei-Faktor-Authentisierung verzichtet, sondern zusätzlich kommt bei der realisierten Lösung hinzu, dass für Mitarbeiter der FHH die behördeninternen Zugangsdaten genutzt werden. Der Mitarbeiter muss sich also bei Zuvex mit dem gleichen Passwort anmelden, das auch bei der Anmeldung am Arbeitsplatz-PC genutzt wird. Die Auswirkungen eines möglichen Missbrauchs eines ausgespähten Passwortes gehen somit weit über die in Zuvex bestehenden Möglichkeiten hinaus. Man könnte sich nämlich mit diesem Passwort an einem Arbeitsplatz-PC der FHH anmelden und hätte Zugang zu allen IT-Verfahren, für die der ausgespähte Mitarbeiter berechtigt wäre, auch solche, die

nicht über Zuvex erreichbar sind.

Als weiterer Schwachpunkt der Lösung haben wir aufgezeigt, dass dieses Passwort während der Zuvex-Session im UAG in Klarschrift vorgehalten wird. Ein Auslesen durch die Administratoren wäre möglich.

Kurz vor Redaktionsschluss wurde bekannt, dass über Zuvex nun auch von außen auf dienstlichen Mails und Kalenderdaten zugegriffen werden kann, die in der FHH-internen Exchange-Anwendung verarbeitet werden. Da dienstliche Mails auch Daten mit hohem Schutzbedarf enthalten können, können diese besonders schutzwürdigen Daten somit über Zuvex auf die privaten Geräte gelangen. Daher teilen wir nicht die von der Finanzbehörde vorgenommene Wertung, die den Schutzbedarf der Anwendung mit „normal" bewertet. Hierzu werden wir in 2014 die Gespräche mit der Finanzbehörde fortsetzen.

Aus unserer Sicht sind die verbleibenden Sicherheitsrisiken insbesondere beim Zugriff auf Daten mit hohem Schutzbedarf zu groß und es sollte daher nach alternativen technischen Lösungen gesucht werden.

4. Keine Ende-zu-Ende-Verschlüsselung mehr bei E-Mails in der Hamburgischen Verwaltung

Wegen gravierender Mängel an der extra beauftragten Verschlüsselungslösung kommt diese nicht zum Einsatz. Der Schutz der sensiblen Daten bleibt somit auf der Strecke.

Bis 2010 war die E-Mail-Welt innerhalb der FHH „noch in Ordnung": Mails mit sensiblen personenbezogenen Daten konnten mit wenigen Klicks so verschlüsselt werden, dass sie auf der gesamten Übertragungsstrecke verschlüsselt waren und nur der Empfänger sie öffnen konnte. An mehreren tausend Arbeitsplätzen der FHH war diese Technik der „Erweiterten Sicherheit" ausgerollt.

Im Berichtszeitraum hat sich die Finanzbehörde jedoch dafür entschieden, den E-Mailverkehr innerhalb des FHH-Netzes zukünftig auch dann nicht mehr mit einer Ende-zu-Ende-Verschlüsselung zu schützen, wenn sich darin sensible personenbezogene Daten befinden. Dies bedeutet, dass sensible Daten unverschlüsselt auf den E-Mail-Servern verbleiben, wo sie den Gefährdungen z.B. durch gezielte Angriffe ausgesetzt sind. Auch können sich Administratoren im Falle einer Datenpanne kaum noch gegen den Vorwurf schützen, unberechtigt auf die sensiblen Inhalte zugegriffen zu haben.

Hintergrund dieses Rückschrittes ist, dass mit der Umstellung auf die aktuelle Mail-Server-Version die „Erweiterte Sicherheit" von Microsoft nicht mehr zur Verfügung gestellt wurde. Überraschend war die Entscheidung dennoch, da die Finanzbehörde nach intensiver Diskussion mit uns ein Zusatzprodukt in Auftrag gegeben hat, das die so entstandene Lücke schließen sollte (vgl. 23. TB II 4.). Dieses Software-Modul des Rights Management Systems (RMS) erwies sich jedoch in der Pilotanwendung als nicht praxisgerecht. Insbesondere wurden E-Mail-Anhänge, die keinem Microsoft-spezifischen Format entsprechen, nicht verschlüsselt. Dies führte zu der kuriosen Situation, dass selbst PDF-Dokumente, dem Standard-Format der elektronischen Akte in der hamburgischen Verwaltung, nicht verschlüsselt wurden. Statt jedoch die mangelnde technische Umsetzung an die Praxisanforderungen anzupassen, wurde die Nutzung des Produktes RMS für die zahlreichen Arbeitsplätze, an denen sensible personenbezogene Daten verarbeitet werden, ad acta gelegt.

Gerade vor der bundesweit in der Öffentlichkeit geführten Diskussion um die Anforderungen an einen gesicherten elektronischen Datenaustausch, die begann, als das Abhören des E-Mail-Verkehrs durch ausländische Geheimdienste bekannt wurde, ist diese veränderte Haltung der Finanzbehörde unverständlich und nicht zeitgemäß.

Als Reaktion auf die gerade aktuellen Gefährdungslagen und Herausforderungen der Datensicherheit bedarf es der Bereitstellung anwenderfreundlicher technischer Komponenten, um einen möglichst umfassenden Schutz elektronischer Daten zu gewährleisten. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder verabschiedete dazu die Entschließung „Sichere elektronische Kommunikation gewährleisten – Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln". Neben den in der Entschließung behandelten bundesweiten Kommunikationsprozessen sollte die Ende-zu-Ende-Verschlüsselung auch innerhalb des Netzes der FHH verbindlich als Sicherheitsstandard zugrunde gelegt werden. Die anforderungsgerechte Weiterentwicklung und Einführung des RMS-Softwaremoduls wäre ein wichtiges Signal, dass sich die FHH den Herausforderungen der Cybersicherheit stellt und hierfür angemessene Sicherheitsmaßnahmen umsetzt.

5. Einführung NGN in der FHH

Die Dienststellen der FHH werden auf internetbasierte Telefonie (Voice over IP, kurz: VoIP) umgestellt. Die neue Technologie und die neuen Telefongeräte werfen datenschutzrechtliche Fragen auf.

Wie in der Wirtschaft und im privaten Bereich findet auch bei der Freien und Hansestadt Hamburg (FHH) ein Umstieg von den bisherigen analogen Telefonen bzw. ISDN-Anlagen hin zu internetbasierender Telefonie statt. Um der Bedeutung und Neuartig-

keit des Wandels Rechnung zu tragen, erhielt das Projekt den Namen „Next Generation Network", kurz „NGN". Es soll dadurch ein „Netzwerk der nächsten Generation" realisiert werden. „Internetbasierend" bedeutet in diesem Fall, dass die Gesprächsdaten nicht mehr über klassische Telefonleitungen laufen, sondern über das interne Netzwerk der Stadtverwaltung, über welches auch die Arbeitsplatz-PCs miteinander verbunden sind. Dabei werden spezielle Telefongeräte eingesetzt, welche die Stimmen der Gesprächspartner digital erfassen, blitzschnell in Datenpakete umsetzen und diese über das Netzwerk versenden. Es wird somit Sprache per Internet-Protokoll verschickt. Von der englischen Beschreibung „Voice over Internet Protocol" leitet sich auch der heute für diese Technologie gängige Name „Voice over IP" bzw. kurz „VoIP" ab.

Im Privatbereich ist Voice over IP durch Programme wie z.B. Skype längst verbreitet. Und genau wie Privatpersonen Skype nutzen, um günstig über das Internet anstatt über teure Telefonanbieter zu kommunizieren, liegt auch für die FHH einer der Vorteile in der Senkung der Gesprächskosten. Zusätzliche Telefonkabel oder raumfüllende Telefonanlagen sind ebenfalls nicht mehr erforderlich und sorgen für weitere Einsparungen. Zur technischen Versorgung eines Arbeitsplatzes genügt zukünftig ein Netzwerk-Anschluss, der ohnehin in nahezu allen Dienststellen der FHH vorhanden ist.

Da die FHH mehrere tausend Telefonapparate an unterschiedlichsten Standorten im Einsatz hat, wurde der Prozess der Umstellung des Telefonsystems auf NGN seit 2007 geplant und umfassend vorbereitet. Auch der HmbBfDI war frühzeitig eingebunden. Eine unserer Kernforderungen bestand darin, dass das VoIP-System eine verschlüsselte Übertragung der Sprachdaten bietet – ein wichtiger Punkt, der bereits in der Ausschreibung berücksichtigt werden muss, da nicht alle Hersteller von VoIP-Systemen dies anbieten oder unterschiedliche Aufpreise hierfür fordern (vgl. 22. TB II. 3.). Die Umsetzung der Verschlüsselung wurde entsprechend 2011 von der Lenkungsgruppe des Projekts beschlossen („Die Risikoanalyse aus 2009 hat weiterhin Bestand – der Einsatz von Verschlüsselung für den Sprachdienst ist zwingend erforderlich", 23. Sitzung), dann jedoch unter Verweis auf die erwarteten Kosten für diese Maßnahme von ca. 1 Mio. Euro (bei einem Gesamtbudget des NGN-Projekts von ca. 34 Mio Euro) nicht realisiert.

Der Planungs- und Beschaffungsprozess für das NGN-System lief seinen geordneten Weg und ab 2012 wurde mit dem Roll-Out begonnen, d.h. die neuen VoIP-Telefone gelangten auf die Schreibtische der Mitarbeiter. Zu der Freude über die fortschrittliche Technik – viele Mitarbeiter hatten an ihren Telefonen erstmalig Displays zur Anzeige von Rufnummern - kamen jedoch schnell kritische Stimmen, vor allem zum Thema Datenschutz. Denn die Geräte der „nächsten Generation" bieten Möglichkeiten, deren datenschutzrechtliche Tragweite selbst wir nicht in allen Einzelheiten vorausgeahnt hatten.

Durch Erfahrungen in der eigenen Dienststelle, aber auch durch kritische Meldungen

der behördlichen Datenschutzbeauftragten, wurde schnell klar, dass an der „schönen neuen Telefonwelt" noch einige Korrekturen nötig sind.

Dies betrifft beispielweise die (Rufjournale), in denen ein- und ausgehende Anrufe automatisch im Telefon protokolliert wurden. Diese pauschale längerfristige Speicherung und zur Verfügungstellung für den Nutzer des Telefonapparates ist nach der aktuell gültigen Rahmenvereinbarung mit den gewerkschaftlichen Spitzenverbänden nach § 94 HmbPersVG und der Telekommunikationsrichtlinie der Stadt Hamburg nicht zulässig. Diese Funktion kann jedoch an jedem Apparat ausgeschaltet werden. Dies müssen die einzelnen Dienststellen veranlassen.

Bedenken erzeugt auch die Gruppenschaltung, bei der eingehende Anrufe bei mehreren Mitarbeitern angezeigt werden. Hierbei gelangen Rufnummern von Gesprächspartnern auch den Kollegen im Team zur Kenntnis. Was vor allem in Bereichen kritisch ist, in denen Anrufer oder angerufene Personen Diskretion und besondere Vertraulichkeit erwarten und zugesichert bekommen. Beispielsweise in sozialen Einrichtungen oder bei Mitarbeitern mit Sonderaufgaben wie Personalräten oder Datenschutzbeauftragten.

Die Liste der „kritischen" Funktionalitäten wuchs schnell an und konnte in Zusammenarbeit mit der zuständigen Stelle, der Finanzbehörde als zentralem Auftraggeber für das VoIP-System, weitgehend abgearbeitet werden. Ein unerwarteter Höhepunkt trat ein, als uns bekannt wurde, dass die Verschlüsselung der Sprachkommunikation, die ja Bestandteil der Ausschreibung war, in dem nun umgesetzten System doch nicht realisiert ist. Ein entsprechender Beschluss der Lenkungsgruppe zum Verzicht auf die Verschlüsselung sei jedoch „nicht schriftlich fixiert" worden, ferner hatte die Finanzbehörde in einer internen Risikoabschätzung den Verzicht auf die Verschlüsselung angesichts der Mehrkosten als vertretbar eingestuft. Der HmbBfDI teilt diese Einschätzung nicht, da das Telefonsystem der FHH damit eine massive Schwachstelle aufweist und aufgrund der ungeschützten Übertragung aller Kommunikationsinhalte Dienststellen mit besonderen Vertraulichkeitsanforderungen wie Sozial- und Gesundheitsbehörden oder Justiz und Gerichte somit nicht über die NGN-Telefone kommunizieren dürften.

Die für die IT-Infrastruktur zuständige Finanzbehörde sollte – nicht zuletzt vor dem Hintergrund der umfassenden Abhöraktivitäten durch Geheimdienste – die ihr obliegende Pflicht zum Schutz des Grundrechts auf Integrität und Vertraulichkeit informationstechnischer Systeme ernst nehmen, den Mitarbeitern der FHH Kommunikationssysteme an die Hand zu geben, die nach dem aktuellen Stand der Technik als „sicher" einzustufen sind. Das NGN-System ohne Verschlüsselung ist dies definitiv nicht.

6. Smart TV / HbbTV

Die neuen Flachbild-Fernseher sparen Platz und Energie und bringen mehr Komfort. Sind sie „smart", machen sie den Zuschauer im Gegenzug oft gläsern.

In immer mehr Wohnzimmern hat die gute alte „Röhre" ausgedient und wurde durch einen schicken Flachbildfernseher ersetzt. Von denen gibt es - neben einfachen Modellen, die weiterhin nur das klassische Fernsehsignal wiedergeben – auch Geräte mit Zusatzfunktionen wie Zugang zu Online-Videotheken oder sozialen Netzwerken. Möglich wird dies durch Anbindung des Fernsehers an das Internet. Ähnlich wie im Mobilfunkbereich mit den Smartphones hat sich für TV-Geräte mit Internetzugang die Bezeichnung „Smart-TV" etabliert.

Wie bei anderen „smarten" Geräten auch, entstehen dem Benutzer Vorteile in Form zusätzlicher Verwendungsmöglichkeiten und durch mehr Komfort und Bequemlichkeit, da das Gerät sich den Nutzergewohnheiten anpasst und „mitdenkt". Genau darin liegt jedoch die Schattenseite vieler smarter Technologien: damit ein Gerät sich auf die Benutzer einstellen kann, erfasst es systematisch ihre Nutzungsgewohnheiten und legt ein Nutzerprofil an. Dieses wird im Gerät gespeichert und im Laufe der Nutzung immer umfangreicher. Gelangt das Gerät dann ans Internet, wird das gespeicherte Nutzerprofil in vielen Fällen an den Gerätehersteller oder an Dritte übermittelt. Als Argument dafür dient entweder die Verbesserung der Produkt- oder Servicequalität oder auch - ganz offen – die Verwendung zu Werbezwecken.

Konsumenten sollten daher bei der Kaufentscheidung für smarte Geräte nicht nur auf die vordergründigen Funktionen achten, sondern auch berücksichtigen, welchen (unsichtbaren) Mehrpreis sie eventuell bezahlen, weil sie Dritten ihr persönliches Nutzungsverhalten preisgeben.

Smart-TVs bergen noch eine weitere und bislang kaum kritisch hinterfragte Möglichkeit zum Ausspähen des Zuschauers, speziell seiner Sehgewohnheiten. Die Basis hierfür bietet der sog. „HbbTV"-Standard, der von immer mehr Fernsehgeräten unterstützt wird. Die Abkürzung „HbbTV", die viele vielleicht schon einmal beim eigenen Fernseher gelesen haben, steht für „Hybrid broadcast broadband TV". Dahinter steht eine Technologie, die Fernsehen und Internet miteinander verbindet. Dabei wird über das Fernsehbild eine unsichtbare Webseite gelegt, auf der TV-Sender oder andere Dienstanbieter die Möglichkeit haben, direkt im TV-Bild an beliebigen Stellen Informationen aus dem Internet einzublenden. Es wird damit Interaktivität möglich. So lassen sich beispielweise Auswahl-Menüs oder Verweise auf weiterführende Inhalte darstellen, die der Zuschauer über spezielle Funktionstasten auf seiner Fernbedienung anwählen kann. Dies funktioniert im Prinzip genauso, wie wenn im Internet mit der Maus auf einen Link oder ein Bild geklickt wird.

Diese Vereinigung von TV- und Internet-Technologie ermöglicht jedoch auch, dass Erfassungsmethoden, mit denen Internet-Surfer heute fast überall im Netz identifiziert und verfolgt werden, nun in die Fernsehwelt gelangen. Während den meisten Internetnutzern heute beispielsweise bewusst ist, dass es „Cookies" gibt - kleine Textdateien, die von Webseiten auf den eigenen Rechner übertragen werden und anhand derer der Nutzer anschließend von Webseiten identifiziert und wiedererkannt werden kann - ist bislang kaum bekannt, dass diese Technologie auch bei Smart-TV-Geräten eingesetzt wird. Nur mit dem Unterschied, dass der Benutzer dort kaum Möglichkeiten hat, angesammelte Cookies wieder zu löschen oder deren Einsatz ganz zu untersagen. Solche Funktionalitäten sind in den unsichtbaren Web-Browsern der Smart-TV-Geräte noch kaum vorhanden.

So kann es vorkommen, dass ein Zuschauer sich mit jedem angesehen TV-Sender unbemerkt ein Cookie „einfängt", welches dauerhaft in seinem TV-Gerät gespeichert bleibt und ihn für diesen Sender zukünftig identifizierbar macht. Als Konsequenz kann genau verfolgt werden, wann der Zuschauer erneut diesen Sender einschaltet oder wann und wohin er umschaltet. Solche Nutzungsdaten sind für Fernsehsender und Medienkonzerne sehr wertvoll, vor allem wenn sie in Echtzeit und auf Sekundenbasis anfallen. Für die Erfassung des TV-Konsums haben sich mittlerweile senderübergreifende Analysenetzwerke gebildet, die systematisch das Nutzungsverhalten der Zuschauer erfassen. Teilweise stehen dahinter die gleichen Anbieter wie bei den Analysediensten für normale Webseiten. So kommt beispielsweise auch hier Google Analytics zum Einsatz (vgl. 23. TB. IV. 4.1).

Ein Zuschauer kann diese Verfolgung seiner Sehgewohnheiten momentan nur verhindern, indem er sein Smart-TV-Gerät konsequent „offline" betreibt, d.h. es nicht an das Internet anschließt.

Im Jahr 2013 wurden wir angefragt, weil ein bekannter Hersteller von Unterhaltungselektronik, der auch eine Niederlassung in Hamburg hat, seine Kunden dazu „zwingt", ihr Smart-TV-Gerät an das Internet anzuschließen. Ansonsten steht die Möglichkeit für TV-Aufnahmen oder zeitversetztes Sehen (sog. „Time Shift") nicht zur Verfügung. Nach unserer Ansicht besteht keine technische Notwendigkeit für diesen Zwang, da die Speicherung des aufgezeichneten TV-Signals schließlich nicht „im Internet" erfolgt, sondern - wie bei anderen Herstellern auch – auf einem Speichermedium zuhause beim Nutzer, üblicherweise eine externe Festplatte. Da die TV-Sparte des Herstellers jedoch nicht in Deutschland, sondern bei einer Tochterfirma in den Niederlanden aufgehängt ist, wurde das Thema von den dortigen Datenschutzbehörden verfolgt. Der kritisierte Hersteller hat mittlerweile Korrekturen zugesichert und will zukünftig die Nutzer seiner TV-Geräte besser informieren. Unter anderem soll für das Setzen von Cookies die Zustimmung der Nutzer eingeholt werden.

7. Migration Datennetz und Anwendungen - Verfahrenskataster Polizei

Seit mehreren Jahren erfüllt die Polizei Hamburg ihre datenschutzrechtlichen Dokumentationspflichten nur unvollständig. Das neu entwickelte Verfahrenskataster muss jetzt unverzüglich genutzt werden, um diesen Mangel zu beheben.

In den letzten drei Tätigkeitsberichten (vgl. 21.TB, 2.7, 22.TB, II 7, 23.TB II 7) berichteten wir von der Übergabe des Polizei-Netzwerks an Dataport und insbesondere den Mängeln in der Dokumentation. Seit 2007 betreibt Dataport das Netzwerk und zahlreiche Anwendungen der Polizei Hamburg. Zahlreiche Informations-, Auskunfts- und Vorgangsbearbeitungsverfahren der Polizei sind in die Betreuung von Dataport übergegangen. Es bestanden erhebliche Bedenken, ob die realisierten Datenschutz- und Datensicherheitsstandards des Dienstleisters ausreichen, um den notwendigen Schutzbedarf für das Polizeinetz zu gewährleisten. Diese Bedenken sollten durch die Polizei Hamburg und uns nachträglich gemeinsam bewertet werden, um daraus eventuelle Handlungsnotwendigkeiten abzuleiten und auch die Vollständigkeit der erforderlichen datenschutzrechtlichen Unterlagen festzustellen.

Das damals vereinbarte Vorhaben, die uns vorliegenden Dokumente zu vervollständigen, kam jedoch nur schleppend voran. Motiviert gestartete Auftaktveranstaltungen zur Darstellung komplexer Verfahren bei der Polizei Hamburg blieben ohne Folgeveranstaltungen, eine Projektgruppe Migration versandete nach drei Sitzungen ohne greifbares Ergebnis.

Die Reorganisationsnotwendigkeit im IT-Bereich der Polizei Hamburg führte auch zu einem Verfahrensregister. Auch wenn dieses Register nicht primär entstand, um datenschutzrechtliche Dokumentationsverpflichtungen zu erfüllen, hatten wir die Hoffnung, dass mit der Datenbank auch unsere Forderungen Berücksichtigung finden würden.

Mit Hinweis auf diese Verfahrensdatenbank wurde unserer Kritik über immer noch ausstehende datenschutzrechtliche Dokumentationsverpflichtungen im August 2012 im Unterausschuss Datenschutz begegnet. Alles würde endlich gut, versicherte man uns noch im Dezember 2012 bei einem Termin mit der Polizei zum weiteren Verfahren und Abgleich der Dokumentationsstände. Trotz mehrfacher Nachfragen mussten wir jedoch Ende 2013 zur Kenntnis nehmen, dass zwar wichtige Vorarbeiten für das Verfahrenskataster weitgehend abgeschlossen sind, das Verfahrenskataster nach wie vor noch nicht genutzt wird, um die Dokumentationspflicht umfänglich zu erfüllen. Eine Beschlussfassung durch die Leitungsebene der Polizei war bei Redaktionsschluss noch nicht erfolgt, soll aber „in Kürze" erfolgen. Ob dann erste datenschutzrechtlich gesetzlich vorgesehene Dokumente zumindest für neue IT-Verfahren vorliegen, werden wir im Frühjahr 2014 prüfen.

8. Prüfung von Smartphone Apps

Viele Anwendungen für Smartphones und Tablet-PCs sind aus Datenschutzsicht bedenklich und übermitteln unerlaubt Daten oder ermöglichen eine Überwachung des Gerätenutzers. Der HmbBfDI entwickelt hierfür ein Prüfsystem.

Anwendungen für mobile Geräte, im Sprachgebrauch als „Apps" bekannt, erfreuen sich zunehmender Beliebtheit. Dies liegt vor allem an der steigenden Verbreitung von Smartphones und Tablet-Computern. Diese werden überwiegend mit den Betriebssystemen Android oder iOS betrieben. Android, entwickelt von Google, hat sich binnen weniger Jahre zum Marktführer entwickelt, da es ohne Lizenzkosten genutzt werden kann und daher von vielen Geräteherstellern wie Samsung, HTC oder Sony in die eigenen Produkte integriert wird. Das ebenfalls verbreitete Betriebssystem iOS des Unternehmens Apple hingegen kommt nur in Apple-eigenen Geräten wie dem iPhone oder iPad zum Einsatz. Einer der Erfolgsfaktoren der mobilen Betriebssysteme ist ihre Erweiterbarkeit durch die Installation von Apps. Die Nutzer können dadurch ihr Gerät dem individuellen Bedarf anpassen. Auch kann jeder mit entsprechendem technischen Know-how eigene Apps herstellen. Die Verbreitung erfolgt über sog. „App Stores". Dies sind zentrale Software-Marktplätze im Internet, auf denen jedermann Programme zum Download anbieten kann, wahlweise kostenfrei oder gegen Bezahlung.

Die Beliebtheit mobiler Geräte und der Umstand, dass ihre Benutzer immer mehr und immer umfassendere Informationen darauf speichern, macht sie zu interessanten Werkzeugen für Datensammler aller Art. Der „harmlose" Fall sind die Betreiber von Werbenetzwerken, die das Nutzungsverhalten von Apps auf dem Gerät erfassen und daraus Kapital schlagen wollen. Kritischer sind Apps, die Kontaktdaten aus dem persönlichen Adressbuch oder der SIM-Karte auslesen. Bekanntes Beispiel hierfür ist die verbreitete Chat-Anwendung WhatsApp. Selbst wenn ein Nutzer den Zugriff auf sein Adressbuch bewusst freigibt, kann dies deutschen Datenschutzgesetzen widersprechen, wenn hierunter auch Daten von Dritten sind, für deren Weitergabe der Nutzer keine explizite Erlaubnis der Betroffenen hat.

Zunehmend bieten auch Kriminelle Apps an, die als Schadsoftware (engl. „Malware") bezeichnet werden und für den Nutzer nachteilige Funktionen enthalten. Die Spanne reicht vom Erzeugen wirtschaftlichen Schadens durch heimliche SMS-Nachrichten oder Anrufe zu teuren Sondernufnummern über das Mitschneiden von Tasteneingaben (zur Gewinnung von Zugangsdaten für E-Mail- oder Bankkonten) bis hin zu ausgefeilten Spionageanwendungen, die eine permanente Überwachung des Nutzers ermöglichen. So wurden im Februar 2013 von einem Hersteller von Sicherheits-Software Apps mit weitreichenden Spionage-Funktionalitäten enttarnt: die Apps konnten das Mikrofon des Smartphones aktivieren, um eine akustische Überwachung durchzuführen und die

Aufnahmen über das Internet zu versenden. Ferner konnten nahezu alle Daten auf dem Gerät - Kontaktdaten, Nachrichten, Bilder usw. - oder einer eingesteckten Speicherkarte abgegriffen werden. Die Apps konnten den Webbrowser manipulieren und SMS-Nachrichten versenden, löschen oder weitere Schadsoftware installieren. Damit nicht genug - wurde das umfassend überwachte Smartphone an einen Windows-PC angeschlossen, konnte auch dort das PC-Mikrofon zum Mithören genutzt und weitere Schadsoftware nachgeladen werden. All diese Funktionalität steckte in einer einzigen App, vermarktet als scheinbar harmloses Programm zur Optimierung des Betriebssystems und kostenlos angeboten im größten App-Store für Android, dem „Play-Store" von Google.

Natürlich werden „böse" Apps nach dem Bekanntwerden ihrer Schadfunktion schnell aus den App-Stores entfernt und ihre Anbieter gesperrt. Jedoch hilft dies nur kurzzeitig, da bald modifizierte Varianten unter neuen Namen auftauchen. Auch nützt es wenig, sich vor der Installation einer unbekannten Anwendung auf das in den App-Stores übliche soziale Bewertungssystem zu verlassen - die dargestellten Schad-Apps hatten mit 90 Prozent eine hervorragende Einstufung, da die bewertenden Nutzer von den Schadfunktionen ja nichts wussten. Oftmals werden positive Bewertungen auch von den App-Entwicklern oder ihren Helfern fingiert.

Auch wenn viele App-Anbieter im Ausland sitzen und somit nur bedingt der deutschen Gesetzgebung unterfallen, ist es für die Datenschutzbehörden ein dringendes Anliegen, auch hier ihrer Prüf- und Aufsichtspflicht nachzukommen. In der Praxis zeigt sich übrigens häufig, dass viele Datenschutzverstöße nicht vorsätzlich, sondern aufgrund von Rechtsunkenntnis des Anbieters oder der Arglosigkeit von Entwicklern begangen werden, welche vorgefertigten Programmcodes auf dem Internet (z.B. von Werbenetzwerken) ungeprüft übernehmen und in die eigene Anwendung einbauen.

Um die Prüfung von Apps durch die deutschen Datenschutzbehörden zu intensivieren, fanden bereits länderübergreifende Arbeitstreffen statt, in denen ein kooperatives Vorgehen abgestimmt wurde. Unsere Dienststelle ist dabei aktiv involviert und entwickelt eine portable und plattformunabhängige Prüfumgebung, die anderen interessierten Datenschutzbehörden zur Verfügung gestellt werden kann.

9. Speicherung von WLAN-Passwörtern bei Android Geräten

Wer als Nutzer eines Smartphones oder Tablet-PCs mit dem Betriebssystem Android seine Gerätedaten auf Google-Servern sichert, liefert die Zugangsdaten zu allen genutzten WLAN Verbindungen an Google aus. Damit drohen Verstöße gegen Verschwiegenheitspflichten oder Corporate Governance Auflagen.

Das mobile Betriebssystem Android wird von Google konzipiert und vorangetrieben, auch wenn dies nach außen nicht direkt ersichtlich ist, da es in Geräten verschiedenster Hersteller zum Einsatz kommt. Wer heute ein aktuelles Smartphone oder Tablet von z.B. HTC, Motorola, Samsung oder Sony nutzt, kann davon ausgehen, dass dieses mehr „Google" enthält als Software des Geräteherstellers selbst. Da Android vor iOS oder Windows Phone das mit Abstand führende Betriebssystem bei mobilen Endgeräten ist, ist die Mehrheit der Nutzer von Google und den davon angebotenen Diensten mehr oder weniger abhängig. In Android sind die technischen Verstrickungen zum „Mutterschiff Google" so eng, dass man dort tiefe Einblicke in das Nutzungsverhalten jedes Besitzers eines Android-Gerätes erlangt. Es fängt beim „Play Store" an, dem weltweit größten Internet-Marktplatz für Zusatzprogramme zu Android. Dort können zahllose Anwendungen, sogenannte „Apps", bezogen werden, um die Funktionalität eines Android-Gerätes zu erweitern. Der Play Store kann – selbst wenn man nur kostenfreie Apps herunterladen möchte und somit überhaupt kein Kaufvorgang zustande kommt – nur genutzt werden, wenn man ein Kundenkonto bei Google hat, das daher auch nahezu jeder Android-Nutzer irgendwann anlegt.

Auch Android-Funktionen wie Kontakt- oder Terminplanung, E-Mail oder Navigation - für all dies gibt es zwar alternative Anbieter, am besten funktioniert es aber, wenn man es über Google erledigt. Auf diese Weise bindet Google Android-Nutzer eng an das eigene Unternehmen und erhält umfangreiche Einsicht in deren Leben. Besonders problematisch wird das vor dem Hintergrund, dass Google sich in den Datenschutzbedingungen vorbehält, die Daten der unterschiedlichen Dienste zu Mega-Profilen zusammenzulegen (siehe V 6.1).

Android bietet auch die Möglichkeit, eine Sicherung der Gerätedaten vorzunehmen. Wählt man hierfür ein Google-Konto, werden viele persönliche Daten des Nutzers vom Gerät an Google-Server übertragen und dort gespeichert. Diese Funktionalität erforderte im Jahr 2013 ein Tätigwerden unserer Dienststelle, als publik wurde, dass hierbei sämtliche WLAN-Zugangsdaten, die auf einem Gerät gespeichert sind, an Google übermittelt werden. Dies umfasst auch die dabei verwendeten Passwörter bzw. Schlüssel.

Personen, die beispielsweise ein Android-Gerät von ihrem Arbeitgeber erhalten haben und die Sicherungsfunktion nutzen, begehen ggf. einen Verstoß gegen arbeitsrechtliche Verschwiegenheits-Verpflichtungen oder Corporate Governance Vorgaben, weil sie damit das Passwort zum Firmennetzwerk an Dritte weitergeben. Gleiches gilt für Studenten und deren Zugang zum Hochschulnetzwerk.

Google hatte es versäumt, die Nutzer vor Aktivierung der Sicherung über diesen Umstand zu informieren. Dies wurde aufgrund unserer Forderungen mittlerweile umgesetzt, zumindest für aktuelle Android-Versionen: Leider nur in Form einer „Entweder-oder"-Option, d.h. der Nutzer muss entweder der Übermittlung aller WLAN-Passwörter zustimmen oder auf die Sicherungsfunktion verzichten. Jeder Android-Nutzer sollte daher gut abwägen, wie er diese Funktionalität nutzt bzw. ob er sie aufgrund von Geheimhaltungsverpflichtungen überhaupt nutzen darf. Unternehmen, die Android-Geräte an ihre Mitarbeiter ausgeben, sollten dieses Thema klar in den firmeninternen Sicherheitsrichtlinien regeln.

DATENSCHUTZ IM ÖFFENTLICHEN BEREICH III.

1. Polizei 46
2. Verfassungsschutz 57
3. Justiz 62
4. Strafvollzug 65
5. Gesundheitswesen 68
6. Sozialwesen 86
7. Schulwesen 96
8. Forschung 114
9. Bauen, Wohnen, Umwelt 116
10. Finanzwesen 119
11. Behördliche Datenschutzbeauftragte 126
12. Verkehr 127
13. Hochschulwesen 137
14. Wirtschaftsverwaltung 139
15. Parlamentsangelegenheiten Wahlen und Volksabstimmungen 141
16. Bezirke 143
17. Statistik 153
18. Personenstandswesen 157
19. Meldewesen 163
20. Personalausweis- und Passwesen 165

1. Polizei

1.1 Auswertung der Protokolle von Zugriffen auf polizeiliche Dateien

Unsere jahrelangen Bemühungen um eine effektivere datenschutzrechtliche Kontrolle der Zugriffe auf polizeiliche Dateien haben zu einem erfolgversprechenden Vorschlag der Polizei geführt.

Schon im 22.TB 2008/2009 4.5. hatten wir ausführlich auf Defizite bei der Kontrolle der polizeilichen Dateizugriffe hingewiesen. Wir kritisierten insbesondere, dass die Reaktion der Vorgesetzten auf die bei ihnen eingehenden Stichprobenmeldungen nicht dokumentiert wird und damit nicht revisionsfähig ist. Es ist auch für uns nicht zu ermitteln, ob und wie oft Polizeibedienstete ohne ausreichenden Grund bzw. missbräuchlich auf automatisierte Dateien zugegriffen haben.

Zur Umsetzung von § 27 Abs.1 (Stichprobenkontrolle) Gesetz über die Datenverarbeitung der Polizei werden bisher alle Zugriffe von Polizeibediensteten auf automatisierte Dateien protokolliert. Zugriffe auf das Polizeiliche Auskunftssystem zu Strafermittlungsverfahren POLAS, das Vorgangsverwaltungssystem ComVorIndex und das Einwohnermelderegister EWO protokolliert die Hamburger Polizei selbst. (Bei den häufigen polizeilichen Zugriffen auf das Verkehrszentralregister ZEVIS erfolgt die Protokollierung und Auswertung dagegen beim Kraftfahrtbundesamt.) Bei jedem 500. Zugriff wird die zugreifende Person durch eine besondere Abfragemaske aufgefordert, in zwei Freitextfeldern den Zugriffsgrund – z.B. ein konkretes Aktenzeichen - und ggf. den Auftraggeber anzugeben. In Eilfällen kann darauf verzichtet werden. Das System erzeugt über die Daten dieses Zugriffs automatisch eine E-Mail-Kontrollmitteilung an ein besonderes Datenschutzpostfach. Dieses kann nur der Vorgesetzte bzw. die von ihm beauftragte Person öffnen, um die Berechtigung des Dateizugriffs zu überprüfen. Was diese Überprüfung ergab, konnte jedoch bisher nicht nachvollzogen werden.

In einem Gespräch mit dem Polizeipräsidenten im April 2013 wiesen wir noch einmal auf die bestehenden Defizite hin. Der Polizeipräsident sagte eine Prüfung zu und ließ erkennen, dass eine Fortsetzung unserer Bemühungen auf Arbeitsebene zu einer Umsetzung der Anforderungen führen könne.

Nach weiteren Nachfragen unsererseits schlug uns die Polizei im Oktober 2013 folgende Erweiterung des automatisierten Kontrollverfahrens vor: Der Vorgesetze bzw. die beauftragte Person muss im Datensatz der Stichprobe neben ihrem Namen und dem Prüfungszeitpunkt die Art der Überprüfung angeben und entweder vermerken, dass und warum die Zugriffsberechtigung vorlag, oder dass der Zugriff nicht ordnungsgemäß war und welche Maßnahme deswegen ergriffen wird – Abgabe an die Abteilung Interne Ermittlungen bzw. an die Rechtsabteilung der Polizei zur Aufnahme von Ermittlungen wegen einer möglichen Ordnungswidrigkeit nach § 33 HmbDSG (Un-

befugtes Erhebung personenbezogener Daten). Durch die Protokollierung der Vorgesetztenentscheidung kann und wird die Revisionsabteilung der Polizei jeden als „nicht ordnungsgemäß" bewerteten Zugriff weiter verfolgen. Auch wir können den Fortgang der Angelegenheit dann innerhalb der Speicherfrist von 6 Monaten nachvollziehen.

Wichtig erschien uns außerdem, dass ein „Herunter-Delegieren" der Überprüfungsaufgabe durch den bzw. die Vorgesetze/n nicht dazu führen darf, dass Kollegen derselben Hierarchiestufe oder eng kooperierende Mitarbeiter sich gegenseitig kontrollieren.

Um dringende Eilfälle nicht zu behindern, haben wir auch weiterhin auf eine technisch erzwungene Ausfüllung der Abfragemaske vor einer Fortsetzung des Dateizugriffs verzichtet. Eine fehlende Zugriffsbegründung in der Kontrollmitteilung wird bei der Vorgesetztenprüfung jedoch besondere Nachforschungen auslösen.

Die Einführung dieser aus unserer Sicht geeigneten Systemerweiterung hängt nach Auskunft der Polizei vor allem von der aktuellen Prioritätensetzung der IT-Abteilung ab. Trotz unseres Drängens wollte die Polizei sich nicht auf einen baldigen Umsetzungstermin festlegen. Angesichts der langjährigen Defizite bei der gesetzlich vorgesehenen Datenschutzkontrolle fordern wir eine Umsetzung im Jahre 2014.

1.2 Ergänzung des PolDVG um Bestandsdatenabfrage

Im Datenverarbeitungsgesetz für die Polizei (PolDVG) wurde die Befugnis konkretisiert, von Telekommunikations- und Telemedienanbietern Kundendaten und Zugangssicherungscodes abzufragen. Wir konnten dabei einzelne Verbesserungen erreichen, nicht jedoch einen Richtervorbehalt für die Abfrage von Sicherungscodes und die Verwendung von dynamischen IP-Adressen.

Mit Urteil vom 24. Januar 2012 stellte das Bundesverfassungsgericht fest, dass es für die Abfrage von Bestandsdaten (insbesondere Namen und Anschrift der Telekommunikationskunden) und von besonderen Zugangssicherungscodes einer normenklaren gesetzlichen Ermächtigung für die abfragenden Stellen bedarf. Dies gelte besonders, wenn die Abfrage sich auf dynamische IP-Adressen stützt.

Am 11.März 2013 legte die Behörde für Inneres und Sport einen Entwurf zur Änderung des PolDVG und parallel des Hamburgischen Verfassungsschutzgesetzes vor. In unserer Stellungnahme kritisierten wir die Einführung eines neuen Begriffs der „Bestandsdaten", der gegenüber der gesetzlichen Definition in § 95 Telekommunikationsgesetz (TKG) weitere Daten nach § 111 TKG umfassen soll. Wir erinnerten an das sog. Zitiergebot aus Art. 19 Abs.2 Grundgesetz, bei Grundrechtseingriffen das betroffene Freiheitsrecht ausdrücklich zu nennen. Der Grundrechtseingriff ergibt sich aus der be-

absichtigten Nutzung der dynamischen IP-Adressen, die sich auf konkrete Kommunikationsverbindungen beziehen und deswegen als personenbezogene Verkehrsdaten vom Fernmeldegeheimnis (Art.10 GG) geschützt werden. Schließlich regten wir eine Konkretisierung der möglichen Anlässe für eine Bestandsdatenabfrage an.

In einer Überarbeitung des Gesetzentwurfs vom 27. März 2013 berücksichtigte die Behörde für Inneres und Sport das Zitiergebot und ergänzte die Gesetzesbegründung um eine Konkretisierung. Im Übrigen sah sie von einer Änderung ab.

Parallel zum Hamburger Gesetzgebungsverfahren ergänzte auch der Bundesgesetzgeber die Eingriffsbefugnisse von Bundeskriminalamt, Bundespolizei und Zollfahndung im Hinblick auf eine Bestandsdatenabfrage. Nach einem Änderungsantrag vom 14. März 2013 im Bundestags-Innenausschuss wurde in den Gesetzentwürfen nun für die Abfrage besonderer Zugangssicherungscodes (PIN und PUK) grundsätzlich ein Richtervorbehalt und eine Benachrichtigungspflicht verankert. Eine Benachrichtigung der Betroffenen wurde nun auch bei der Nutzung dynamischer IP-Adressen vorgesehen, allerdings mit Ausnahmen. Im Mai 2013 stimmte auch der Bundesrat diesen datenschutzfreundlicheren Regelungen zu, die damit Gesetz wurden.

Mit Schreiben vom 17. Mai 2013 regten wir die Übernahme dieser bundesrechtlichen Datenschutzregelungen auch für das PolDVG an. Die Behörde für Inneres und Sport lehnte eine nachträgliche eigene Initiative in dieser Richtung ab und verwies auf den Innenausschuss der Bürgerschaft, an den der Gesetzentwurf inzwischen überwiesen worden war. Dieser griff unseren Vorschlag, das Hamburger Recht an das Bundesrecht anzupassen, nur zum Teil auf: In den neuen § 10 f PolDVG wurde ein Absatz 4 eingefügt. Anstelle eines Richtervorbehalts räumt er dem Polizeipräsidenten bzw. seinem Vertreter – in Eilfällen auch dem zuständigen Polizeiführer - die Befugnis zur Anordnung einer Abfrage von Zugangssicherungscodes ein. Für die Abfrage von Zugangssicherungscodes und im Falle der Nutzung von dynamischen IP-Adressen für die Abfrage normiert Absatz 4 nun eine grundsätzliche Pflicht, die betroffene Person zu benachrichtigen.

Mit einer zu Protokoll nachgereichten Übersicht informierten wir den Innenausschuss nach einer Länderumfrage über den Stand der Gesetzesvorhaben in den anderen Bundesländern. In den wenigsten Ländern waren die Vorhaben so weit fortgeschritten; die Inhalte der Entwürfe waren keineswegs einheitlich.

Das Änderungsgesetz vom 19.6.2013 mit dem neuen § 10 f PolDVG trat am 1. Juli 2013 in Kraft - ohne Richtervorbehalt, aber mit Benachrichtigungspflichten.

1.3 Videoüberwachung der Polizeikommissariate nach Hausrecht

Viele Videokameras zur Überwachung der Außenbereiche von Polizeikommissariaten überschritten den zulässigen Aufnahmeumfang und erfassten in unzulässiger Weise auch die Nutzer öffentlicher Wege. Auf unsere Kritik hin wurden die Kameraeinstellungen geändert.

Im Rahmen unserer Bestandsaufnahme der Videoüberwachung durch öffentliche Stellen (23. TB 1.2) haben wir am 30. August 2012 endlich auch die notwendigen Unterlagen der Polizei erhalten. Daraus haben wir die Videoüberwachungsanlagen der 25 Polizeikommissariate und ihrer Außenstellen ausgewählt und die Kameras für die Außenbereiche geprüft. Bei neun Kommissariaten mussten wir feststellen, dass zumindest eine, oft aber auch mehrere Kameras so eingestellt waren oder per Fernsteuerung so eingestellt werden können, dass sie weit in den öffentlichen Raum hinein filmten. Zufällig vorbei kommende Fußgänger und Kfz wurden von der Aufnahme erfasst und konnten über einen Monitor im Wachraum beobachtet werden. Zum Teil werden die Aufnahmen zusätzlich gespeichert.

Dies ist von § 30 Hamburgisches Datenschutzgesetz (HmbDSG), der 2010 neu in das Gesetz aufgenommen wurde und die Videoüberwachung regelt, nicht gedeckt. Die Vorschrift legitimiert Videoüberwachungen ausschließlich über das Hausrecht. Zwar stehen der Polizei grundsätzlich auch spezialgesetzliche Ermächtigungsnormen für Bild- und Tonaufzeichnungen zur Verfügung. Diese waren vorliegend jedoch nicht einschlägig. Insbesondere kann § 8 Hamburgisches Gesetz über die Datenverarbeitung der Polizei (PolDVG) eine flächendeckende Videoüberwachung des Außenbereiches von Polizeikommissariaten ohne besondere Gefährdungslage nicht rechtfertigen.

Das Hausrecht erfordert andererseits eine enge Beziehung zwischen dem von der Kamera erfassten und beobachteten Bereich und dem Zugang zu dem Gebäude. Sinn von § 30 HmbDSG ist es einerseits, die Integrität des öffentlichen Gebäudes (Türen, Fenster, Fassaden) und seiner in ihm befindlichen Personen und Sachen zu schützen, und andererseits, den Zu- und Ausgang für Personen mit einem legitimen Interesse am Zutritt zu dem Amtsgebäude zu gewährleisten. Nur zu diesem Zweck schränkt § 30 HmbDSG das informationelle Selbstbestimmungsrecht der betroffenen Personen – der Mitarbeiter, Besucher, Anzeigenerstatter, aber auch möglicher Angreifer – ein. Der notwendige Bezug zum Zugang zu dem Gebäude fehlt jedoch, wenn die Videokamera auch völlig Unbeteiligte erfasst, die das Amtsgebäude weder verlassen haben noch betreten wollen. Deren Grundrecht auf informationelle Selbstbestimmung verbietet eine anlasslose Beobachtung und Aufzeichnung durch Videokameras der öffentlichen Stelle.

Wir haben deswegen im April 2013 den Aufnahmebereich von 18 Überwachungskameras an 6 Polizeikommissariaten kritisiert. Nach einer Antwort der Rechtsabteilung der Polizei haben wir im Juli 2013 die Überwachung von Polizeiparkplätzen von der Kritik ausgenommen, im Übrigen aber den Datenschutzverstoß von 12 Kameras konkretisiert.

Als ein weiteres Defizit mussten wir das generelle Fehlen von Hinweisschildern feststellen, die § 30 Abs.3 HmbDSG für eine im Übrigen zulässige Videoüberwachung fordert. Auch zur Behebung dieses Mangels forderten wir die Polizei bereits im April 2013 auf.

Keine Bedenken haben wir dagegen gegen die Videokameras geäußert, die den durch einen Zaun zur öffentlichen Straße abgegrenzten Grünbereich um das Gebäude oder – bei fehlendem Grünbereich – nur einen schmalen Streifen des öffentlichen Weges unmittelbar an der Hausmauer sowie die Stellplätze für die Dienstfahrzeuge vor dem Gebäude erfassten.

Kurz vor Redaktionsschluss, am 19. Dezember, erreichte uns die Reaktion der Polizei. Für fast alle von uns beanstandeten Kameras bestätigte das Justiziariat, dass eine Neuausrichtung der Geräte möglich ist und die IuK-Abteilung der Polizei damit beauftragt wurde. Im Übrigen konnten wir die Gegenargumente der Polizei akzeptieren. Der angekündigten Dokumentation nach erfolgter Neuausrichtung und nach Anbringung der geforderten Hinweisschilder sehen wir entgegen.

1.4 Videoüberwachung von Fußballstadien durch die Polizei

Nach jahrelanger Diskussion über den Einsatz von Videokameras in Fußballstadien besuchten wir die HSV-Anlage vor Ort, klärten die Voraussetzungen für eine Kameranutzung durch Polizei und Vereine und erreichten, dass die Einzelheiten in einem Vertrag zwischen Polizei und Verein festgeschrieben werden.

Seit 2010 beschäftigen wir uns mit der Überwachung der Fußballstadien von St.Pauli und HSV durch Videokameras. Seit Juli 2012 gelten neue „Richtlinien zur Verbesserung der Sicherheit bei Bundesspielen" des Deutschen Fußballbundes. § 10 Abs.5 der Richtlinie fordert von den Vereinen die Installation von „Video-Kameras mit Zoom-Einrichtung", „Die Anlage sollte von der Befehlsstelle der Polizei zu bedienen, an die Polizeimonitore angeschlossen sein" und eine Täter-Identifizierung durch Standbildaufnahmen zulassen. „Die Anlage sollte auch von der Befehlsstelle des Ordnungsdienstes aus bedient werden können."

Die Polizei übersandte uns im September 2012 die Verschlusssache „Fachanweisung für Videoüberwachungen bei Veranstaltungen und Ansammlungen", lehnte aber die

Vornahme einer eigenen Risikoanalyse nach § 8 Abs.4 Hamburgisches Datenschutzgesetz ab. Sie sah zunächst auch keinen Anlass, mit den betroffenen Vereinen vertragliche Vereinbarungen über die technisch-organisatorische Gestaltung der Überwachungseinsätze abzuschließen. Einigkeit bestand über die Rechtsgrundlage für die Nutzung der Vereinskameras durch die Polizei zu Zwecken der Gefahrenabwehr: § 8 Abs.1 Gesetz über die Datenverarbeitung der Polizei (PolDVG) ermächtigt die Polizei, bei öffentlichen Veranstaltungen mit Hilfe technischer Mittel Bilddaten von Teilnehmern zu erheben, wenn Tatsachen dafür sprechen, dass bei der Veranstaltung Straftaten begangen werden.

Anfang November 2012 besuchten wir mit Vertretern der Polizei das HSV-Stadion - auch stellvertretend für den FC St.Pauli - und diskutierten mit Vereinsvertretern. Das mit allen Beteiligten abgestimmte Protokoll vom März 2013 beschreibt die Funktionen und Eigenschaften der eingesetzten 44 Kameras sowie technische Einzelheiten der Kameraführung, Aufzeichnung und Wartung der Anlage. Der Verein nutzte die Anlage während Bundesligaspielen selbst nicht, wünschte aber entsprechend der DFB-Richtlinien für die Zukunft eine Einsicht seines Ordnungsdienstes auf die Polizei-Monitore. Ergänzend erbaten und erhielten wir von der Polizei eine Reihe technischer und organisatorischer Auskünfte.

Mitte Juli 2013 übersandten wir der Polizei einen rechtlichen Vermerk zur Nutzung der Videoüberwachung durch die Polizei und den Verein. Danach hat die Polizei bei Bundesligaspieltagen die ausschließliche Verantwortung und Sachherrschaft über die Videoanlage. Der Ordnungsdienst des Vereins darf allenfalls im Rahmen von Ermächtigungen durch die Polizei tätig werden, z.B. Einsicht auf die Monitore nehmen. Rechtlich handelt es sich insoweit um Übermittlungen der Polizei an Stellen außerhalb des öffentlichen Bereichs, wie sie in § 21 PolDVG geregelt sind. Bei anderen Veranstaltungen an Tagen, an denen die Polizei nicht vor Ort ist und keine Maßnahme nach § 8 Abs.1 PolDVG durchführt, darf der Verein die Überwachungsanlage unter den Voraussetzungen des § 6 b Bundesdatenschutzgesetz nutzen. Soweit hierbei Bilder aufgezeichnet werden, die für eine Strafverfolgung geeignet sind, kann die Polizei diese später nach der Strafprozessordnung sicherstellen.

Am 4. Dezember 2013 übersandte uns die Polizei den Entwurf eines Mustervertrages „zur Datenverarbeitung im Auftrag" zwischen der Polizei (Auftraggeber), dem Fußballverein (Auftragnehmer) und der Wartungsfirma (Unterauftragnehmer). Darin werden die Weisungs- und Kontrollrechte des Auftraggebers, die gegenseitigen Pflichten sowie die notwendigen technischen und organisatorischen Maßnahmen konkretisiert. Der Vertrag bezieht sich ausschließlich auf die Veranstaltungstage, an denen die Polizei die Videoanlage des Fußballvereins für ihre Zwecke einsetzt und steuert. Über die Einzelheiten der Regelungen sind wir weiter mit der Polizei im Gespräch.

1.5 Eingaben zur Löschung von Daten in polizeilichen Dateien

Sind einmal personenbezogene Daten in polizeilichen Dateien gespeichert, ist es nicht leicht, sie bei entfallener Erforderlichkeit unverzüglich wieder löschen zu lassen.

Im Berichtszeitraum haben wir eine Reihe von Eingaben erhalten, die das Ziel hatten, Datenspeicherungen, die aus Sicht der Bürger nicht bzw. nicht mehr für polizeiliche Zwecke erforderlich waren, wieder rückgängig zu machen. Dabei ging es um Daten im kriminalpolizeilichen Auskunftssystem POLAS und um das Register der Vorgangsverwaltung (ComVor-Index), aber auch um Daten aus dem Vorgangsverwaltungssystem MESTA der Staatsanwaltschaft.

Wir haben die Polizei darauf hingewiesen, dass qualifizierte Löschungsbegehren im Einzelfall nicht mit dem allgemeinen Hinweis auf die automatisierten Prüfungsfristen im Vorgangsverwaltungssystems ComVor-Index abgewehrt werden können. Die von § 15 S. 1 Gesetz über die Datenverarbeitung der Polizei (PolDVG) geforderten Prüffristen sollen vielmehr nur sicherstellen, dass einmal gespeicherte Daten nicht vergessen, sondern automatisch zur Prüfung der weiteren Erforderlichkeit wieder vorgelegt werden, soweit sie nicht inzwischen mit dem Ende des Speicherungs-Erfordernisses ordnungsgemäß gelöscht wurden.

So kostete es einigen Schriftverkehr und fünf Monate Zeit, bis die Daten und ein Foto eines 16-jährigen Schülers gelöscht wurden, den die Polizei auf dem Heimweg von der Schule angehalten hatte, weil in der Nähe ein Raub geschehen war und die Kleidung des Schülers zunächst der des möglichen Täters ähnlich sah. Obwohl die Polizei die Ermittlungen bereits einen Monat nach der Überprüfung des Schülers abgeschlossen und der Staatsanwaltschaft übermittelt hatte, nahmen Aktenzeichensuche und Entscheidungen der zuständigen Staatsanwaltschaft weitere 4 Monate in Anspruch.

Andere Bürger, die pauschal die Löschung ihrer polizeilichen Daten forderten, haben wir zunächst auf ihr Recht auf Auskunft hingewiesen, um genau zu erfahren, über welche Daten die Polizei im kriminalpolizeilichen Auskunftssystem POLAS und im Vorgangsverwaltungssystem ComVor-Index verfügt. Sinnvoll ist ferner ein Antrag an die Staatsanwaltschaft auf Auskunft aus ihrem Vorgangsverwaltungssystem MESTA (s.o. 3.2) und dem staatsanwaltlichen Zentralregister, da die Polizei abgeschlossene Ermittlungsvorgänge an die Staatsanwaltschaft abgibt und über den weiteren Fort- und Ausgang des Verfahrens oft keine Auskunft geben kann.

Immer wieder müssen wir Bürger auch darüber aufklären, dass Verfahrenseinstellungen, ja selbst ein späterer Freispruch nicht ohne Weiteres zu einer unmittelbaren Löschung in den Polizeidateien führen. Vielmehr bleiben die Daten regelmäßig bis zum Ablauf

der festgelegten Prüffristen gespeichert, wenn die Daten zur Auffindung der Vorgänge (ComVor-Index) oder für künftige Ermittlungen (POLAS) gebraucht werden könnten, also hinsichtlich der betroffenen Person eine sog. „Negativprognose" besteht. Dies kann auch bei Verfahrenseinstellungen mit Auflagen (§ 153 a StPO) oder wegen Geringfügigkeit (§ 153 StPO) oder bei einem Freispruch wegen Mangels an Beweisen der Fall sein. Hier kann nur ein Antrag auf Einzelfallbearbeitung (§ 24 Abs.2 S.1 Nr.3 PolDVG; § 489 Abs.2 S.1 StPO) mit qualifiziertem Löschungsbegehren eine aktuelle Erforderlichkeitsprüfung bewirken. In mehreren Fällen führte eine solche Prüfung allerdings nicht zu einer vorgezogenen Löschung. Eine polizeiliche Negativprognose haben wir nur bei offensichtlichen Fehlbeurteilungen datenschutzrechtlich zu kritisieren.

Die Trennung zwischen Polizei und Staatsanwaltschaft hat auch zur Folge, dass Änderungen – ggf. auch Abschwächungen - des Tatvorwurfs im weiteren Strafverfahren grundsätzlich nicht in die polizeilichen Dateien übertragen werden. In einem Fall fühlte sich ein Bürger wegen einer solchen scheinbaren Unrichtigkeit von POLAS-Einträgen diskriminiert, weil er bei Polizeikontrollen immer erläutern müsse, dass die Eintragungen nicht zuträfen. In POLAS werden die Ergebnisse des Verfahrens allerdings nachgetragen; zwischen der Abgabe an die Staatsanwaltschaft und der Entscheidung und Datenpflege kann jedoch ein längerer Zeitraum liegen. Ein Zugriff auf die ComVor-Index-Daten, die nur die Vorgangsbearbeitung durch die Polizei dokumentieren, ist nach Auskunft der Polizei im Übrigen für Zwecke der Strafverfolgung oder der vorbeugenden Bekämpfung von Straftaten nicht zugelassen.

1.6 Ausländervereine

Anlässlich einer Eingabe konnten wir eine datenschutzwidrige Behandlung von Ausländervereinen durch die Polizei korrigieren.

Der Vorsitzende eines Sportvereins, dessen Mitglieder zumeist (deutsche) Kinder aus Migrantenfamilien sind, bat uns um Überprüfung einer Aufforderung der Polizei. Der Vereinsvorsitzende sollte, „soweit es sich bei Ihrem Verein um einen Ausländerverein handeln sollte", ein beigefügtes polizeiliches Anmeldeformular ausfüllen und zusammen mit der Satzung und dem Gründungsprotokoll übersenden. Die Definition von „Ausländerverein" wurde beigefügt. Das Anschreiben der Polizei endete mit dem Satz: „Für den Fall, dass es sich bei Ihrem Verein nicht um einen Ausländerverein handelt, bitte ich Sie um eine entsprechende Nachricht unter Beifügung der Namen und Anschriften der Mitglieder".
Das beigefügte Anmeldeformular fragte unter anderem folgendes ab: die Tätigkeit des Vereins, Namen und Anschriften der Vorstandsmitglieder, die Staatsangehörigkeit der Mitgliedermehrheit und „bei politischer Betätigung des Vereins" a) Namen und Anschriften der Vereinsmitglieder, b)-d) Nachweise zur Herkunft und Verwendung der Mittel.

Die von der Polizei richtig zitierte Definition eines Ausländervereins ergibt sich aus § 14 Abs.1 S.1 Vereinsgesetz. Gemäß § 20 Abs.1 Nr.2a der Durchführungsverordnung zum Vereinsgesetz darf die Polizei bei Ausländervereinen, die sich politisch betätigen, auch Auskunft fordern über Namen und Anschriften der Mitglieder und die Herkunft und Verwendung der Mittel. Nach der Rechtsprechung ist die Auskunftsaufforderung aber selbst dann kein Automatismus, sondern setzt eine Abwägung zwischen den Nachteilen für die Vereinsmitglieder und dem öffentlichen Interesse an der Auskunftserteilung voraus.

Das Anmeldeformular der Polizei war von den genannten Vorschriften gedeckt und grundsätzlich nicht zu beanstanden. Das Anschreiben war jedoch fehlerhaft. Es hätte dem Vereinsvorstand deutlicher machen müssen, dass ausschließlich Ausländervereine überhaupt auskunftspflichtig sind, dass der angeschriebene Vorstand das selbst zu prüfen hat und dass selbst ein Ausländerverein nur dann die Namen und Anschriften von Mitgliedern offenbaren muss, wenn er sich politisch betätigt.

Die Polizei ist unserer Rechtsauffassung schließlich beigetreten und sagte zu, auf den letzten Satz des Anschreibens zukünftig zu verzichten. Sie wertete die erbetene Auskunft zunächst als „freiwillig", was jedoch schon wegen fehlender Aufklärung nicht zutraf. Dem Vereinsvorsitzenden konnten wir mitteilen, dass er mangels politischer Betätigung des Vereins die Namen und Adressen der Mitglieder nicht zu offenbaren brauchte. Ob es sich bei dem Verein überhaupt um einen Ausländerverein handelte, blieb offen und der Bewertung durch den Vorsitzenden überlassen.

1.7 Funkzellenabfragen

Trotz politischer Bemühungen um eine Eingrenzung von massenweisen Funkzellenabfragen konnte bisher noch nicht einmal die Anzahl der Funkzellenabfragen ermittelt werden, die in Hamburg zu präventiven oder repressiven Zwecken angeordnet wurden.

Im Zusammenhang mit einer größeren Demonstration gegen Neo-Nazis hatte die Dresdner Polizei im Februar 2011 verschiedene Mobilfunkanbieter befragt, welche Telefone bzw. deren Besitzer zu einer bestimmten Zeit in dem betroffenen (Funkzell-) Bereich angemeldet waren. Durch diese massenweisen Funkzellenabfragen erfuhr die Polizei die Kommunikations-Verkehrsdaten von zehntausenden Demonstranten und unbeteiligten Anwohnern. Dies führte auf Bundesebene und auch in Hamburg zu Gesetzesinitiativen, um die Voraussetzungen für die sog. nichtindividualisierte Funkzellenabfrage nach § 100 g Abs.2 S.2 Strafprozessordnung (StPO) zu verschärfen. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder forderte bereits 2011 in einer Entschließung die Einschränkung der Funkzellenabfragen.

Wir nahmen die bislang weitgehend folgenlose Diskussion 2013 noch einmal zum Anlass für Anfragen bei der Staatsanwaltschaft und bei der Polizei.
Nach § 100 g Abs.4 StPO muss die Staatsanwaltschaft einmal jährlich eine Übersicht über die Erhebungen von Verkehrsdaten aufgrund von § 100 g StPO erstellen. Diese legte sie uns im September 2013 für die Jahre 2008 bis 2012 vor. Aber weder die vom Bundesamt für Justiz für die Jahre 2008 – 2011 veröffentlichte Länderübersicht, noch die von der Hamburger Staatsanwaltschaft für das Jahr 2012 übersandte eigene Übersicht weisen Funkzellenabfragen nach § 100 g Abs.2 S.2 StPO gesondert aus. Diese sind vielmehr Unterfälle der 1413 Verkehrsdatenabfragen nach § 100 g Abs.1 Nr.1 StPO, die die Staatsanwaltschaft Hamburg für das Jahr 2012 angab. Neben der Funkzellenabfrage fallen auch alle Daten über Telefonnummern, Zugangscodes, Beteiligte, sowie Ort und Zeit einer konkreten Kommunikation unter den Begriff der Verkehrsdaten (§ 96 Abs.1 Telekommunikationsgesetz). Da § 100 g Abs.4 StPO eine gesonderte Berichterstattung über Funkzellenabfragen nicht vorschreibt, erfasst die Staatsanwaltschaft Hamburg diese auch zukünftig nicht.

Für Zwecke der Gefahrenabwehr erlaubt auch § 10 d Polizeidatenverarbeitungsgesetz (PolDVG) der Polizei Funkzellenabfragen. Nach § 10 e Abs.7 PolDVG hat der Senat die Bürgerschaft jährlich „über die nach §§ 10 b - 10 d angeordneten Maßnahmen" zu unterrichten. Die entsprechende Übersicht wurde uns im Rahmen einer Senatsdrucksachenabstimmung im September 2013 übermittelt. Auch hier ist die Funkzellenabfrage nur ein nicht gesondert erfasster Unterfall der für den Zeitraum Juni bis Dezember 2012 ermittelten drei Maßnahmen nach § 10 d Abs.3 PolDVG. Wir haben die zuständige Justizbehörde gebeten, hier in Zukunft zu differenzieren.

Sowohl Senatsantworten auf mehrere Kleine Anfragen als auch eine direkte Mitteilung der Polizei an uns bestätigten, dass die Anzahl der Funkzellenabfragen in Hamburg weder im repressiven noch im präventiven Bereich feststellbar ist. Wir sehen darin einen Mangel und behalten uns die direkte datenschutzrechtliche Prüfung erfolgter Funkzellenabfragen vor. Im August 2013 teilte uns die Polizei auf unsere Anregung mit, dass das Landeskriminalamt eine interne Richtlinie für die Durchführung von Funkzellenabfragen vorbereite. Sie ist uns bis Redaktionsschluss noch nicht zugegangen.

1.8 Sicherheitsüberprüfungen bei Abschleppunternehmen

Vor der Auftragsvergabe von Abschleppleistungen für 2014-2018 will die Polizei dem Abschleppunternehmen die Einwilligung aller seiner Fahrer in eine Sicherheitsüberprüfung abverlangen. Wir sehen dafür keine Rechtsgrundlage und halten das für unverhältnismäßig.

2012 kritisierten wir, dass die Hamburger Polizei alle Fahrer des beauftragten Ab-

schleppunternehmens einer Sicherheitsüberprüfung unterwirft. Zuvor hatte eine bundesweite Umfrage ergeben, dass eine solche Praxis in keinem der acht Bundesländer besteht, die sich an der Befragung beteiligten.

Im Juli 2013 erhielten wir den Entwurf der Leistungsbeschreibung für die Ausschreibung der Abschleppleistungen im Zeitraum Juli 2014 bis Juni 2018. In § 26 des Entwurfs heißt es: „Der Auftragnehmer hat ...(vor Auftragsvergabe) ... die aktuellen polizeilichen Führungszeugnisse seines ...Personals sowie für jede einzelne Person eine Einwilligungserklärung in eine polizeiliche Sicherheitsüberprüfung beizufügen." Jeden Personalwechsel hat das Abschleppunternehmen der Polizei anzuzeigen.

In § 25 des Entwurfs behielt sich die Polizei ferner vor, einzelne Beschäftigte des Abschleppunternehmens bei Bedenken „jederzeit" abzulehnen. Der Auftragnehmer darf den Beschäftigten dann nicht mehr für polizeiliche Aufträge einsetzen. „Die Polizei braucht solche Bedenken dem Auftragnehmer gegenüber nicht zu begründen." Unsere Kritik an dieser Regelung führte zu der Ergänzung, dass dem betroffenen Mitarbeiter vor einer Ablehnung „rechtliches Gehör anzubieten und Gelegenheit zu geben ist, sich persönlich zu den für die Entscheidung erheblichen Tatsachen zu äußern."

Unsere erneute Kritik an den geplanten Sicherheitsüberprüfungen blieb dagegen bislang erfolglos. Die Polizei begründete ihre Forderung mit § 34 Hamburgisches Sicherheitsüberprüfungs- und Geheimschutzgesetz (HmbSÜG). Danach kann der Senat auch für nicht benannte sicherheitsempfindliche Bereiche bestimmen, „dass Personen, die dort tätig sind oder werden sollen, einer Sicherheitsüberprüfung zu unterziehen sind." In der entsprechenden Rechtsverordnung werden zu diesen sicherheitsempfindlichen Bereichen auch „Polizeidienststellen" gerechnet. Um eine solche handele es sich auch bei der Kfz-Verwahrstelle Halskestraße, die ca. 2500 mal im Jahr von Abschleppwagen angefahren werde. Außerhalb der normalen Dienstzeiten betreten die Fahrer des Abschleppunternehmens die unbewachte Verwahrstelle mit Hilfe einer Transponder-Chipkarte. Dem dadurch entstehenden Risiko müsse durch eine vorbeugende Sicherheitsüberprüfung aller Abschleppfahrer begegnet werden.

Wir äußersten Zweifel an der Auslegung, dass die Abschleppwagenfahrer in der Polizeidienststelle Halskestraße „tätig sind oder werden sollen". Das Anfahren und Abstellen von Kraftfahrzeugen ist nach unserer Auffassung nicht gleichzusetzen mit dem vom Gesetz gemeinten dauerhaften, zumindest längerfristigen Arbeiten auf dem Verwahrplatz selbst.

Darüber hinaus beanstandeten wir die Unverhältnismäßigkeit der Maßnahme. Wenn die Polizei die Verwehrstelle Halskestraße als sicherheitsempfindlichen Bereich einstuft, ist es kaum nachzuvollziehen, dass sie keine Rund-um-die-Uhr-Bewachung durch eigenes oder beauftragtes Personal sicherstellt, wie etwa bei der zentralen Fahrzeugverwahrstelle Ausschläger Allee. Vielmehr entsteht der Eindruck, dass das mögliche

Sicherheitsrisiko auf die vielen Abschleppfahrer des Auftragnehmers abgewälzt wird, die sich praktisch nicht wehren können. Denn wenn sie einer Sicherheitsüberprüfung nicht zustimmen, verhindert das den Zuschlag für ihren Arbeitgeber und damit möglicherweise auch ihre zukünftige Weiterbeschäftigung. Wer nach einem Zuschlag als neuer Abschleppfahrer die Sicherheitsüberprüfung verweigert, wird nicht nur von polizeilich verfügten Abschleppleistungen ausgeschlossen, sondern wohl auch den Arbeitsplatz überhaupt verlieren.

Eine Sicherheitsüberprüfung stellt einen nicht unerheblichen Grundrechtseingriff dar: Nach § 13 Hamburgisches Sicherheitsüberprüfungsgesetz sind in der Sicherheitserklärung eine Fülle von sehr persönlichen Angaben zu machen. Sie reichen von den Wohnsitzen seit dem 18. Lebensjahr über die Personalien der Eltern und durchgeführte Zwangsvollstreckungsmaßnahmen bis zu Kontakten zu bestimmten Organisationen und anhängigen Straf- und Disziplinarverfahren.

Wägt man ab zwischen dem relativ geringen finanziellen Aufwand für eine ergänzende persönliche Bewachung bzw. eine Monitor-Beobachtung der bereits installierten fünf Videokameras einerseits und dem starken Eingriff in die informationelle Selbstbestimmung aller Mitarbeiter des Auftragnehmers andererseits, erscheinen „flächendeckende" Sicherheitsüberprüfungen aller Abschleppfahrer unverhältnismäßig. Tatsächliche Kontrollen und Sicherheitsmaßnahmen vor Ort erscheinen zudem geeigneter als die unterschiedslose Abfrage persönlicher Daten lange vor einer konkreten Auftragsdurchführung. Es ist auch nicht ersichtlich, warum die anderen Bundesländer ohne eine Sicherheitsüberprüfung auskommen und nur die Polizei Hamburg darauf nicht glaubt verzichten zu können.

Wir werden das Thema weiter auf der Tagesordnung haben und auf eine datenschutzkonforme Praxis drängen.

2. Verfassungsschutz

2.1 Verdeckte Ortung über Mobilfunkeinrichtungen im Ausland

Unsere gutachterliche Stellungnahme an das Landesamt für Verfassungsschutz führte zu einer Ergänzung des Hamburgischen Verfassungsschutzgesetzes um eine Rechtsgrundlage für die Ortung von Mobilfunkgeräten im Ausland.

Der Parlamentarische Ausschuss zur Kontrolle des Senats auf dem Gebiet des Verfassungsschutzes und das Landesamt für Verfassungsschutz (LfV) baten uns im Mai 2012 um ein Gutachten zur datenschutzrechtlichen Zulässigkeit von Ortungen über Mobilfunkeinrichtungen. Dazu wurden uns umfangreiche Unterlagen zur Verfügung gestellt.

Aus Gründen des Geheimschutzes muss hier auf eine genaue Beschreibung der Funktionsweise des konkreten Ortungsverfahrens verzichtet werden.

Unser Gutachten bearbeitete insbesondere die Frage, ob es für diese Art von nachrichtendienstlichem Mittel eine ausreichende Rechtsgrundlage gab. Wir verneinten zwar einen Eingriff in das Fernmeldegeheimnis, da die Ortung über Mobilfunkeinrichtungen keine näheren Umstände einer konkreten Gesprächsverbindung betrifft, forderten aber für den Eingriff in das informationelle Selbstbestimmungsrecht eine gesetzliche Ermächtigung. Das LfV sah diese in § 8 Abs.2 Nr.3 HmbVerfSchG („planmäßig angelegte Beobachtungen – Observationen"). Dem konnten wir nicht folgen. Aus Sicht des Betroffenen bzw. der Person, die Ziel nachrichtendienstlicher Mittel ist, besteht zwischen einer optischen Wahrnehmung eines Menschen und einer technischen Ermittlung des Standorts seines Mobilfunkgeräts ein erheblicher Unterschied. Gerade im Bereich der verdeckten Ermittlung stellen das Rechtsstaatsprinzip und die Grundrechte jedoch besondere Anforderungen an die Normenklarheit und Bestimmtheit möglicher Grundrechtseingriffe. Der Bürger muss erkennen können, welche Maßnahmen der Staat ergreifen darf.

Auch die anderen in Betracht kommenden Ermächtigungsgrundlagen im HmbVerfSchG haben wir geprüft, aber nicht für tragfähig gehalten. Im Ergebnis stellten wir vielmehr den Mangel an einer wirksamen Rechtsgrundlage für eine Ortung über Mobilfunkeinrichtungen fest. Darüber hinaus problematisierten wir die Form der Inanspruchnahme privater Dritter (des Netzbetreibers) bei diesem Verfahren.

Das Gutachten stellten wir neben dem LfV auch dem Parlamentarischen Ausschuss vor. In der Folge schlug der Senat im Zusammenhang mit anderen Änderungen von Vorschriften auf dem Gebiet des Verfassungsschutzes (Bü-Drs. 20/6333) auch eine Ergänzung von § 8 Abs.2 Nr.8 HmbVerfSchG (Beobachten und Aufzeichnen des Funkverkehrs) vor. Nach Inkrafttreten des Gesetzes zählt nun auch „die verdeckte Standortbestimmung mit technischen oder telekommunikativen Mitteln" zu den gesetzlich zugelassenen nachrichtendienstlichen Mitteln (Gesetz vom 2.4.2013, GVBl 2013, S.121-130).

Ferner soll die Ortung über Mobilfunkeinrichtungen auch in die Dienstvorschrift „Nachrichtendienstliche Mittel" (vgl. § 8 Abs.2 S.2 HmbVerfSchG) aufgenommen werden. Dabei wiesen wir – wie schon im Gutachten - noch einmal auf unsere Bedenken gegen die Einstufung der gesamten Dienstvorschrift als Verschlusssache hin. Die gesetzlich vorgeschriebene Dienstvorschrift soll die nachrichtendienstlichen Mittel „abschließend" benennen, um dem Rechtsstaatsgebot der Normenklarheit und –bestimmtheit zu genügen. Dann muss aber nach unserer Auffassung auch der normunterworfene Bürger Zugang zu dieser abschließenden Benennung – wenn auch nicht zu allen Erläuterungen - haben. Das LfV hat unsere Bedenken aufgenommen und den Entwurf der Dienstanweisung so angepasst, dass auf eine Einstufung des Inhaltes als Verschlusssache verzichtet werden konnte.

Nicht abschließend geklärt blieb die Rechtsnatur der Einbeziehung des privaten Dienstleisters (Netzbetreibers) in die Ortungen über Mobilfunkeinrichtungen. Das LfV bedient sich eines Partners des Bundesamts für Verfassungsschutz (BfV). Der Auffassung des LfV, es handele sich um die bloße Einholung einer Auskunft bei diesem, steht unsere Auffassung einer Auftragsdatenverarbeitung im Sinne des § 3 HmbDSG gegenüber. Die aus unserer Meinung abzuleitenden Verantwortlichkeiten und Kontrollpflichten des Auftraggebers hat das LfV allerdings unabhängig von der abweichenden Rechtsauffassung für sich anerkannt. Es teilte mit, dass es die zugrundeliegenden vertraglichen Unterlagen des BfV einschließlich der vereinbarten Sicherheitsmaßnahmen geprüft habe.

2.2 BVerfG-Urteil zur Antiterrordatei und die Folgen

Nach dem Urteil des Bundesverfassungsgerichts zum Antiterrordateigesetz (ATDG) haben wir uns bei der Innenbehörde, dem Verfassungsschutz und dem Landeskriminalamt versichert, dass die Voraussetzungen für eine eingeschränkte Weitergeltung bis zur angemahnten Gesetzesänderung eingehalten werden.

Mit Urteil vom 24. April 2013 erklärte das Bundesverfassungsgericht die Errichtung einer Antiterrordatei verschiedener Sicherheitsbehörden grundsätzlich für verfassungsgemäß. Hinsichtlich des Datenaustauschs zwischen Polizeibehörden und Nachrichtendiensten folgerte das Gericht aus dem Datenschutzgrundrecht jedoch ein „informationelles Trennungsprinzip". Dieses verlange für eine Verbunddatei wie die Antiterrordatei eine normenklare und „dem Übermaßverbot entsprechende" Festlegung insbesondere der zu erfassenden Daten und der Möglichkeiten ihrer Nutzung. Gegen diese Forderung verstoße eine Reihe von Regelungen des ATD-Gesetzes:

1. die Speicherung von Daten über Personen, die terroristische Vereinigungen und Gewaltanwendungen nur indirekt fördern (unterstützen von Unterstützern; befürworten von Gewalt);

2. die Speicherung von Daten bloßer Kontaktpersonen, die nicht selbst terrorismusverdächtig sind,

3. die uneingeschränkte Einbeziehung von Daten, die durch Eingriffe in das Brief- und Fernmeldegeheimnis und in das Recht auf Unverletzlichkeit der Wohnung erhoben wurden,

4. der Zugriff auf „erweiterte Grunddaten" einer betroffenen Person, wenn die Suche ohne den Namen der Person, sondern nur anhand einzelner Merkmale erfolgt („Invers"-Suche).

Zur Neuregelung der beanstandeten Normen setzte das Gericht dem Gesetzgeber eine Frist bis Ende 2014. Eine übergangsweise Fortgeltung der für verfassungswidrig erklärten Normen gelte bis dahin nur für die unter 1. genannten Regelungen. Die unter 2.- 4. genannten Regelungen müssten dagegen – außer in Eilfällen - auch in der Übergangszeit ausgesetzt werden.

Ferner betonte das Bundesverfassungsgericht die Bedeutung der Kontrolle durch die Datenschutzaufsichtsbehörden. Diese bezieht sich besonders auf die Auswertung der Protokolldaten „in angemessenen Abständen - ...etwa zwei Jahre...". Die Kontrolle fordere zudem eine effiziente Kooperation der Datenschutzbeauftragten untereinander.

Mit Schreiben vom 21. Juni 2013 wendeten wir uns an die Behörde für Inneres und Sport sowie an die Leiter des Landeskriminalamtes und des Landesamts für Verfassungsschutz. Wir stellten die wesentlichen Aussagen des Urteils und die aus unserer Sicht auf Landesebene zu ziehenden Konsequenzen dar. Auch soweit das Gericht eine Fortgeltung verfassungswidriger Normen bis Ende 2014 zuließ, forderten wir zu einer vorgezogenen Anpassung der Praxis auf.

Am 19. Juli 2013 antwortete uns der Staatsrat der Behörde für Inneres und Sport und fügte Stellungnahmen des Bundesinnenministeriums, des Bundesamts für Verfassungsschutz und des Bundeskriminalamtes bei. Danach wurden in Hamburg Daten zu Kontaktpersonen entweder in der Vergangenheit gar nicht erhoben oder in der Zwischenzeit gelöscht. Dasselbe gelte für Daten, die aus Eingriffen in das Wohnungsgrundrecht oder in das Brief- und Fernmeldegeheimnis stammten. Eine Inverssuche werde derzeit weder von der Polizei noch vom Landesamt für Verfassungsschutz durchgeführt. Daten von Personen, die Terrorismus oder Gewalt nur indirekt fördern, seien von der Polizei nicht gespeichert und vom LfV nicht in die Antiterrordatei eingestellt worden.

Damit entspricht die gegenwärtige Hamburger Praxis aus unserer Sicht den Vorgaben des Bundesverfassungsgerichts für die Übergangszeit bis Ende 2014.

Der von der Innenbehörde zitierte Beschluss der Innenministerkonferenz vom Mai 2013 sowie die Ausführungen der Bundesinstitutionen lassen erkennen, dass die Vorgaben des Bundesverfassungsgerichts auch dort geprüft und umgesetzt werden sollen, aber gleichzeitig weiterhin eine effiziente Bekämpfung der Terrorismusgefahr durch die erforderliche Zusammenarbeit der Sicherheitsbehörden aufrecht zu erhalten ist. Auch die Datenschutzbeauftragten des Bundes und der Länder kooperieren in ihrem Arbeitskreis Sicherheit und begleiten die Umsetzung des BVerfG-Urteils durch Gesetzgeber und Verwaltungspraxis. Auf die vom Gericht ausdrücklich angemahnte regelmäßige Kontrolle durch die Landesdatenschutzbeauftragten haben wir auch die Leitung der Behörde für Justiz und Gleichstellung aufmerksam gemacht, die für die personelle und sachliche Ausstattung unserer Dienststelle mitverantwortlich ist (zur defizitären personellen Situation der Dienststelle siehe oben).

2.3 Datenerfassung zur Werbung von V-Leuten

Mit dem Landesamt für Verfassungsschutz erörtern wir die Datenverarbeitung im Zusammenhang mit der Ansprache, Anwerbung und Mitarbeit von V-Leuten für den Verfassungsschutz.

Kurz vor Redaktionsschluss übersandte uns das Landesamt für Verfassungsschutz (LfV) auf unsere Erinnerung hin die Verfahrensbeschreibung zu einer Datei, mit der das LfV die Anwerbung und Mitarbeit von V-Leuten bereits seit 2010 unterstützt. Durch einen Personalwechsel war beim LfV die eigene Zusage in Vergessenheit geraten, die Datei erst nach einer Zustimmung durch den Hamburgischen Datenschutzbeauftragten in Betrieb zu nehmen.

In unserer Stellungnahme vertraten wir folgende Auffassung:

Eine Datenverarbeitung zum Zwecke der Anwerbung von V-Leuten, z.B. zur Feststellung der persönlichen Eignung eines „Kandidaten", kann sich nur sehr begrenzt auf § 8 bzw. § 9 Hamburgisches Verfassungsschutzgesetz stützen, der den verdeckten Einsatz nachrichtendienstlicher Mittel regelt – etwa zur Schaffung der „erforderlichen Nachrichtenzugänge". Fraglich ist, ob die „Erhebung" und „Verwendung" in diesem Stadium der V-Leute-Anwerbung auch eine Datenspeicherung in einer Datei rechtfertigt.

Wer nach „Eignungsprüfung" als V-Person nicht in Betracht kommt bzw. vom LfV aus welchen Gründen auch immer nicht angesprochen wird, muss so gestellt werden, wie jeder andere, der nichts mit dem Verfassungsschutz zu tun hat; denn es liegt nicht in der Hand der betroffenen Person, ob das LfV sie für geeignet hält, als V-Person angeworben zu werden. Damit kommt nach unserer Auffassung eine Speicherung personenbezogener Daten der nicht weiter umworbenen Personen in einer Datei des LfV grundsätzlich nicht in Betracht.

Wird eine Person vom LfV angesprochen, hat das LfV das Grundrecht dieser Person auf informationelle Selbstbestimmung zu achten. Das bedeutet, dass das LfV sie darüber aufklären muss, welche Daten es über sie erhoben hat und wie sich die weitere Datenverarbeitung im Falle der Ablehnung oder der Mitarbeit gestalten wird. Denn dies ist auch eine der Grundlagen für die Entscheidung der angesprochenen Person.

Lehnt die Person die Mitarbeit kategorisch ab, muss sie so gestellt werden wie jeder andere, der nichts mit dem Verfassungsschutz zu tun hat. Stimmt sie der Mitarbeit als V-Person zu, ist sie über die weitere Datenerhebung und –verarbeitung beim LfV aufzuklären.

Scheidet eine V-Person aus der Zusammenarbeit mit dem LfV aus, muss es weitgehend ihr überlassen bleiben zu bestimmen, welche Daten weiterhin wie lange über sie gespeichert werden. Angesichts der potentiellen Brisanz und Gefährlichkeit der Eintragung in einer V-Leute-Datei des LfV werden die Interessen des LfV im Konfliktfall häufig hinter den (ggf. Überlebens-)Interessen der betroffenen Person zurücktreten.

Vor Redaktionsschluss konnte die Auseinandersetzung mit dem LfV zu dem Verfahren nicht abgeschlossen werden.

3. Justiz

3.1 Übersendung von Anklageschriften an die Ausländerbehörde

Bei Strafverfahren gegen Ausländer konnten die Mitteilungen der Staatsanwaltschaft an die Ausländerbehörde auf das erforderliche und zulässige Maß reduziert werden; insbesondere erhält die Ausländerbehörde nicht mehr regelmäßig eine Kopie von Anklageschrift oder Strafbefehlsantrag.

Für die Information der Ausländerbehörde über Strafverfahren gegen Ausländer benötigt die Staatsanwaltschaft eine gesetzliche Grundlage. Diese findet sich in § 87 Aufenthaltsgesetz (AufenthG): Nach Abs.4 haben die für die Einleitung und Durchführung von Straf- und Bußgeldverfahren zuständigen Stellen „die zuständige Ausländerbehörde unverzüglich über die Einleitung des Strafverfahrens sowie die Erledigung des Straf- oder Bußgeldverfahrens bei der Staatsanwaltschaft, bei Gericht ... unter Angabe der gesetzlichen Vorschriften zu unterrichten". Die Allgemeine Verwaltungsvorschrift zu § 87 AufenthG (AVwV) und Nr.42 der Anordnung über die Mitteilungen in Strafsachen (MiStra) konkretisieren den Umfang dieser Pflicht. Danach sind neben dem Umstand der Verfahrenseinleitung bzw. -erledigung und den zugrunde liegenden gesetzlichen Vorschriften auch Namen, Geburtsdaten, Staatsangehörigkeit und Anschrift „mit anzugeben".

In der Vergangenheit erfüllte die Staatsanwaltschaft diese Mitteilungspflicht mit Übersendung der gesamten Anklageschrift bzw. des vollständigen Strafbefehlsantrages. Hierin sind jedoch regelmäßig Daten enthalten, die über den genannten Übermittlungsumfang weit hinausgehen. So enthalten Anklageschriften auch Daten über Opfer, Zeugen, Sachverständige sowie die Tatumstände im Einzelnen, welche für die Erfüllung der Übermittlungspflicht nach § 87 Abs.4 AufenthG regelmäßig nicht erforderlich sind. Außerdem bilden Anklageschrift und Strafbefehlsantrag nur einen Zwischenteil eines Strafverfahrens, leiten dieses jedoch weder ein noch schließen sie es ab.

Die von uns angeschriebene Staatsanwaltschaft berief sich dagegen auf § 87 Abs.2 S.1 Nr.3 AufenthG: Danach hat jede öffentliche Stelle, die von „einem sonstigen Ausweisungsgrund" Kenntnis erlangt, die Ausländerbehörde zu informieren. Ein solcher Ausweisungsgrund kann nach § 55 Abs.2 Nr.3 AufenthG im Einzelfall auch einmal in einem hinreichenden Straftatverdacht bestehen, der immer Voraussetzung für eine Anklageerhebung ist. Dabei kommt es für die Qualifizierung als Ausweisungsgrund jedoch auf den konkreten Straftatvorwurf und weitere Umstände an. Eine regelmäßige Übersendung der Anklageschrift kommt danach nicht in Betracht und kann wie gezeigt auch die Unterrichtungspflicht nach § 87 Abs.4 AufenthG nicht erfüllen.

Für die regelmäßige Unterrichtung der Ausländerbehörde über Strafverfahren gegen Ausländer kommt deswegen nur § 87 Abs.4 AufenhG in Verbindung mit Nr. 42 Mistra als lex specialis in Frage, d.h. der Ausländerbehörde sind nur Einleitung und Ausgang eines Verfahrens „unter Angabe der gesetzlichen Vorschriften" sowie die Namen, Geburtsdaten, Anschriften und Staatsangehörigkeit(en) des Betroffenen zu übermitteln. Hierüber waren und sind wir uns auch mit den anderen Landesdatenschutzbeauftragten einig. Die Staatsanwaltschaften der anderen Bundesländer agieren bei der Mitteilung nach Nr. 42 MiStra unterschiedlich; einige wenige bestehen weiterhin auf der Versendung von Kopien der Anklageschriften oder Strafbefehlsanträge. Andere haben hierauf schon immer verzichtet. Nach ausführlicher vorbereitender Korrespondenz unterrichtete uns der Leitende Oberstaatsanwalt der Staatsanwaltschaft Hamburg am 1. August 2013 über eine Änderung des bisherigen Mitteilungsverfahrens nach Nr. 42 MiStra:

Für alle ab 1.8.2013 bei der Staatsanwaltschaft Hamburg eingehenden und im Vorgangsverwaltungssystem MESTA erfassten Strafverfahren werden der Ausländerbehörde zukünftig zwei Monate nach Erfassung nur noch die oben dargestellten in Nr.42 MiStra genannten Daten übermittelt. Zwei Monate nach endgültiger Verfahrenseinstellung bei der Staatsanwaltschaft werden der Ausländerbehörde auch Art und Datum der Einstellung übermittelt. „Haftbefehle, Strafbefehlsanträge... ...sowie Anklageschriften werden nicht mitgeteilt." Die Mitteilungen werden in MESTA automatisiert erzeugt und als PDF-Dokument „bis auf weiteres postalisch" der jeweils zuständigen Ausländerbehörde übersandt.
Dieses neue Verfahren der Staatsanwaltschaft entspricht unserer Rechtsauffassung.

3.2 Auskunft an Betroffene über Ermittlungsdaten der Staatsanwaltschaft

Auf unsere Anregung hat die Staatsanwaltschaft Hamburg ein in Schleswig-Holstein entwickeltes Konzept für die Auskunftserteilung aus dem Vorgangsverwaltungssystem MESTA übernommen.

Nach § 491 Strafprozessordnung (StPO) in Verbindung mit § 19 Bundesdatenschutzgesetz ist jeder Person, die von einem Ermittlungsverfahren der Staatsanwaltschaft betroffen ist bzw. war, auf Antrag Auskunft zu erteilen über die in einer automatisierten Datei zu ihr gespeicherten Daten. Ausgenommen sind Verfahren, die innerhalb von 6 Monaten vor dem Auskunftsbegehren eingeleitet wurden.

Die Staatsanwaltschaft Hamburg verarbeitet ihre Vorgänge - wie auch die in Schleswig-Holstein und einzelnen anderen Bundesländern - im System MESTA. Diese umfangreiche Datei enthält Daten für Zwecke des aktuellen Strafverfahrens (§ 483 StPO), künftiger Strafverfahren (§ 484 StPO) und für Zwecke der Vorgangsverwaltung (§ 485 StPO). Beantragt eine betroffene Person Auskunft nach § 491 StPO, erhielt sie bislang eine äußerst kurz gefasste Information aus MESTA, die im Wesentlichen nur die Verfahrensdaten: Aktenzeichen, Deliktsbezeichnung, Tatzeit und Entscheidung der bisher bei der Staatsanwaltschaft geführten Verfahren enthielt. Diese Kurzauskunft umfasste keineswegs alle zu der Person in MESTA gespeicherten Daten. Eine Vollauskunft müsste andererseits mehrere hundert Datenfelder einbeziehen und würde die betroffene Person mit einer nicht mehr überschaubaren Datenmenge konfrontieren und damit den Sinn des Auskunftsrechts in Frage stellen.

Aus diesem Grunde hatte der schleswig-holsteinische Landesdatenschutzbeauftragte mit der dortigen Staatsanwaltschaft 2012 einen übersichtlichen, aber aussagekräftigen Katalog von Daten verabredet. Dieser wurde in den MESTA-Verbundländern abgestimmt. Nachdem wir die Staatsanwaltschaft Hamburg im August 2012 allgemein auf die Problematik der Auskunft nach § 491 StPO hingewiesen hatten, informierte diese uns im Oktober 2012 darüber, dass sie sich einem abgestimmten Auskunftsumfang anschließen würde. Im April 2013 berichtete die Staatsanwaltschaft Hamburg bereits von der laufenden technischen Umsetzung des gefundenen Konzepts, und im Juni 2013 erhielten wir die allgemeine Muster-Antwort der Hamburger Staatsanwaltschaft auf Auskunftsanträge und die Liste der MESTA-Daten, über die nun Auskunft erteilt wird.

Das allgemeine Anschreiben nennt die rechtlichen Grundlagen und die Ausnahme von der Auskunftspflicht bei Ermittlungen, die in den letzten 6 Monaten eingeleitet wurden. Ergänzend weist es die den Antrag stellende Person darauf hin, dass eine Auskunft über die Herkunft der Daten nicht gegeben wird und die angegebenen Daten eine mit dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit abgestimmte Auswahl aus allen MESTA-Daten darstellt, „die rein interne Datenfelder, die für den Auskunftssuchenden von keinem Informationsgehalt sein dürften, nicht berücksichtigt". Als Anlage wird dem Anschreiben der abstrakte Datenkatalog beigefügt, dem der Antragsteller auch entnehmen kann, zu welchen Datenfeldern keine Informationen über ihn in MESTA gespeichert sind. Der Katalog umfasst insgesamt 22 Personalien-Daten, einschließlich Führerschein- und Insolvenzangaben, 11 Delikts-Daten, 5 Entscheidungs-Daten, 4 U-Haft-Daten, 7 Freiheitsstrafen-Daten, 4 Geldstrafen-Daten, 4 Gnaden-Daten und 5 Ordnungsgeld-Daten.

Diesen in den MESTA-Verbundländern abgestimmten Auskunftsdaten-Katalog begrüßen wir als gelungenen Kompromiss zwischen der bisherigen Kurzauskunft und einer kaum verständlichen Vollauskunft über alle in MESTA gespeicherten Daten.

4. Strafvollzug

4.1 Neue Strafvollzugsgesetze

Unsere Anregungen zum Entwurf eines Gesetzes über den Vollzug der Sicherungsverwahrung (HmbSVVollzG) und zur Änderung anderer Justizvollzugsgesetze wurden teilweise übernommen.

Anfang Oktober 2012 erreichte uns der Entwurf für ein HmbSVVollzG und Änderungen geltender Vollzugsgesetze. In unserer Stellungnahme gaben wir insbesondere folgende Anregungen:

- Klarere Benennung der Beteiligten von Vollzugsplan-Konferenzen,
- Verzicht auf externe psychiatrische oder psychologische Fachkräfte für Stellungnahmen zu Vollzugslockerungen,
- Übernahme der Begrifflichkeit des Hamburgischen Datenschutzgesetzes zur Videoüberwachung (Oberbegriff für Beobachtung und Aufzeichnung),
- Besuchsüberwachung durch Videokameras nur als Ausnahmeregelung,
- Klarere Regelung, wer einen Gesprächspartner von einer beabsichtigten Telefonüberwachung unterrichtet,
- Klarstellung, dass die allgemeine Anordnungsbefugnis der Vollzugsleitung keine Befugnis zur Verarbeitung personenbezogener Daten enthält,
- Berücksichtigung der Schweigeverpflichtung von Bewährungshelfern, so weit sie Sozialarbeiter oder Sozialpädagogen sind,
- Keine vorsorgliche Datenübermittlung von der JVA an „künftig zuständige" Bewährungshelfer/innen.

Die Behörde für Justiz und Gleichstellung (BJG) lehnte leider alle unsere Anregungen zu Regelungen ab, die aus anderen, bereits geltenden Vollzugsvorschriften in den SVVollzG-Entwurf übernommen worden waren. Dies betraf (s.o.) die Benennung von Beteiligten der Vollzugsplan-Konferenzen, die Besucherüberwachung durch Videokameras und die Unterrichtung von Telefongesprächspartnern. Allerdings übernahm die BJG die datenschutzrechtliche Terminologie zur Videoüberwachung / -beobachtung nicht nur im SVVollzG-E, sondern auch in den anderen Vollzugsgesetzen. Die Stellungnahme für Vollzugslockerungen werde nicht „extern", sondern von „vollzuglichen Mitarbeiterinnen oder Mitarbeitern" erstellt, die bisher nicht mit dem konkreten Gefangenen befasst waren. Die Anordnungsbefugnis der Vollzugsleitung umfasse keine spezialgesetzliche Befugnis zur Verarbeitung personenbezogener Gefangenendaten.

Hinsichtlich der Einbindung von Bewährungshelfern in die Vollzugs-Kommunikation blieb die BJG zunächst bei Ihrer Auffassung, weil der frühzeitige und möglichst umfassende Informationsaustausch für einen effizienten Vollzug besonders wichtig sei.

Im Oktober 2012 kam die BJG jedoch auf unsere Anregung zurück: Sowohl bei der Behandlungsuntersuchung des Gefangenen als auch bei den Konferenzen zum Vollzugsplan – bei Vollzugsbeginn und vor der Entlassung - sollten Erkenntnisse der Bewährungshilfe bzw. die Teilnahme von Bewährungshelfern nun von der „Zustimmung der Gefangenen" abhängig gemacht werden.

Da dies die informationelle Selbstbestimmung der Gefangenen hinreichend berücksichtigt – vorausgesetzt, die Freiwilligkeit der Entscheidung kann gewährleistet werden – konnten wir unter Zurückstellung der verbliebenen weniger bedeutenden Kritikpunkte dem Gesetzentwurf schließlich zustimmen.

4.2 Beschwerden und Eingaben

Nur wenige der nicht seltenen Eingaben von Gefangenen hatten Erfolg.

Ein sicherheitsverwahrter Gefangener wandte sich gegen eine einseitig negative und zum Teil identifizierende Presseberichterstattung. Diese habe sich auf staatliche Informationen gestützt. Wir haben die offiziellen Pressekontakte der Gerichte, Staatsanwaltschaft und Justizbehörde nachvollzogen und konnten keine identifizierenden Pressemitteilungen feststellen. Die Behörde hatte keine Namen oder Namensteile veröffentlicht oder weitergegeben. In Beantwortung einer Kleinen parlamentarischen Anfrage sprach sie hinsichtlich der Sicherheitsverwahrten nur von Fallgruppen. Der Gefangene unterschätzte offensichtlich die Möglichkeiten der Presse, durch eigene Recherchen – auch aus eigenen früheren Redaktionsbeiträgen zu Verhaftungen, Prozessen u.ä. – Rückschlüsse auf die Identität der Betroffenen zu ziehen. Das sog. Medienprivileg verwehrt es uns, bei unangemessen identifizierenden Pressebeiträgen die jeweilige Redaktion zu kritisieren. Vielmehr verweisen wir Petenten in diesen Fällen an den Presserat.

Eine andere Eingabe warf einem Vollzugsbediensteten vor, er habe noch nach der Entlassung des Gefangenen wichtige Informationen über diesen an den früheren Arbeitgeber des Gefangenen (als Freigänger) übermittelt. Der Ex-Gefangene habe durch diese Offenbarung Nachteile in einem Arbeitsgerichtsprozess erlitten. Aussagen des Rechtsvertreters des Arbeitgebers bestätigten nach unserer Auffassung die Vorwürfe des Gefangenen; die Einlassung des Vollzugsbediensteten konnte uns nicht überzeugen. Wir haben den Vorgang an das Strafvollzugsamt abgegeben, weil dieses – und nicht der HmbBfDI - für die Verfolgung von datenschutzrechtlichen Ordnungswidrig-

keiten einzelner öffentlich Bediensteter zuständig ist. Das Verfahren wurde später eingestellt.
Eine weitere Beschwerde beklagte die Praxis, dass Gefangene sich bei einem Ausgang für ein Vorstellungsgespräch oder für die Wohnungssuche vom möglichen Arbeitgeber oder Vermieter den Ausgangsschein mit JVA-Kopf abstempeln lassen müssen. Damit würde ihre Inhaftierung offenbart und der Zweck des Ausgangs vereitelt. Auf unsere Anfrage teilte das Strafvollzugsamt mit, dass den Arbeitgebern und Vermietern die Inhaftierung oft bereits durch Vorgespräche bekannt sei. Wenn der Ausgang ohne Zweckbindung, z.B. „zur Pflege sozialer Kontakte" erlaubt und – zulässigerweise - für die Anbahnung von Arbeits- oder Mietverhältnissen genutzt werde, bedürfe es keiner Bestätigung bzw. Gegenzeichnung. In den verbleibenden Fällen, in denen die Bestätigung auf dem Ausgangsschein tatsächlich nicht erforderliche Daten offenbaren würde, könne der Gefangene die Bestätigung auch auf einem neutralen Bogen ohne JVA-Kopf einholen (z.B. „Bestätigung eines Bewerbungsgesprächs mit ... am ... zur Vorlage beim gegenwärtigen Arbeitgeber / Stempel"). Eine nach § 12 HmbStrafVollzG mögliche Weisung für eine Vollzugslockerung sollte die Bestätigung / das Abstempeln auf dem Ausgangsschein mit JVA-Kopf grundsätzlich nicht vorsehen, es sei denn, die Offenbarung der Inhaftierung ist für das angestrebte Rechtsverhältnis – z.B. zum Schutze Dritter – im Einzelfall erforderlich. Darüber sollte das Vollzugspersonal jedoch mit dem Gefangenen zuvor sprechen.

Interessant war auch die Eingabe eines anderen Gefangenen, der aus der Untersuchungshaft heraus verhindern wollte, dass die Staatsanwaltschaft seinem Vermieter Einsicht in die Ermittlungsakte gewährte. Nach Auskunft des Gefangenen suchte sein Vermieter seit langem einen Weg, ihn aus der Wohnung heraus zu drängen, obwohl die Straftat nichts mit dem Mietverhältnis zu tun habe. Wir konnten dem Gefangenen nur raten, der Staatsanwaltschaft seine Sicht der unterschiedlichen Interessen und Hintergründe vorzutragen bzw. über den Verteidiger vortragen zu lassen. Die Staatsanwaltschaft muss nach § 475 Strafprozessordnung das „berechtigte Interesse" des Vermieters prüfen und mit dem „schutzwürdigen Interesse" des Betroffenen abwägen. Wir haben den Betroffenen darauf hingewiesen, dass gegen die Entscheidung der Staatsanwaltschaft nach § 478 Abs.3 StPO eine richterliche Entscheidung beantragt werden kann. Eine datenschutzrechtliche Kontrolle der staatsanwaltschaftlichen Entscheidung musste dahinter zurückstehen.

Andere Eingaben bezogen sich auf den inneren Vollzugsbetrieb, die Handhabung von Anträgen und Beschwerden und die Postkontrolle. Soweit wir den tatsächlichen Sachverhalt aufklären konnten, gab es im Ergebnis keinen Anlass zu Beanstandungen gegenüber der JVA oder dem Strafvollzugsamt.

5. Gesundheitswesen

5.1 Bußgeld wegen Altakten-Entsorgung durch Asklepios-Klinik

Eine nicht ordnungsgemäße Entsorgung von Krankenhausakten durch mehrere Dienstleistungsunternehmen offenbarte eine unzureichende Organisation und Kontrolle durch die verantwortliche Auftraggeberin Asklepios Kliniken Hamburg GmbH. Wir haben dies mit einem Bußgeld geahndet.

Im März 2012 teilte uns ein Journalist mit, er habe personenbezogene Krankenhausakten aus einem offen zugänglichen Entsorgungscontainer mit Hunderten von Aktenordnern sichergestellt. Wir informierten daraufhin die Polizei, die vor Ort ermittelte und weitere Altakten an sich nahm. Sie sah jedoch keinen strafrechtlichen Tatvorwurf und gab den Vorgang zur Verfolgung einer möglichen datenschutzrechtlichen Ordnungswidrigkeit an uns ab.

Noch am selben Tage meldete die Asklepios Kliniken Hamburg GmbH (Asklepios GmbH) ihrerseits den „Datenschutzvorfall" und kündigte Strafanzeige wegen Diebstahls der Altakten an. Sie stellte detailliert die näheren Tatumstände dar und kündigte Maßnahmen zur Sicherung der Altakten und zur weiteren Aufklärung an.

Unsere tatsächliche und rechtliche Prüfung der näheren Umstände ergab, dass der Asklepios GmbH eine unbefugte Daten"verarbeitung" - etwa eine Übermittlung geschützter Personal- oder Patientendaten an Dritte - nicht vorzuwerfen war. Die Versäumnisse der Auftragnehmer waren der Asklepios GmbH nicht zuzurechnen. Wir verlangten aber, dass die Asklepios GmbH das Krankenhaus-Grundstück und die Entsorgungscontainer vor dem Zugriff Dritter besser sicherte. Ferner forderten wir die Asklepios GmbH auf, die Auftragnehmer über ihre Datenschutz- und Datensicherungspflichten zu belehren und uns die vertraglichen Auftragsunterlagen vorzulegen.

Da es sich um viele Jahre alte Akten aus der Personalverwaltung und Abrechnungsabteilung handelte, die sichergestellten Akten der ordnungsgemäßen Vernichtung zugeführt wurden und kein Anhaltspunkt für eine Entwendung weiterer Akten vorlag, drohte nach unserer Ansicht keine „schwerwiegende Beeinträchtigung" der Betroffenen. Eine solche hätte nach § 42a Bundesdatenschutzgesetz (BDSG) - neben der erfolgten Benachrichtigung der Aufsichtsbehörde - eine individuelle Information von Hunderten Betroffener erforderlich gemacht.

Mitte April 2012 übersandte uns die Asklepios GmbH die Dokumentation der Auftragsverhältnisse, die zum Zwecke der Altakten-Entsorgung abgeschlossen worden waren. Danach waren an der Entsorgungs-Aktion vier Unternehmen beteiligt, eines davon als Unterauftragnehmer. Der Auftrag zum Einpacken von ca.450 Aktenordnern und zur

Ablage in bereitgestellte Entsorgungscontainer erfolgte nach einem kurzen Angebot durch eine schriftliche „Bestellung", die weder Hinweise auf die datenschutzrechtliche Sensibilität der Akten noch Anforderungen an notwendige Sicherheitsmaßnahmen enthielt. Der Auftrag zum An- und Abfahren der Entsorgungscontainer wurde aufgrund eines (Sonder-)Angebots „Aktion Aktenvernichtung an ‚unsere Treukunden'" telefonisch erteilt. Eine Spezifizierung der Entsorgungscontainer unterblieb ebenso wie eine Vereinbarung notwendiger Sicherheitsmaßnahmen zum Schutz der sensiblen Daten in den zu entsorgenden Ordnern. Auch über die Unterbeauftragung einer Aktenvernichtungsfirma traf die Asklepios GmbH keine Feststellungen mit dem Container-Unternehmen. In dem schriftlichen Unterauftrag wurde dann nur Bezug genommen auf „Kundendaten", nicht aber auf die der Schweigepflicht unterliegende Patienten- und Mitarbeiterdaten der Asklepios GmbH. Ein vierter Dienstleister übernahm die Vorbereitung und Einweisung der Mitarbeiter und das „Koordinieren des Abtransportes".

Die Entsorgung der Altakten stellte für die Asklepios GmbH eine Auftragsdatenverarbeitung – nämlich die Löschung / Vernichtung personenbezogener Daten - im Sinne des § 11 BDSG dar. Diese Norm fordert eine schriftliche Auftragserteilung mit Festlegungen zu zehn vorgegebenen Vertragsgegenständen, unter anderem zu Unterauftragsverhältnissen. Der Auftraggeber muss sich zudem vor und während der Auftragsdurchführung von der Einhaltung der verabredeten Sicherheitsmaßnahmen überzeugen.

Nach unseren Feststellungen hatte die Asklepios GmbH die Aufträge jedoch – wie dargestellt - „nicht in der vorgeschriebenen Weise erteilt" und sich auch nicht ausreichend von der „Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt" und damit nach § 43 Abs.1 Nr.2b BDSG eine Ordnungswidrigkeit begangen. Wir verhängten deswegen ein vierstelliges Bußgeld, gegen das kein Einspruch eingelegt wurde.

5.2 Neuer Behandlungsvertrag für die Asklepios-Kliniken

Um Patienten bei der Krankenhausaufnahme nicht zu überfordern, haben wir mit der Asklepios Kliniken Hamburg GmbH den Standard-Behandlungsvertrag und die verschiedenen Einwilligungserklärungen auf das unverzichtbare Minimum reduziert.

Obwohl die Asklepios Kliniken Hamburg GmbH (Asklepios GmbH) schon Ende 2008 Ideen zur Eindämmung der Vordruck- und Erklärungsflut entwickelt hatte, bedurfte es zur datenschutzrechtlichen Abstimmung des Standard-Behandlungsvertrags nebst Einwilligungen noch mehrerer Jahre.

Zu klären waren im Wesentlichen folgende Fragen:

- Muss der Patient bei der Krankenhausaufnahme auch in die Einbeziehung jedes einzelnen externen Dienstleisters einwilligen?
- Gilt dies auch für mit- und nachbehandelnde Leistungserbringer und für Dienstleister, die das Krankenhaus nur selten bzw. in besonderen Fällen beauftragt?
- Muss der Patient einwilligen bzw. widersprechen können, dass das Krankenhaus frühere Behandlungsunterlagen aus demselben Haus oder aus anderen Asklepios-Häusern zur aktuellen Behandlung heranzieht?
- Kann das Krankenhaus die Aufnahme eines Patienten verweigern, wenn dieser die vorgesehenen Einwilligungen nicht erteilt?
  Muss das Krankenhaus dem Patienten die Möglichkeit geben, einzelne Vertragsbestandteile abzulehnen, oder kann es im Sinne einer „Alles oder Nichts-Lösung" nur die eine Unterschrift unter das „Gesamtpaket" fordern?

Nach einem umfangreichen schriftlichen Meinungsaustausch, persönlichen Gesprächen und Formulierungsvorschlägen unsererseits gestaltete die Asklepios GmbH ihre Aufnahmeunterlagen wie folgt (hier am Beispiel der Asklepios Klinik Barmbek):

Der eigentliche Behandlungsvertrag besteht nun aus 2 Sätzen unter Bezugnahme auf die Allgemeinen Vertragsbedingungen (AVB) und mit einem Hinweis auf Wahlleistungsvereinbarungen mit Selbstzahlungspflicht. Außerdem ist für die Entgegennahme u.a. des Behandlungsvertrages, der AVB und „des Hinweises auf die Datenverarbeitung, einschließlich Einverständniserklärung zur Datenübermittlung" ein Empfangsbekenntnis zu unterzeichnen.

In dem letztgenannten Hinweis bekommt der Patient verschiedene Wahlmöglichkeiten:

- Er kann sich durch Ankreuzen von ja-/nein-Feldern einverstanden erklären, dass die aufnehmende Klinik Unterlagen aus anderen Asklepios-Kliniken heranzieht – über die Heranziehung früherer Unterlagen der aufnehmenden Klinik selbst wird der Patient nur informiert.
- Er kann sich in derselben Weise einverstanden erklären, dass das aufnehmende Krankenhaus dem zu benennenden Hausarzt und/oder Facharzt die Krankenhausunterlagen übermittelt
- und/oder deren Unterlagen für die aktuelle Behandlung abfordert.
- Nur durch seine Unterschrift unter den Hinweis insgesamt (nicht durch Ankreuzen eines entsprechenden ja/nein-Feldes) erklärt sich der Patient damit einverstanden, dass seine Behandlungsdaten – „bei Bedarf" - an ein bezeichnetes externes Labor, an das Hamburger Gesundheitszentrum (Entlassungsmanagement) und gegebenenfalls an weitere drei namentlich benannte kooperierende Facharztpraxen übermittelt werden. Der Verzicht auf die Unterschrift hier lässt den Vertrag insgesamt – und damit die Aufnahme im Krankenhaus – scheitern.

Diesem zweieinhalb-seitigen Musterformular haben wir Ende November 2012 im Ergebnis zugestimmt. Es bleibt übersichtlich und gewährt bei den ersten drei Punkten die notwendigen datenschutzrechtlichen Wahlmöglichkeiten. Insbesondere ist eine Liste mit 40 Dienstleistungsunternehmen entfallen, deren Beauftragung der Patient in der Asklepios Klinik St.Georg früher zustimmen sollte. Einer Einwilligung bedarf es jedoch weder bei einer (meist technischen) Auftragsdatenverarbeitung im Sinne des § 9 Hamburgisches Krankenhausgesetz (HmbKHG) noch bei der Datenübermittlung an regelmäßig in die Behandlung einbezogene Kooperationspartner, § 11 Abs.1 Nr.1 HmbKHG.

Akzeptiert haben wir auch den vierten Punkt, dass nämlich bei einer Verweigerung der Datenübermittlung an die oben genannten externen Leistungserbringer die Klinik-Aufnahme abgelehnt wird: Diese externen Datenempfänger sind konstitutiver Teil der Behandlungsorganisation, zu der es – für einzelne Patienten - keine zumutbare Alternative gibt. Das Ankreuzen der ja/nein-Felder (Punkte 1 bis 3) muss dagegen Ausdruck echter Wahlfreiheit und informationeller Selbstbestimmung des Patienten bleiben und darf die Krankenhausaufnahme nicht beeinflussen.

5.3 Beanstandung des UKE wegen Notzugriffsberechtigung

Die Möglichkeit jedes UKE-Arztes, über einen „Not-Zugriff" auf die Behandlungsdaten aller UKE-Patientendaten zuzugreifen, wurde bis 2012 unverhältnismäßig oft genutzt. Dies beanstandeten wir formell und konnten in der Folge eine drastische Abnahme dieser Zugriffszahlen erreichen.

Bereits im 22.TB 2008/2009, III 9.2 und im 23.TB 2010/2011, III 9.1.3 machten wir auf die Probleme der Notzugriffsberechtigung aller UKE-Ärztinnen und –Ärzte aufmerksam: Jeder Mediziner des UKE-Konzerns kann außerhalb seines Zuständigkeits- und Berechtigungsbereichs mit der Funktion „user contact" des Krankenhausinformationssystems SOARIAN nach Patientennamen suchen und bei Treffern auf die vollständigen Behandlungsdokumentationen zugreifen. Zwar ist der Zugriff verbunden mit einem Hinweis auf die Ausnahmeberechtigung, die Verfolgung missbräuchlicher Zugriffe und die Protokollierung des Zugriffs sowie mit der Aufforderung, einen Grund für den Zugriff anzugeben. Dennoch bleiben prominente Patienten, im UKE behandelte Kolleginnen und Kollegen, aber auch Nachbarn, Freunde und Bekannte dem Risiko ausgesetzt, von ärztlichen Mitarbeitern des UKE unerkannt ausfindig gemacht und medizinisch ausgeforscht zu werden. Wie wir angesichts der zunehmenden Implementierung von SOARIAN vermuteten, sich aber erst später nachweisen ließ, stieg die Anzahl der Notzugriffe kontinuierlich an: von 4000 im Januar 2010 auf über 11.500 im März 2012. Dies entsprach einem Anteil von 0,47 % aller Zugriffe auf elektronische Patientendaten in diesem Monat.

In mehreren Gesprächen mit dem UKE hatten wir deutlich gemacht, dass wir die Anzahl der Zugriffe über „user contact" nicht für vertretbar und eine aussagekräftige Dokumentation wie auch eine stärkere Kontrolle der Zugriffsgründe für erforderlich hielten. Das UKE strebte seinerseits eine Notzugriffs-Quote von höchstens 0,1% aller Zugriffe an. Außer der Zugriffszahl vom Oktober 2010 und einem Auswertungskonzept 2011 wurden uns bis Anfang 2012 jedoch keine weiteren Unterlagen vorgelegt, insbesondere erreichten uns trotz Erinnerung keine neuen Zugriffszahlen.

Mit Schreiben vom 4. März 2012 sprachen wir deswegen gegenüber dem Vorstand des UKE eine formelle Beanstandung nach § 25 Hamburgisches Datenschutzgesetz (HmbDSG) aus. Wir kritisierten das Fehlen erforderlicher technischer und organisatorischer Maßnahmen nach § 8 HmbDSG, um die Vertraulichkeit und die Revisionsfähigkeit von Zugriffen auf Patientendaten über die Notfallberechtigung „user contact" zu gewährleisten. Wir forderten das UKE auf,

- eine Aufstellung über die Anzahl der monatlichen Zugriffe seit Januar 2012 vorzulegen,
- das schon vereinbarte Protokollauswertungskonzept umzusetzen,
- mit dem wissenschaftlichen Personalrat des UKE eine Dienstvereinbarung zur Protokollauswertung abzuschließen und
- die „Prozessablaufprobleme" in Angriff zu nehmen, die das UKE für einen Großteil der „user contact"-Zugriffe verantwortlich machte.

Unabhängig von seinen eher rechtfertigenden Presseerklärungen, Hausmitteilungen und dem Beitrag zu einer Parlamentarischen Kleinen Anfrage (20/3507) reagierte das UKE auf die Beanstandung konstruktiv. In einem Gespräch am 19. März 2012 legte es eine vollständige monatliche Zugriffsdokumentation von Januar 2010 bis Februar 2012 sowie eine Analyse der hauptbetroffenen Abteilungen vor – auffällig war vor allem die Anästhesie. Die schriftliche Stellungnahme des UKE vom 30.3.2012 erläuterte die Gründe für häufige Rückgriffe auf die Funktion „user contact" und nannte konkrete Maßnahmen zur Behebung der beanstandeten Defizite.

In der Folgezeit korrigierte das UKE das Berechtigungskonzept in einzelnen Abteilungen, stellte die Suchmöglichkeit für Forschung und Labore auf Fallnummern statt Namen um und schloss im April 2012 eine Dienstvereinbarung mit dem Wissenschaftlichen Personalrat über die Auswertung der Zugriffsprotokolle ab. Ferner verabredeten wir regelmäßige Quartalsbesprechungen mit dem IT-Leiter, der internen Datenschutzbeauftragten und dem für Personalratsangelegenheiten zuständigen Mitarbeiter des UKE.

Bereits im April 2012 sanken die user-contact-Zugriffszahlen daraufhin auf unter 7.500 und eine Quote von 0,32 %. Im August 2012 wurde eine Quote von 0,21 % und damit mehr als eine Halbierung der Zugriffszahlen vom März 2012 erreicht. Diesen Erfolg nahmen wir zum Anlass für eine entsprechende Pressemitteilung. Im April 2013 sank

die Zugriffsquote auf 0,17 %. Auch gegen Ende des Berichtszeitraums setzte das UKE durch abteilungsbezogene Analysen und Korrekturen sowie eine zielgenauere Auswertung der Zugriffsprotokolle seine Bemühungen um eine weitere Reduzierung der Notfallzugriffe fort.

5.4 Änderungen der Gesetze zu psychischen Krankheiten und zum Maßregelvollzug

Den langwierigen Prozess zur Änderung des Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (HmbPsychKG), des Gesetzes über den Vollzug von Maßregeln der Besserung und Sicherung (HmbMVollzG) sowie des Hamburgischen Ausführungsgesetzes zum Betreuungsbehördengesetz (HmbAGBtG) haben wir insbesondere hinsichtlich der Videoüberwachung von Patienten erfolgreich begleitet und beeinflusst.

Nachdem wir schon 2010 das datenschutzrechtliche Problem der Videoüberwachung von Psychiatriepatienten aufgeworfen und 2011 eine restriktive Übergangsregelung mit der Gesundheitsbehörde abgestimmt hatten, erhielten wir im November 2012 den ersten Gesetzentwurf zur Änderung von PsychKG, MVollzG und HmbAGBtG zur Stellungnahme. Neben der Beleihung von Privaten und dem Thema „Zwangsbehandlung" waren datenschutzrechtlich die Regelungen zur Videoüberwachung und die Schaffung einer Rechtsgrundlage für die Datenerhebung der Betreuungsbehörde bei Dritten von besonderem Interesse.

Wir regten an, die Videoüberwachung grundsätzlich nicht an eine subjektive Absicht („zur Abwehr von Gefahren"), sondern objektiv an die Erforderlichkeit zur Gefahrenabwehr zu binden. Auch baten wir angesichts der Einbeziehung des „Geländes der Krankenhausabteilung" in den zugelassenen Überwachungsbereich um einen Verzicht auf die räumliche Ausdehnung auch noch auf die „unmittelbare Umgebung" des Krankenhauses. Schließlich war die Reichweite der Überwachung in Bezug auf andere Personen (andere Patienten, Besucher, Dritte) zu klären. Der neuen Befugnis der Betreuungsbehörde, zur Klärung des Sachverhalts für das Betreuungsgericht Daten bei Dritten zu erheben, konnten wir zustimmen, weil sie – wenn möglich – an die Einwilligung der psychisch kranken Person sowie an eine Abwägung mit deren schutzwürdigen Interessen gebunden war.

Der zweite Entwurf des Änderungsgesetzes vom Januar 2013 setzte unsere Anregungen vollständig um. Im März 2013 folgte eine dritte Abstimmungsrunde. In unserer Stellungnahme zu diesem Entwurf wiesen wir ergänzend darauf hin, dass die Videoüberwachung von „gemeinschaftlich genutzten Bereichen" nur beispielhaft („insbesondere") konkretisiert und die Überwachung z.B. von Sanitärräumen nicht ausgeschlossen wird. Ferner schlugen wir vor, im Falle der Beleihung Privater die Einsicht

in die hoch sensiblen Patientenakten durch die Rechts- und Fachaufsichtsbehörde von der Erforderlichkeit für deren Aufgabenwahrnehmung abhängig zu machen.

Im Mai 2013 erhielten wir einen weiteren Gesetzentwurf, der die Videoüberwachung von Psychiatriepatienten neu regelte, ohne unsere letzten Anregungen umzusetzen. Dennoch konnten wir unsere Vorbehalte zurückstellen, weil die neue Gesamtregelung mit einem eindeutigen Verbot der Videoüberwachung in psychiatrischen Abteilungen beginnt und dann restriktive Ausnahmeregelungen anschließt. Neu ist die Videoüberwachung nicht fixierter Patienten in sog. „weichen Räumen". Einer solchen Überwachung darf der „natürliche Wille" der betroffenen Person nach einer Aufklärung nicht entgegenstehen, es muss die Gefahr einer Fremd- oder Selbstgefährdung bestehen und ein umfangreicher Katalog von organisatorischen Sicherungsmaßnahmen eingehalten werden. Im Übrigen wiederholten wir unsere Auffassung, dass eine Videoüberwachung von Sanitärräumen nicht in Betracht kommt.

Im Juni 2013 nahmen wir zu diesem Gesetzentwurf an einer Sachverständigenanhörung im Gesundheitsausschuss der Bürgerschaft teil. Neben dem fachlichen Hauptthema „Zwangsbehandlung von Untergebrachten" kam auch der Datenschutz zur Sprache. Angesichts der strengen Voraussetzungen für eine Videoüberwachung von Psychiatriepatienten konnten wir uns auf die bereits vorgetragenen Anmerkungen beschränken und auf eine grundsätzliche Kritik verzichten. Wichtig war den Parlamentariern unsere Bestätigung, dass nach dem Wortlaut des Gesetzentwurfs das Verbot der Aufzeichnung und Speicherung von Videoaufnahmen nicht nur für die „weichen Räume", sondern generell gilt.

Im September 2013 beschloss die Bürgerschaft die Annahme des Gesetzes in erster und zweiter Lesung.

5.5 Mitteilung von Gutachten durch den MDK an die Krankenkassen

Die seit langem kritisierte Übermittlung nicht erforderlicher Gutachtendaten durch den Medizinischen Dienst (MDK) an die Krankenkassen haben wir vor Ort geprüft und bundesweit aufgegriffen. Die interne Datenschutz-Empfehlung einer überregionalen MDK-Arbeitsgruppe geht auf unsere Initiative zurück.

Im letzten Tätigkeitsbericht (23.TB 2010/2011 9.5) hatten wir darüber berichtet, dass MDK-Gutachter immer wieder umfangreiche Gutachten an die beauftragenden Kassen übermitteln, ohne § 277 Abs.1 Sozialgesetzbuch V (SGB V) einzuhalten und sich auf die „Ergebnisse der Begutachtung" und „die erforderlichen Angaben über den Befund" zu beschränken. Immer wieder wurden detailliert medizinische Sachverhalte, Krankheitsvorgeschichten oder Beschreibungen des äußeren Zustands, der Familiensituation

oder des Auftretens der Betroffenen nicht nur erhoben, sondern auch an die Krankenkasse weitergegeben, obwohl diese Angaben für die Erfüllung des Auftrags der Kasse nicht relevant waren.

Im Januar 2012 führten wir im MDK Nord ein Gespräch mit den verantwortlichen Personen und ließen uns aus dem Archiv eine Stichprobe von 13 Gutachten / Stellungnahmen für eine datenschutzrechtliche Prüfung geben. In unserem Prüfbericht vom 15. März 2012 stellten wir eine sehr unterschiedliche Handhabung der vorgegebenen Gutachtenstruktur und des Umfangs der Übermittlungen durch die einzelnen medizinischen Gutachter fest.

So wurde das Gutachten in einem Fall zwar „ohne Vorgeschichte und ohne Befund" an die Krankenkasse übermittelt, stattdessen aber mit einer ausführlichen inhaltlichen Wiedergabe der „vorliegenden Unterlagen", die eigentlich nur aufgezählt werden sollten. In einem anderen Fall erklärte der Gutachter in der Rubrik „Fremdbefunde", aus Gründen der Schweigepflicht auf Auszüge aus einem Befundbericht der Psychotherapeutin verzichten zu müssen, fügte seinem Gutachten aber genau diesen Befundbericht insgesamt als Anlage bei. Setzt man den Auftrag der Kasse an den MDK und das Gutachtenergebnis einerseits mit dem Umfang der medizinischen und sozialmedizinischen Ausführungen im Gutachten andererseits in Beziehung, fällt nicht selten ein Missverhältnis auf. Bei einer sozialmedizinischen Begutachtung waren sich alle Beteiligten – später auch der Betroffene selbst – über das Ende einer Arbeitsunfähigkeit einig; dennoch enthielt das MDK-Gutachten ausführlichste Angaben über die Anamnese, die weit über die Arbeitsunfähigkeitszeit hinausreichte. Schließlich fehlte den meisten Gutachten der Hinweis darauf, dass die betroffene Person nach § 277 Abs.1 S.3 SGB V über die Möglichkeit unterrichtet wurde, der Befundübermittlung an den in Anspruch genommenen Leistungserbringer (Arzt) zu widersprechen.

Erst im März 2013 erhielten wir – nach einem zwischenzeitlichen Gespräch mit dem neuen ärztlichen Leiter des MDK Nord - eine Antwort auf unseren Prüfbericht. Im Grundsatz konnten wir weitgehende Einigkeit über das Ziel und die nötigen Folgen des § 277 Abs.1 SGB V feststellen. Im Detail unterschiedlichen Bewertungen der Erforderlichkeit einzelner Datenübermittlungen für die Entscheidungsfindung der Krankenkassen gingen wir nicht weiter nach. Jeder Einzelfall hätte einer intensiven Diskussion bedurft. Das Angebot an uns, im Rahmen der Qualitätssicherung des MDK dauerhaft als Prüfer tätig zu werden, konnten wir aus verschiedenen Gründen nicht annehmen. Uns ging es in erster Linie um eine nachhaltig datenschutzbewusstere Einstellung und Praxis der MDK-Gutachter und eine entsprechende Selbstorganisation des MDK.

Wie im 23. TB berichtet, hatte der Medizinische Dienst des Spitzenverbandes Bund der Krankenkassen e.V. (MDS) aufgrund unserer Initiative 2011 eine Arbeitsgruppe mit den Datenschutzbeauftragten einiger MDK zu diesem Thema eingerichtet. Diese hatte im Februar 2012 zum ersten Mal getagt. Im Januar 2013 – parallel zur Stellungnahme

des MDK Nord auf unseren Prüfbericht - übersandte uns der MDS die mittlerweile erarbeitete „Gemeinsame Empfehlung zur Umsetzung des § 277 SGB V".

Der zuständige Bund-Länder-Arbeitskreis der Datenschutzbeauftragten nahm das Papier als deutlichen Fortschritt grundsätzlich positiv auf. Festgestellt wurden allerdings auch starke Unterschiede in der Verfahrensweise der einzelnen MDK in den Bundesländern. Im Auftrag des Arbeitskreises wandten wir uns im März 2013 an den MDS mit einigen ergänzenden Anregungen zu der Gemeinsamen Empfehlung.

Im Weiteren werden wir beobachten, wie diese Empfehlung im MDK Nord konkret umgesetzt wird und ob bzw. in welcher Weise sie die Praxis der Gutachter bei der Übermittlung von sensiblen medizinischen Daten der Betroffenen an die Krankenkasse und die Leistungserbringer beeinflusst.

5.6 Externe Abrechnung und Bonitätsprüfung für Zahnärzte

Die bei Zahnärzten vielfach übliche Praxis, auch von Kassenpatienten eine Einwilligung zur externen Bonitätsprüfung und Abrechnung einzuholen, ist nur unter engen Voraussetzungen datenschutzrechtlich zulässig.

Eingaben und Medienanfragen veranlassten uns, an ein größeres zahnärztliches Serviceunternehmen und an die Zahnärztekammer heranzutreten. Wir ermittelten folgenden Sachverhalt:

Vielfach erhalten auch gesetzlich Versicherte bereits beim Betreten der Zahnarztpraxis vom Empfangspersonal eine Einverständniserklärung, die sie noch vor dem ersten Kontakt mit dem Zahnarzt unterschreiben sollen. Mit der Unterzeichnung erklären sich die Patienten einverstanden, dass

- die „zum Zwecke der Abrechnung und Geltendmachung jeweils erforderlichen Informationen (Name, Befunde...) an die Servicegesellschaft – eine externe Abrechnungsstelle - weitergegeben werden,
- Informationen „bei einer Auskunftei zur Prüfung meiner Bonität" eingeholt werden,
- die sich aus der Behandlung ergebenden Forderungen an die Servicegesellschaft abgetreten werden,
- im Rahmen der Refinanzierung eine Weiterabtretung an eine benannte Bank erfolgt,
- der behandelnde Zahnarzt von der ärztlichen Schweigepflicht befreit ist, soweit dies für die Abrechnung und Geltendmachung der Forderungen erforderlich ist.

Nach Unterzeichnung erfragt die Zahnarztpraxis mit einem Mausklick über eine spezielle Software der Servicegesellschaft / Abrechnungsstelle in Sekundenschnelle die

Bonität des zukünftigen Patienten. Diese wird der Praxis in Form einer Ampel mitgeteilt („rot" für hohes Risiko).

Auf unsere Anfrage erklärte die Zahnärztekammer das dargestellte Verfahren für unproblematisch. Die Rechtsprechung fordere die Einholung einer Einwilligung vor der Behandlung. Diese Rechtsauffassung trifft jedoch nicht zu. Richtig ist nur, dass die (medizinische) Einwilligung in den körperlichen Eingriff diesem - natürlich – vorausgehen muss. Auch für eine Bonitätsabfrage ist dies sinnvoll; für die Einwilligung in die externe Abrechnung gilt dies jedoch nicht. Denn die Honorarforderung wird erst nach der Behandlung fällig, und die Abrechnung über eine externe Stelle ist keine innere Bedingung für den Behandlungsbeginn.

Grundsätzlich muss ein Zahnarzt seine Leistungen für gesetzlich Versicherte nach dem Sozialgesetzbuch V (SGB V) über die Kassenzahnärztliche Vereinigung abrechnen. Hierfür gibt das SGB V den Zahnärzten die notwendigen gesetzlichen Datenverarbeitungsbefugnisse; einer Einwilligung in eine externe Abrechnung bedarf es nicht. Da die Krankenkassen unabhängig von der Zahlungsfähigkeit der Versicherten zur Zahlung an den Zahnarzt verpflichtet sind, entfällt auch das Bedürfnis nach einer Bonitätsprüfung.

Eine Bonitätsabfrage und eine externe Abrechnung kommen also nur dann in Betracht, wenn der gesetzlich Versicherte über den gesetzlichen Leistungsumfang hinaus mit dem Zahnarzt eine besondere, privatärztlich abzurechnende Leistung vereinbart. Dies kann nur im Zusammenhang mit einer ganz konkreten Behandlung geschehen. Der Patient muss dabei ausreichend darüber aufgeklärt werden, welche Leistung nicht von der Krankenkasse bezahlt wird, sondern ggf. von ihm selbst finanziert werden muss. Erst nach einer solchen Aufklärung und Vereinbarung kommt die Vorlage einer Einwilligungserklärung für die Bonitätsprüfung in Betracht. Die Einwilligung in die externe Abrechnung ist dagegen erst nach der Behandlung zur Abwicklung der durch sie entstandenen Honorarabrechnung erforderlich. Ist allerdings die privatärztlich abzurechnende Leistung auch bezüglich der Kosten so bestimmt, dass der Patient erkennen kann, was auf ihn zukommt, kann die Einwilligung in die externe Abrechnung und Forderungsabtretung auch vor der Behandlung und zusammen mit der für die Bonitätsprüfung erfolgen. In keinem Falle darf der gesetzlich versicherte Patient bereits vom Praxispersonal und vor einem Arztkontakt um die Unterschrift unter die dargestellte Einverständniserklärung gebeten werden.

Die dargestellte Praxis vieler Zahnärzte führt dagegen dann zu einer unzulässigen Datenerhebung und Vorratsspeicherung, wenn die gesetzlich Versicherten sich auf die gesetzlichen Leistungen beschränken wollen.

Doch selbst bei der wirksamen Vereinbarung von privatärztlich abzurechnenden Zusatzleistungen darf der Patient nicht durch die Androhung einer Behandlungsverweigerung gezwungen werden, die Einwilligung zu erteilen. Zwar ist eine Bonitätsprüfung

im Falle eines Vorleistungsrisikos nach § 28 Bundesdatenschutzgesetz grundsätzlich vertretbar; sie könnte aber nach Klärung der Zusatzkosten auch durch die Vereinbarung von Vorkasse oder Sicherheitsleistung abgewendet werden. Die Einwilligung in eine externe Abrechnung muss zudem freiwillig erfolgen: Die Behandlung, die in keinem zwingenden inneren Zusammenhang mit der Art der Abrechnung steht, darf nicht von der Erteilung der Einwilligung abhängig gemacht werden (unzulässiges Koppelungsgeschäft).

Im Übrigen erklärte die Rechtsprechung die eingangs dargestellte Formular-Einwilligung in die Weiterabtretung an refinanzierende Banken für unwirksam. Es werde den Patienten nicht klar, dass dies mit der Weitergabe aller forderungsbegründenden medizinischen Leistungsdaten verbunden ist.

Wir haben der Zahnärztekammer die Rechtslage verdeutlicht und die Formulierung entsprechender Mitgliederinformationen angeboten. Die Kammer kam auf dieses Angebot nicht zurück. Der Zahnarzt, dessen Patient uns um Prüfung bat, sicherte jedoch zu, die dargestellte Einwilligung zukünftig erst nach einer Vereinbarung privatärztlich abzurechnender Zusatzleistungen einzuholen.

5.7 Vereinbarung des HmbBfDI mit der Ethikkommission der Ärztekammer

Nachdem die Ethikkommission der Ärztekammer und wir Projekte medizinischer Forschung teilweise doppelt und in Einzelfällen auch sich widersprechend beraten hatten, konnte für die zukünftige Kooperation Einigung über Grundsätze und Verfahren erzielt werden.

Häufig wenden sich Forscher mit umfangreichen Projektunterlagen an uns, weil die Ethikkommission der Ärztekammer sie in einem Zwischenbescheid aufgefordert hatte, ein Votum des Hamburgischen Datenschutzbeauftragten einzuholen. Im August 2012 erhielten wir in diesem Zusammenhang Kenntnis von folgendem Problem: Nachdem wir ein bestimmtes Forschungsprojekt geprüft und schließlich für unbedenklich erklärt hatten, forderte die Ethikkommission der Ärztekammer die Wissenschaftler auf, für dasselbe Projekts statt der mit uns abgestimmten Aufklärungs- und Einwilligungs-Texte die von der Ethikkommission herausgegebenen Musterformulare zu verwenden.

Zuvor, im Jahre 2011, hatten wir aus fachlicher Sicht Änderungen dieser Formulare angeregt, blieben damit jedoch weitgehend erfolglos. Auch hatten wir die Erfahrung gemacht, dass die uns vorgelegten Forschungsprojekte so vielgestaltig und verschieden waren, dass allgemeingültige Musterformulare zur Einhaltung des Datenschutzes oft nicht passten. Wir prüften die Unterlagen deswegen immer individuell und konnten

so durchgehend angepasste konkrete Verbesserungen des Datenschutzes erreichen.

Um eine Klärung dieser unbefriedigenden Situation zu erreichen, wandten wir uns im August 2012 an den Vorsitzenden der Ethikkommission, beschrieben das Problem und regten ein Gespräch an. Dieses fand am 30. Oktober statt, konnte Missverständnisse aufklären und schuf eine neue Basis für die datenschutzrechtliche Prüfung und Beratung von medizinischen Forschungsprojekten. Folgende Punkte sind dem gemeinsamen Protokoll entnommen:

- Während für uns die gesetzlichen Regelungen, insbesondere die §§ 12, 12a Hamburgisches Krankenhausgesetz, die Prüfungs- und Beratungsgrundlage bilden, berücksichtigt die Ethikkommission darüber hinaus auch internationale Grundsätze und untergesetzliche Fachleitlinien.
- Beide Seiten befürworteten den Aufbau einer UKE-weiten standardisierten Forschungsdatenbank, in der die Patientendaten sicher pseudonymisiert und den Forschern datenschutzgerecht zur Verfügung gestellt werden können.
- Verlangt die Ethikkommission von den Forschern ein Votum des Hamburgischen Datenschutzbeauftragten, wird sie dieses – nach individueller Prüfung und konkreten Vorgaben durch uns – als abschließende und verbindliche Bearbeitung des Datenschutzaspekts in ihre Gesamtbewertung aufnehmen.
- Hinsichtlich der Aufklärung der Probanden und ihrer Einwilligung in die Datenverarbeitung des Forschungsprojekts blieb es bei der Alternative: Entweder erhalten Proband und Forscher je ein unterzeichnetes (kürzeres) Dokument, das Aufklärung und die darauf bezogene Einwilligung enthält. Oder die beim Forscher verbleibende unterzeichnete Einwilligung muss die Aufklärung, auf die sie sich bezieht, wieder aufnehmen, wenn die Aufklärung selbst beim Probanden verbleibt.
- Die Aufbewahrungsdauer von Projektdaten muss begrenzt, die von Daten in Biobanken kann langfristig für zukünftige Forschungen vorgehalten werden.
- Die Bedeutung und unterschiedliche Verwendung des Begriffs „Datentreuhänder" wurde geklärt.
- Schließlich vereinbarten wir eine frühzeitige gegenseitige Information und Einbeziehung bei der Vorlage von Forschungsprojekten.

5.8 Klinisches Krebsregister

Die Freie und Hansestadt Hamburg wahrt die Rechte von Krebspatienten dadurch, dass ihnen gesetzlich ein umfassendes und individuell teilbares Widerspruchsrecht bezüglich der Meldung zum Krebsregister eingeräumt wird.

Im Jahr 2012 brachte die Bundesregierung den Entwurf eines Gesetzes zur Weiterentwicklung der Krebsfrüherkennung und zur Qualitätssicherung durch klinische Krebs-

register (Krebsfrüherkennungs- und –registergesetz – KFRG) in den Deutschen Bundestag ein. Hierdurch wurde im Jahr 2013 unter anderem auch der neue § 65c in das Fünfte Buch Sozialgesetzbuch (SGB V) eingefügt. § 65c Abs. 1 S. 1 SGB V bestimmt, dass die Länder zur Verbesserung der Qualität der onkologischen Versorgung klinische Krebsregister einrichten. In der Gesetzesbegründung heißt es dazu:

„Die Regelung in Satz 1 verpflichtet die Länder zur Einrichtung klinischer Krebsregister und benennt mit der Verbesserung der Qualität in der onkologischen Versorgung das mit der Regelung verfolgte Ziel. Die flächendeckende Einführung klinischer Krebsregister wird im Fünften Buch Sozialgesetzbuch damit als spezielles Instrumentarium zur Qualitätssicherung und Weiterentwicklung der onkologischen Versorgung verankert." (BT-DrS 17/11267, Seite 26)

Bereits derzeit wird in Hamburg ein epidemiologisches Krebsregister geführt, das auf dem bisherigen Hamburgischen Krebsregistergesetz (HmbKrebsRG) beruht. Das nach § 65c SGB V verpflichtend neu einzurichtende klinische Krebsregister unterscheidet sich insbesondere insofern von dem bereits bestehenden Krebsregister, dass auch klinische Daten erhoben werden sollen. Ferner soll das klinische Krebsregister auch die interdisziplinäre Zusammenarbeit zwischen den am Behandlungsprozess Beteiligten unterstützen; hierzu sollen auch Daten aus dem klinischen Krebsregister den Leistungserbringern personenbezogen zur Verfügung gestellt werden.

Die Freie und Hansestadt Hamburg hat begonnen, die Erfüllung dieser gesetzlichen Pflicht zur Einrichtung eines klinischen Krebsregisters im Rahmen einer Novellierung des HmbKrebsRG umzusetzen. Bereits bei der Erstellung dieses Gesetzesentwurfes wurden wir beteiligt. Im Rahmen umfangreicher Besprechungen wurde das neue HmbKrebsRG gemeinsam entworfen. Anfänglich sollten die Betroffenen nur ein Widerspruchsrecht zur personenidentifizierenden Speicherung erhalten, so dass lediglich Name, Anschrift und Geburtsdatum durch ein Pseudonym ersetzt würden; das Krebsregister kann aber dieses Pseudonym aus einer späteren namentlichen Meldung erneut bilden, so dass zu diesem Zeitpunkt alle bis dahin pseudonym gespeicherten Gesundheitsdaten diesem Patienten zugeordnet werden können. Durch unsere Intervention werden die Betroffenen nun gesetzlich die Möglichkeit haben, nicht nur der personenidentifizierenden Speicherung, sondern auch der Meldung an sich zu widersprechen.

5.9 Tierhalterregister

Die Behörde für Gesundheit und Verbraucherschutz löscht das Tierhalterregister vom Share-Point und arbeitet an der Umsetzung einer datenschutzkonformen Lösung.

Die Behörde für Gesundheit und Verbraucherschutz hat ein Tierhalterregister für ganz Hamburg errichtet und auf einem Share-Point abgelegt; über diesen Share-Point hätten alle bezirklichen Mitarbeiter Zugriff auf die Daten gehabt unabhängig davon, ob die Daten im Rahmen der Zuständigkeit erforderlich sind. Ziel dabei ist, dass die Bezirke nicht eigene Listen führen müssen, sondern auf ein zentrales Register lesend und schreibend sowohl ohne Vorliegen einer Seuche wie auch in Situationen eines drohenden oder erfolgten Seuchenfalles zurückgreifen können.

Derzeit besteht keine gesetzliche Grundlage, die eine solche Datei rechtfertigt. § 11a des Hamburgischen Datenschutzgesetzes (HmbDSG) bestimmt, dass eine gemeinsame Datei, in oder aus der mehrere Daten verarbeitende Stellen personenbezogene Daten verarbeiten sollen, einer gesetzlichen Grundlage bedarf. Da bezüglich dieser Gesetzesanwendung Meinungsverschiedenheiten auftraten, wurden wir im März 2013 in dieses Verfahren einbezogen und stellten die geltende Rechtslage dar. Gleichzeitig verwiesen wir auf zukünftige rechtliche Grundlagen: Im Frühjahr 2014 wird das Tiergesundheitsgesetz (TierGesG) in Kraft treten, das in § 22 TierGesG zum einen bestimmt, welche Daten jeder Tierhalter der zuständigen Stelle übermitteln muss, und zum anderen eine Rechtsgrundlage für ein automatisiertes Abrufverfahren im Einzelfall gibt.

Allerdings ist das Ziel nicht mit einem automatisierten Abrufverfahren erreichbar, sondern nur mit der geschilderten gemeinsamen Datei: Vor allem in Fällen, in denen die Bezirke gar keine Kenntnis von einer Tierhaltereigenschaft haben, führt ein automatisiertes Abrufverfahren nicht zu einer wirksamen Tierseuchenverhütung, da der jeweilige Sachbearbeiter gar nicht weiß, dass er diesbezüglich einen Abruf vornehmen könnte. Da es weder derzeitig noch unter Geltung des zukünftigen Tiergesundheitsgesetzes eine dem § 11a HmbDSG entsprechende gesetzliche Grundlage für eine gemeinsame Datei gibt, wurde auf unseren Vorschlag hin vereinbart, dass in das neu zu schaffende Ausführungsgesetz zum Tiergesundheitsgesetz eine entsprechende Rechtsgrundlage aufgenommen wird. Bei der Umsetzung muss auf die Zugriffsberechtigung der jeweils zuständigen Stellen geachtet werden; hierbei müssen auch Möglichkeiten eines Zugriffs auf Daten anderer Bezirke berücksichtigt werden, soweit dies erforderlich ist.

In Folge unseres Tätigwerdens wurde die in den Share-Point eingestellte, aber noch nicht freigeschaltete Tierhalterdatei aus dem Share-Point wieder gelöscht. Derzeit arbeitet die Behörde für Gesundheit und Verbraucherschutz an der Umsetzung der rechtlichen und technischen Anforderungen für das Tierhalterregister.

5.10 Veröffentlichung von Patientendaten im Internet (UKE)

Das UKE schließt eine Datenschutzlücke in Bezug auf Patientendaten und intensiviert die Mitarbeiterschulungen zum Datenschutz.

Wir erhielten von einem besorgten Bürger den Hinweis, dass im Internet die Untersuchungsergebnisse dreier Patienten des UKE, einschließlich Namen und Geburtsdatum frei einsehbar waren. Diese personenbezogenen Daten waren auf einem sogenannten pastebin zu finden, einer Webanwendung im Internet zur Veröffentlichung meistens von Textbausteinen eines Programmcodes zum Zwecke der späteren Verwendung oder Weitergabe. Befundinhalte sind Angaben über die Gesundheit und stellen somit eine besondere Art personenbezogener Daten nach § 3 Abs. 9 Bundesdatenschutzgesetz (BDSG) dar.

Umgehend forderten wir das UKE auf, angesichts dieser unzulässigen Veröffentlichung sofort Maßnahmen zu ergreifen, u.a. um einen datenschutzgerechten Zustand wieder herzustellen und zukünftig solche Datenschutzverstöße zu verhindern. In enger Abstimmung mit uns leitete das UKE folgende Schritte ein: Erstens ermittelte es den Sachverhalt, zweitens bemühte es sich intensiv darum, dass die Daten nicht mehr im Internet aufrufbar waren. Es sollte zukünftig die Möglichkeit verhindert werden, auf derartige Internetportale Zugriff nehmen zu können. Hierneben informierte das UKE auch umgehend die betroffenen Patienten in persönlichen Gesprächen und kam so seiner Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten gemäß § 42a BDSG nach.

Wenige Tage nach unserer Aufforderung hat das UKE uns mitgeteilt, dass das verwendete Internetportal bereits kurz nach Bekanntwerden dieser unzulässigen Datenveröffentlichung aufgrund des Handelns des UKE alle Daten und auch Google den Cache zum inzwischen toten Link gelöscht hat. Eine Überprüfung durch uns hat ergeben, dass die uns bekannt gewordenen personenbezogenen Daten nicht mehr im Internet eingesehen werden können. Ein Mitarbeiter des UKE hatte die Untersuchungsergebnisse elektronisch verfasst, allerdings nicht in dem besonders stark gesicherten Netz für Patientendaten (KIS 1). Um die Daten nun in dieses Netz zu übertragen, kopierte er die Befundberichte in die Webanwendung; anschließend rief er von einem PC des KIS 1 aus die Webanwendung im Internet auf und kopierte die Daten in das Netz für Patientendaten. Die personenbezogenen Daten der Patienten waren somit aber auch in dem Internetportal gespeichert. Mittlerweile hat der Geschäftsbereich Informationstechnologie die Konfiguration so ergänzt, dass ein Zugriff auf solche Plattformen aus dem besonders stark gesicherten Netz für Patientendaten gesperrt ist. Das UKE hat somit durch unsere Intervention diese Lücke geschlossen, durch die sensible Patientendaten ins Internet gelangen konnten.

Ferner hat das UKE diesen Vorfall zum Anlass genommen, diese Problematik in die internen Datenschutzschulungen einzufügen. Durch Online-Schulungen sollen alle Mitarbeiter jährlich geschult werden, so dass die Datenschutzunterweisung zu Beginn einer jeden Einstellung kontinuierlich erneuert wird. Die Mitarbeiter werden somit nun regelmäßig auf datenschutzrechtliche Gefahren bei der Nutzung solcher Plattformen hingewiesen und verstärkt dafür sensibilisiert, auch insoweit auf den Datenschutz und die eigene Verschwiegenheitspflicht zu achten.

5.11 Geburtsdaten-Übermittlung vom Standesamt an das Gesundheitsamt

Die Weiterleitung einer Geburtsbescheinigung, in der eine Vielzahl an personenbezogenen Gesundheitsdaten enthalten ist, vom Standesamt an das Gesundheitsamt ist mangels Rechtsgrundlage rechtswidrig.

Nach dem Bevölkerungsstatistikgesetz (BevStatG) führen die Standesämter Zählkarten, in denen im Zusammenhang mit einer Geburt z.B. Geburtstag, Geschlecht, Körpergewicht, Körperlänge, Mehrlingsgeburt und vieles mehr einzutragen sind. Die an einer Geburt beteiligten Ärzte oder Hebammen füllen u.a. eine Geburtsbescheinigung aus, die diese statistischen Daten personenbezogen enthält, und übersenden sie an das Standesamt. Das Gesundheitsamt seinerseits beteiligt sich nach § 8 Abs. 2 Hamburgisches Gesundheitsdienstgesetz (HmbGDG) an der Förderung und dem Schutz der Gesundheit u.a. von Säuglingen und berät Mütter und Väter in Fragen der Gesundheitspflege von Säuglingen und Kleinkindern. Damit das Gesundheitsamt über eine Geburt informiert ist, erhielt es vom jeweiligen Standesamt diese Geburtsbescheinigung inklusive aller personenbezogenen Daten. Eine Rechtsgrundlage für diese Datenübermittlung gibt es jedoch nicht.

Nachdem wir von der Weiterleitung der Geburtsbescheinigung erfahren haben, baten wir umgehend sowohl die Leiter der Standesämter als auch die Leiter der Gesundheitsämter um Stellungnahme. Unmittelbar nach Prüfung der eingereichten Unterlagen stellten wir den oben genannten Leitern im August 2013 die Rechtslage dar und forderten sie zur Behebung dieses rechtswidrigen Zustandes auf.

Die Standesämter reagierten sofort und kündigten die zeitnahe Einstellung der Informationsübermittlung an. Zwischenzeitlich wurde uns bekannt, dass die Behörden für Gesundheit und Verbraucherschutz sowie für Inneres und Sport gemeinsam planten, die Meldedatenübermittlungsverordnung (MDÜV) dahin gehend zu ergänzen, dass die Daten aller in Hamburg gemeldeten Neugeborenen an das jeweilige Gesundheitsamt gemeldet werden.

Bereits im Oktober 2013 wurde ein mit uns im Vorfeld abgestimmter Entwurf eines Artikelgesetzes in die externe Behördenabstimmung gegeben, mit dem u.a. auch § 12 Abs. 1 MDÜV dahin gehend geändert werden soll, dass nicht nur Daten zuziehender Kinder bis zum vollendeten 3. Lebensjahr, sondern auch die dort genannten Daten der Neugeborenen an die Gesundheitsämter übermittelt werden dürfen. Da die Mitteilung zukünftig durch die Meldebehörden erfolgen soll, erhalten die Gesundheitsämter im Gegensatz zur bisherigen rechtswidrigen Situation nun auch die Informationen der außerhalb von Hamburg geborenen, aber in Hamburg gemeldeten Kinder. Dadurch liegen den Gesundheitsämtern für ihre wichtige Aufgabe auch vollständige Daten aller Neugeborenen vor, so dass dort keines von ihnen unbekannt bleiben sollte. Die Verabschiedung dieses Artikelgesetzes und damit der Änderung der MDÜV bleibt nun abzuwarten.

5.12 Zugriff Kosmetikinstitut auf Arztpraxis-Software

Auch bei einer Gesellschafteridentität zweier Unternehmen müssen datenschutzrechtliche Regelungen zu Gunsten der Patienten beachtet werden.

Eine Bürgerin informierte uns, dass eine Mitarbeiterin eines Kosmetikinstitutes während der Anwendungen im PC auf ihre Behandlungsdaten aus einer dermatologischen Arztpraxis Zugriff nehmen konnte und hieraus vorlas. Eine Einwilligung zur Datenübermittlung hatte sie der Arztpraxis nicht erteilt.

Erste Ermittlungen ergaben, dass eine Identität der Gesellschafter bei Arztpraxis und Kosmetikinstitut besteht. Wir leiteten daraufhin ein Prüfverfahren ein; hierbei stellten wir insbesondere die Fragen, ob und in welchem Umfang ein Zugriff auf die Behandlungsdokumentation der Arztpraxis bestand. Uns wurde mitgeteilt, dass jede Stelle umfassend Zugriff auf die Dokumentation der anderen Stelle hatte. Ursprünglich existierte nur die Arztpraxis, in der auch kosmetische Leistungen erbracht wurden; hier wurde eine Praxis-Software für alle Patienten/Kunden gemeinsam genutzt. Um in steuerrechtlicher Hinsicht eine Trennung zwischen umsatzsteuerfreien (ärztlichen) und –pflichtigen (kosmetischen) Leistungen zu erzielen, wurde ein eigenes Kosmetikinstitut durch dieselben Gesellschafter gegründet. An der bisherigen Infrastruktur, insbesondere auch an der ursprünglichen einen Patienten-/Kunden-Dokumentation wurde nichts geändert. Wir stellten den Gesellschaftern dar, dass es datenschutz- wie auch berufsrechtlich unzulässig ist, wenn eine eigenständige juristische Person freien Zugriff auf die Patientendokumentation nehmen kann.

Aufgrund unserer Intervention installierte die Arztpraxis ein Zugriffsberechtigungskonzept, wonach jedes Unternehmen nur Zugriff auf seine Patienten bzw. Kunden nehmen kann. Da eine logische Trennung (Mandantentrennung) zwischen den Datensätzen bei-

der juristischer Personen nicht erfolgt, handelt es sich aber weiterhin um eine gemeinsame Datei, deren erhöhtes Risiko darin besteht, dass z.B. aufgrund einer fehlerhaften Berechtigungsvergabe unzulässig Daten bekanntgegeben werden. Die Industrie bietet nach eigenen Recherchen eine Mandantentrennung bisher nicht an.

Angesichts der Entstehungsgeschichte, der nicht wesentlich geänderten Schutzbedürftigkeit der Daten und der Unmöglichkeit einer Mandantentrennung haben wir das Zugriffsberechtigungskonzept bei gleicher Gesellschafterstruktur als ausreichend bewertet. Voraussetzung ist aber, dass die Betroffenen zum einen über die gemeinsame, nur durch ein solches Konzept getrennte Datenhaltung informiert werden und hierin einwilligen; zum anderen müssen sie die Wahlmöglichkeit erhalten, ob sie ihre Daten der jeweils anderen Stelle zugänglich machen wollen. Letzteres soll auf erforderliche Fälle beschränkt sein, z.B. wenn eine gemeinsame Behandlung erfolgt.

5.13 Faxen von Arztbriefen

Beim Faxversand von Arztbriefen sind eine Reihe von rechtlichen, organisatorischen und technischen Anforderungen zu beachten, damit dem Datenschutz entsprochen wird

Wir erhalten immer wieder Eingaben von Bürgern, denen Dokumente mit fremden Patientendaten aus Arztpraxen per Fax zugegangen sind. Datenschutzrechtlich ist der Absendende verantwortlich dafür, dass die Daten z.B. aufgrund fehlerhafter Faxnummer keinem Unbefugten offenbart werden. Dies beinhaltet somit vor allem die Überprüfung der Richtigkeit und Aktualität der Faxnummer wie auch die Vergewisserung, dass der Empfänger auch berechtigt ist, die Daten zu erhalten.

Beim Faxversand ist zu bedenken, dass jeder, der Zugang zum Empfangsgerät hat, Einblick in die übermittelten Daten nehmen kann. Eine aus datenschutzrechtlicher Sicht sicherere Anonymisierung vor dem Versand birgt jedoch beim Empfänger häufig die gerade im Gesundheitswesen ggf. schwerwiegende Gefahr einer Verwechselung in sich. Um somit datenschutz- wie auch berufsrechtliches Fehlverhalten durch unbefugtes Offenbaren zu vermeiden, sollten in der Regel folgende Maßnahmen ergriffen werden:

- Personenbezogene Gesundheitsdaten sollen nur dann gefaxt werden, wenn eine schnelle Übermittlung erforderlich ist; soweit risikolos möglich, sollten die Unterlagen anonymisiert werden.
- Vor dem Versenden muss geprüft werden, ob die Faxnummer des Empfängers noch aktuell ist.

- Es muss sichergestellt sein, dass die richtige Faxnummer des Empfängers eingegeben wurde; regelmäßig sollten daher auch gespeicherte Kurzwahlnummern auf Richtigkeit überprüft werden. Zur Absicherung sollte hierbei das Vier-Augen-Prinzip eingehalten werden.
- Das eigene Faxgerät muss so aufgestellt sein, dass nur Berechtigte Einblick in und Zugriff auf eingehende Faxe haben.
- Im Zweifel oder z.B. bei einem längere Zeit nicht angewählten Empfänger sollte vor dem Versenden (telefonisch) geklärt werden, ob und dass auch beim Empfänger die datenschutz- und berufsrechtlichen Anforderungen eingehalten werden, und das Fax angekündigt wird.
- Um sicher zu gehen, dass der allein Berechtigte das Fax in Empfang nimmt, sollte mit dem Empfänger vor der Versendung bei Bedarf ein bestimmter Übermittlungszeitpunkt vereinbart werden.
- Die Fax-Vorlage darf nach dem Versenden nicht im Faxgerät liegengelassen werden.

Um einen effektiven Datenschutz zu gewährleisten, sollten die Kommunikationsregeln schriftlich fixiert und die Mitarbeiter entsprechend geschult werden.

Da es sich bei Gesundheitsdaten um besondere Arten von personenbezogenen Daten im Sinne des § 3 Abs. 9 Bundesdatenschutzgesetz handelt, müssen gegenüber den Vorteilen eines Faxversandes in Form von Schnelligkeit und Verbreitungsgrad immer die Gefahren für das informationelle Selbstbestimmungsrecht der betroffenen Patienten bei dieser Art der Datenübermittlung abgewogen werden.

6. Sozialwesen

6.1 Frühe Hilfen – Babylotse

Sollen personenbezogene Daten aus den Geburtskliniken und -häusern an die Babylotsen übermittelt werden, so bedarf es hierfür mangels einer entsprechenden Rechtsgrundlage einer Einwilligung der betroffenen Patienten; da aber der Öffentliche Gesundheitsdienst auch Beratung und Unterstützung der Gesundheitspflege von Kleinkindern und Säuglingen bis hin zu Hausbesuchen anbietet, ist eine enge Abstimmung mit den Akteuren der Frühen Hilfe erforderlich.

Seit 2012 ist im Bundeskinderschutzgesetz eine gesetzliche Grundlage für die Frühen Hilfen vorhanden. Im Rahmen des Landeskonzeptes „Frühe Hilfen: Guter Start für Hamburgs Kinder" sollen die Babylotsen an allen Hamburger Geburtskliniken und -häusern ein Kernelement bilden. Träger der „Babylotsen Hamburg" ist eine Stiftung;

ihre Aufgabe besteht darin, junge Familien mit psychosozialen Belastungen bereits im zeitlichen Zusammenhang einer Geburt Hilfen anzubieten oder zu organisieren, die für eine erfolgreiche Elternschaft zum Wohle des Kindes erforderlich sind. Mit Zustimmung der Eltern bieten sie eine Überleitung in das regionale Hilfesystem.
Nachdem zunächst an 2 Geburtskliniken die Babylotsen als Modellprojekt etabliert wurden, sollen sie seit 2013 in ganz Hamburg verstetigt werden. Zur Ermittlung des konkreten Hilfebedarfes sollen die Geburtskliniken und –häuser personenbezogene Daten der Familien einschließlich bestimmter Belastungsparameter an die Babylotsen übermitteln. Nach eingehenden konstruktiven Besprechungen zwischen der Behörde für Gesundheit und Verbraucherschutz, der Stiftung sowie unserer Dienststelle konnte Einvernehmen dahin gehend erzielt werden, dass diese Datenübermittlung mangels gesetzlicher Regelung nur aufgrund einer ausdrücklichen, schriftlichen Einwilligung erfolgen darf, da es sich um Gesundheitsdaten handelt (§ 3 Abs. 9, § 4a Abs. 3 Bundesdatenschutzgesetz). Wir haben daher bei der Entwicklung eines Musters eines entsprechenden Aufklärungs- und Einwilligungsformulars intensiv mitgewirkt. Da aber die jeweilige Geburtsklinik bzw. das Geburtshaus für die konkrete Datenübermittlung verantwortlich ist, haben wir stets darauf hingewiesen, dass diese die Entscheidungen zur konkreten Ausgestaltung des Verfahrens und der erforderlichen Unterlagen bezüglich der Einwilligung zu treffen haben.

Außerdem haben wir darauf hingewiesen, dass zur Vermeidung insbesondere von doppelten Hausbesuchen eine Abstimmung zwischen den Akteuren der Frühen Hilfen und dem Öffentlichen Gesundheitsdienst erfolgen sollte. Im Oktober 2013 wurde der Entwurf des § 7a Hamburgisches Gesundheitsdienstgesetz (HmbGDG) vorgelegt und in die externe Behördenabstimmung eingebracht. Dieser beinhaltet u.a. die gesetzliche Grundlage für die Datenübermittlung an den Öffentlichen Gesundheitsdienst, wobei die zu übermittelnden personenbezogenen Daten (vor allem Name, Anschrift und Geburtsdatum des Kindes und der gesetzlichen Vertreter) ausdrücklich aufgezählt sind; die derzeitige Entwurfsfassung lautet in Teilen wie folgt: „Der Öffentliche Gesundheitsdienst und die anderen Anbieter von Hausbesuchen im Rahmen der Frühen Hilfen kooperieren in den regionalen Netzwerken Frühe Hilfen miteinander und stimmen sich hinsichtlich der Hausbesuche ab. Der Öffentliche Gesundheitsdienst ist berechtigt, die dazu erforderlichen personenbezogenen Daten der Kinder und deren gesetzlichen Vertreter bei den vorgenannten Anbietern abzufordern und zu verarbeiten. Die anderen Anbieter Früher Hilfen sind berechtigt, diese Daten an den Öffentlichen Gesundheitsdienst zu übermitteln." Die Verabschiedung dieser Gesetzesänderung steht jedoch noch aus.

6.2 Obachtverfahren Gewalt u21 läuft ohne erforderliche Mandantentrennung

Die Polizei sieht keinen hohen Schutzbedarf für Daten der strafrechtlich auffälligsten Gewalttäter unter 21 Jahren. Da das Trennungsgebot nicht beachtet wird, wird das IT-Obachtverfahren als gemeinsames Verfahren ohne ausreichende Rechtsgrundlage betrieben.

Das „Obachtverfahren Gewalt u21" verfolgt die Ziele, Kindeswohlgefährdungen abzuwenden sowie schulische, berufliche, sozialintegrative und allgemeine Lebensperspektiven für den Betroffenen zu schaffen und die Grundlagen für ein zukünftig straffreies Leben zu legen (vgl. 23. TB III. 7.2). Ein solches Verfahren sollte nach unserer Auffassung von der Behörde für Arbeit, Soziales, Familie und Integration (BASFI) verantwortlich betrieben werden, da der Schwerpunkt nicht bei der polizeilichen Tätigkeit liegt. Dies hatten wir bereits im 22. und 23. Tätigkeitsbericht gefordert. Trotz intensiver Bemühungen konnten wir die beteiligten Stellen nicht überzeugen, diese behördliche Zuordnung vorzunehmen. Die Koordinierungsstelle, die das IT-Verfahren insgesamt inhaltlich und datenschutzrechtlich verantwortet, verbleibt somit beim Präsidialstab der Polizei. Die Chance, mit der Zuordnung ein deutliches Zeichen zu setzen, dass dies eine primär soziale Aufgabe ist, wurde somit vertan.

Aus unserer Sicht werden in dem IT-Verfahren personenbezogene Daten mit hohem Schutzbedarf verarbeitet. Zweck des Verfahrens ist es, die strafrechtlich auffälligsten Gewalttäter unter 21 Jahren in den Fokus der behördlichen Institutionen zu nehmen und unter eine kontinuierliche Beobachtung zu stellen, so dass die beteiligten Behörden ständig über den aktuellen Sachstand informiert sind und abgestimmt handeln können. In die Obachtliste werden nur unter 21-jährige Personen aufgenommen, die durch die Begehung einer erheblichen Anzahl von Straftaten, insbesondere auch durch die Begehung von Verbrechenstatbeständen (Raub, räuberische Erpressung, Vergewaltigung etc.) oder Vergehen gegen die körperliche Unversehrtheit (gefährliche Körperverletzung), aufgefallen sind. In allen Fällen ist aufgrund einer individuellen Betrachtung des Einzelfalles davon auszugehen, dass sie auch zukünftig Straftaten von erheblicher Bedeutung begehen werden. Außerdem wird bei den Personen - soweit minderjährig - aufgrund einer Betrachtung der persönlichen und familiären Gesamtsituation von einer Kindeswohlgefährdung oder - soweit 18-20-jährig - von einer Gefährdung des Wohls und der zukünftig straffreien Entwicklung der betroffenen Heranwachsenden ausgegangen. Neben dieser Wertung, zur Gruppe der strafrechtlich auffälligsten Gewalttäter unter 21 Jahren zu gehören, wird das Merkmal „Intensivtäter" erfasst. Neben diesen eher in die Vergangenheit der Person gerichteten, aber gleichwohl höchst sensiblen Wertungen wird im Obachtverfahren gleichzeitig eine Prognose zum zukünftigen Verhalten der Person, deren Daten darin verarbeitet werden, vorgenommen. Diese

ergibt sich einerseits aus der Zielstellung des IT-Verfahrens. Gemäß der Errichtungsanordnung werden dort nur Daten von Personen mit vollem Namen, Wohnanschrift und Geburtsdatum aufgenommen, bei denen aufgrund einer individuellen Betrachtung des Einzelfalles davon auszugehen ist, dass sie auch zukünftig Straftaten von erheblicher Bedeutung begehen werden. Andererseits wird im laufenden Verfahren von den beteiligten Stellen eine Wertung durch die Eingabe einer Ampelfarbe vorgenommen, wenn einzelne beteiligte Stellen aufgrund von aktuellen Ereignissen Gesprächsbedarf sehen. Ein Beispiel dafür ist, wenn der Jugendbewährungshilfe bekannt wird, dass sich der Betroffene aktuell in einer anhaltenden persönlichen Krisensituation befindet. Ein Bekanntwerden der Informationen des Obachtverfahrens (Verletzung der Vertraulichkeit) würde erhebliche und kaum vorhersehbare negative Folgen für die Betroffenen in allen gesellschaftlichen Bereichen nach sich ziehen: Angefangen von persönlichen Beziehungen im privaten wie auch im öffentlichen Bereich (z.B. Schule), über Problematiken bei der Ausbildungs- und Arbeitsvermittlung bis hin zu Schwierigkeiten bei der Wahrnehmung gesellschaftlicher Verantwortung mit allen sich mittelbar anschließenden Folgen z.B. auch finanzieller Art (eventuelle Arbeitslosigkeit usw.). Daher ist es aus unserer Sicht nicht nachvollziehbar, dass die Koordinierungsstelle unsere Auffassung nicht teilt, dass diese personenbezogenen Daten einen hohen Schutzbedarf haben.

Das Verfahren „Obachtverfahren Gewalt u21" ist in einer eigenen Site Collection im FHHportal auf der Grundlage der Microsoft Sharepoint-Technologie im FHHPortal realisiert. Die technische Realisierung des IT-Verfahrens haben wir im Berichtszeitraum geprüft. Dabei wurden verschiedene Mängel aufgezeigt. Dazu gehört, dass in der Risikoanalyse keine technischen und organisatorischen Maßnahmen festgehalten wurden, eine Errichtungsanordnung für das Verfahren nicht vorlag, die nach Freigaberichtlinie vorgeschriebenen Tests nicht dokumentiert wurden, Löschfristen für die Zugriffsprotokolle nicht festgelegt waren und eine Indexierung der Daten als Vorbereitung für die Bereitstellung der Suchfunktion vorgenommen wurde, obwohl die „Suche" in der Site Collection dauerhaft deaktiviert war. Im Laufe des Berichtszeitraums konnte erreicht werden, dass diese Mängel weitgehend behoben wurden.

Auch wurde von uns geprüft, ob das IT-Verfahren dem verfassungsrechtlich verankerten institutionellen Trennungsgebot genügt, wonach das für die Bewältigung dieser Fachaufgabe eingesetzte Verfahren von anderen IT-Verfahren getrennt werden muss, um die Rechte der Betroffenen zu gewährleisten. Diese Trennung muss sowohl von anderen IT-Verfahren des Präsidialstabs erfolgen, die für andere Zwecke genutzt werden, als auch von anderen IT-Verfahren anderer Daten verarbeitender Stellen der Polizei und auch anderer Behörden. Das Trennungsgebot muss sich dabei sowohl in der Organisation als auch in der IT-Realisierung widerspiegeln. Der Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder hat die dabei zu erfüllenden Anforderungen in der Orientierungshilfe „Mandantenfähigkeit" niedergeschrieben (vgl. II. 1.). Wenn jedoch keine solche Trennung besteht, wird nach § 11a Hamburgisches Datenschutzgesetz ein gemeinsames Verfahren betrieben. Dafür wäre dann jedoch

eine Rechtsvorschrift erforderlich, die dies ausdrücklich erlaubt.
Dieses eine gemeinsame Verarbeitung mehrerer Daten verarbeitender Stellen einschränkende Trennungsgebot ist unter anderem auch in § 11a Hamburgisches Datenschutzgesetz (HmbDSG) verankert, der in seinem Absatz 1 Satz 1 festlegt:

„Die Einrichtung gemeinsamer oder verbundener automatisierter Dateien, in oder aus denen mehrere Daten verarbeitende Stellen personenbezogene Daten verarbeiten sollen, bedarf der ausdrücklichen Zulassung durch eine Rechtsvorschrift."

Führen somit mehrere Daten verarbeitende Stellen eine gemeinsame Datei, so bedarf es hierfür einer Rechtsvorschrift im Sinne des § 11a HmbDSG.

Die Speicherung der personenbezogenen Daten im Obachtverfahren erfolgt in einer gemeinsamen IT-Infrastruktur auf der Grundlage der Microsoft Sharepoint-Technologie. In dieser werden sowohl das FHHPortal von der Daten verarbeitenden Stelle Finanzbehörde als zentrales Informations- und Arbeitsportal für die FHH als auch weitere spezifische Fachanwendungen von mehreren Daten verarbeitenden Behörden betrieben. Diese technische Infrastruktur „Sharepoint" kann somit grundsätzlich eine gemeinsame Datei im Sinne des § 11a HmbDSG darstellen. Die Sharepoint-Technologie stellt für die Umsetzung des Trennungsgebots dabei verschiedene Mechanismen bereit. Diese werden auch im „Architektur und Betriebskonzept SharePoint Server 2010" des Dienstleisters Dataport explizit benannt.

Die Nutzung dieser gemeinsamen IT-Infrastruktur für das Obachtverfahren ist datenschutzrechtlich somit in zwei Varianten denkbar: Entweder wird eine ausreichende Trennung zwischen den Mandanten und Abgrenzung zu anderen IT-Verfahren errichtet oder die insoweit bestehende gemeinsame Datei könnte theoretisch gemäß § 11a HmbDSG durch eine verfassungskonforme Rechtsvorschrift legitimiert werden. Aus unserer Sicht ist es datenschutzrechtlich jedoch erforderlich und auch praktisch realisierbar, das Obachtverfahren vom FHHPortal und den weiteren IT-Anwendungen zu trennen.

Die technischen und organisatorischen Maßnahmen der Trennung sind in der Risikoanalyse zu betrachten und zu beurteilen; eine solche Betrachtung enthielt die Risikoanalyse zum Obachtverfahren jedoch gerade nicht. Die Koordinierungsstelle musste auf Nachfrage insoweit eingestehen, dass keine Trennung des Mandanten „Obachtverfahren" beauftragt worden ist und dass insbesondere kein verfahrensspezifischer Berechtigungs-Provider für das Verfahren genutzt wird. Dieser Punkt führt dazu, dass z.B. alle ca. 30.000 Nutzer der FHH, die das FHHPortal als Informationsplattform nutzen, mit wenigen Klicks berechtigt werden könnten, auf die sensiblen Daten des Obachtverfahrens zuzugreifen. Da ohne eine ausreichende Abschottung des Verfahrens ein gemeinsames Verfahren mit anderen Daten verarbeitenden Stellen, die ebenfalls die gemeinsame IT-Infrastruktur nutzen, betrieben wird, bedürfte es ansonsten nach

§ 11a HmbDSG einer spezifischen Rechtsgrundlage. Da diese von uns nicht gesehen wird, wird derzeit das Obachtverfahren ohne Legitimation durch eine Rechtsvorschrift innerhalb einer gemeinsamen IT-Infrastruktur betrieben. Wir haben daher die Koordinierungsstelle im November 2013 aufgefordert, diesen Mangel unverzüglich zu beseitigen.

6.3 SDZ Harburg – „baulicher" Datenschutz

Zur Verbesserung des Datenschutzes wurde der Wartebereich im Sozialen Dienstleistungszentrum (SDZ) Hamburg-Harburg weiter vom Anmeldetresen entfernt und den baulichen Gegebenheiten entsprechend in den Bereich der Eingangshalle verlegt.

Eine Bezirksfraktion in Harburg wandte sich mit einem Anliegen bezüglich des SDZ Hamburg-Harburg an uns: Mehrere Bürger beschweren sich über die dortige räumliche Ausgestaltung im Eingangsbereich. Die Mitarbeiter des SDZ wollen durch Klärung der Anliegen bereits am Anmeldetresen vielen Bürgern helfen, um ihnen eventuell unnötige Wartezeiten zu ersparen. Dazu ist es erforderlich, dass die Bürger bereits dort ihre personenbezogenen Daten vortragen. Aufgrund der räumlichen Enge unmittelbar vor dem Anmeldetresen war die Besorgnis nachvollziehbar, dass Wartende die offenbarten Daten mithören konnten. Zwar war ein Diskretionsschild aufgestellt; es war aber, insbesondere bei großem Andrang, nicht auszuschließen, dass der insoweit gesetzte Diskretionsabstand nicht eingehalten wurde.

Aufgrund dieser Eingabe überprüften wir die räumliche Situation vor Ort. Dabei erfuhren wir, dass der jetzige Standort des Anmeldetresens aus der Eingangshalle herausgenommen wurde, u.a. um den Bürgern mehr Wartefläche innerhalb des Gebäudes zu bieten und die Mitarbeiter vor krankheitsverursachender Zugluft zu schützen. Uns wurde bestätigt, dass Bürger auch dann eine Wartenummer erhalten, wenn sie ihr Anliegen nicht schon am Anmeldetresen vorbringen wollen.

Uns fiel zwischen der Eingangshalle und dem Anmeldetresen die bauliche Abtrennung aus Glas auf; hinter dieser Abtrennung befindet sich der Anmeldetresen. Während des Ortstermins stellten wir fest, dass diese Glasabtrennung die Schallausbreitung der Gespräche am Anmeldetresen in die Eingangshalle hinein deutlich verhindert.

Da uns bestätigt wurde, dass auch in Spitzenzeiten die Bürger immer innerhalb des Gebäudes warten, haben wir angeregt, den Wartebereich in die Eingangshalle vorzuverlegen und somit den Datenschutz des Bürgers am Anmeldetresen weitaus stärker als bisher zu realisieren. Dadurch wird der Diskretionsabstand um ca. 1,5 Meter vergrößert; auch der erste Wartende steht nun noch in der Eingangshalle, wo aufgrund

der Glasabtrennung die Wahrnehmungsmöglichkeit des am Anmeldetresen gesprochenen Wortes sehr stark verringert ist. Den Wartenden ist diese Vorverlegung zuzumuten, da die Eingangshalle selbst zu Spitzenzeiten ausreichend Platz bieten dürfte. Neben der Aufstellung des Diskretionsschildes mit einem Piktogramm forderten wir außerdem eine Markierung am Fußboden zur Verdeutlichung des Wartebereichs.

Nach Aussage des SDZ führen diese Maßnahmen bereits dazu, dass der Diskretionsabstand grundsätzlich eingehalten wird und die Bürger datenschutzkonform ihre Anliegen vortragen können.

6.4 Datenerhebung durch Betreuungsbehörde

Eine neue gesetzliche Erhebungsbefugnis erlaubt der Betreuungsbehörde im Rahmen der Prüfung zur Einrichtung einer Betreuung, Daten über den Betroffenen unter bestimmten Voraussetzungen auch bei Dritten zu erheben; hierbei bleiben die Rechte des Betroffenen aber gewahrt.

Betreuungsbehörden klagen seit Längerem über datenschutzrechtliche Probleme, wenn sie während eines betreuungsrechtlichen Gerichtsverfahrens den Sachverhalt aufzuklären haben. Die Betreuungsbehörde fasst in diesem Zusammenhang die von ihr erhobenen personenbezogenen Daten in einem Bericht für das Betreuungsgericht zusammen. Uns wurde immer wieder die Frage gestellt, ob Informationen über den Betroffenen an die Betreuungsbehörde weitergegeben werden dürfen. So erhielten wir z.B. von Seiten eines Mediziners die Anfrage, ob er ohne Vorlage einer Schweigepflichtentbindungserklärung seines Patienten ärztliche Dokumentationen an die Betreuungsbehörde übermitteln durfte; bezüglich dieses Patienten lief ein gerichtliches Verfahren zur Einrichtung einer Betreuung. Da aber das Betreuungsbehördengesetz (BtBG) insoweit keine datenschutzrechtlichen Regelungen vorsieht, war das Hamburgische Datenschutzgesetz (HmbDSG) zur Beurteilung heranzuziehen. Nach diesen bisherigen Regelungen war die Erhebung bei Dritten im vorgenannten Sachzusammenhang ohne Einwilligung des Betroffenen praktisch nicht zulässig.

Die Problematik für die Betreuungsbehörde bestand darin, dass manche Betroffene krankheitsbedingt gar nicht in der Lage sind, eine Einwilligung zur Dritterhebung zu erteilen. Durch die Verhinderung einer Datenerhebung im Umfeld des Betroffenen würden die Gerichte aber ggf. unvollständige Berichte erhalten. Folge hiervon ist unter Umständen ein längeres Verfahren, da das Gericht den Sachverhalt dennoch weiter aufzuklären hat. Dies kann gerade auch für den Betroffenen selbst Nachteile bedeuten, wenn er angesichts seiner Situation auf schnelle Hilfe angewiesen ist.

Mit Drucksache vom 14.05.2013 (SDrs 20/7964) legte der Senat einen Gesetzesent-

wurf vor, mit dem u.a. auch im Hamburgischen Gesetz zur Ausführung des Betreuungsgesetzes (HmbAGBtG) ein neuer § 4 eingeführt wurde. Hiernach darf die zuständige Behörde nunmehr im Rahmen des ihr vom Betreuungsgericht erteilten Auftrags die für die Feststellung des Sachverhalts und für den Vorschlag eines Betreuers erforderlichen Daten erheben, wobei gesetzlich ausdrücklich vorgeschrieben wird, dass die Daten grundsätzlich bei dem Betroffenen zu erheben sind. Eine Datenerhebung bei Dritten wird ausdrücklich nur dann für zulässig erklärt, wenn der Betroffene einwilligt oder krankheits- oder behinderungsbedingt seine Einwilligung nicht erteilen kann und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Durch die gesetzlich geforderte Interessenabwägung bei fehlender Einwilligung werden die Rechte der Betroffenen hinreichend gewahrt.

6.5 JUS-IT: Daten der Jugendämter wurden erneut nicht gelöscht

Da über 30.000 Datensätze entgegen den gesetzlichen Anforderungen nicht gelöscht wurden, wurde eine Beanstandung ausgesprochen. Darüber hinaus sind nach wie vor noch rechtliche Aspekte der integrierten Hilfe und deren technische Umsetzung offen.

Auftrag des Großprojektes Projektes JUS-IT ist es, eine weitgehend integrierte Softwarelösung für die Bereiche Jugendhilfe, Sozialhilfe und Wohngeld fachlich und organisatorisch zu entwickeln und einzuführen sowie die Bestandsverfahren abzulösen. Die angestrebte IT-Lösung setzt auf den modularen Standards der Software Cúram auf. Cúram ist eine Fachsoftware zur Sozial- und Jugendhilfe mit integrierten Geschäftsprozessen, die weltweit, bisher mit einem Schwerpunkt auf dem angelsächsischen Raum, eingesetzt wird (vgl. 23. TB, 7.1). Im Mai 2012 erfolgte mit dem „Release 1" ein erster Realisierungsschritt in den Jugendämtern, im Kinder- und Jugendnotdienst und im Familieninterventionsteam. Mit dem „Release 2" soll die Einführung für den Bereich Jugend mit der neuen Unterstützung Unterhaltsvorschuss, Beistandschaft, Amtsvormundschaft, Jugendgerichtshilfe, Kostenbeitrag und Kostenerstattung im Sommer 2014 abgeschlossen werden. Die Umstellung im Bereich Soziales mit der Ablösung des derzeit genutzten IT-Verfahrens PROSA durch das „Release 3" ist für 2015 vorgesehen.

Seit Beginn des Projektes waren wir in das Vorhaben intensiv eingebunden und haben frühzeitig datenschutzrechtliche Anforderungen eingebracht. Da wir bei einer Prüfung in einem Jugendamt 2008 festgestellt hatten, dass in dem damals produktiv genutzten IT-Verfahren PROJUGA über 500.000 Sozialdatensätze entgegen den gesetzlichen Anforderungen nicht gelöscht wurden (vgl. 22. TB, 7.1), haben wir bereits in der ersten

Kontaktaufnahme mit dem Projekt JUS-IT die große Bedeutung des Themas „Löschen" herausgestellt und darauf hingewiesen, dass die IT-Prozesse zum Löschen von Daten von Anfang an konzeptionell berücksichtigt und bereits vor der Produktivsetzung implementiert werden sollen. Obwohl das Thema Löschen im weiteren Projektverlauf wiederholt Gegenstand von Beratungen mit uns war und das Projekt auch in der Feinspezifikation „Löschung" u.a. differenzierte Löschfristen festgeschrieben hat, wurde die Komponente „Löschen" in der Softwareentwicklung nicht mit dem Produktivstart von JUS-IT implementiert. Dies wurde auch weder mit einem Optimierungsrelease, das ca. 5 Monate später praktisch umgesetzt wurde, nachgeholt, noch war es in einer konkretisierten Planung für das Jahr 2013 vorgesehen.

Diese Entwicklung haben wir zum Anlass genommen, im Februar 2013 eine schriftliche Prüfung des Löschens im IT-Verfahren JUS-IT vorzunehmen. Ziel der Prüfung war es u.a. festzustellen, ob eine fristgerechte Löschung der Daten erfolgt ist. Der frühestmögliche Löschtermin besteht dabei entsprechend den festgelegten Löschfristen für Daten, die aus dem Vorgänger-IT-Verfahren übernommen wurden; da nur Daten übernommen wurden, deren Löschfristen nach dem 20.05.2012 lagen, ist der erste denkbare Löschtermin der 21.05.2012 gewesen. Bei entsprechend der Feinspezifikation monatlich vorgesehen Löschungen (Batchläufen) wäre ein solcher Datensatz im Juni 2012 zu löschen gewesen.

Nach Auskunft der zuständigen Fachlichen Leitstelle erfolgten nach der Produktivsetzung seit dem 21.05.2012 keine Löschungen (Batchläufe). Das bedeutet, dass Daten nicht gelöscht wurden, obwohl Datensätze mit personenbezogenen Daten die Löschfrist erreicht hatten. Zur Abschätzung des Umfanges der trotz Löschpflicht nicht erfolgten Löschung kann die erfolgte Löschung im Alt-Verfahren PROJUGA für den Zeitraum nach dem 21.05.2012 herangezogen werden, da die zu löschenden Datensätze auch dort noch gespeichert waren. Dort wurden zwischen dem 21.05.2012 und dem 01.03.2013 insgesamt 2.071 Datensätze ohne Fallbezug zu einem PROJUGA-Fall sowie 18.745 Mischfälle mit 33.845 Akten gelöscht.

Das Nicht-Löschen der einer Löschpflicht unterliegenden Daten im Bereich der Jugendhilfe stellt einen Verstoß gegen § 68 Abs. 2 Achtes Buch Sozialgesetzbuch (SGB VIII) in Verbindung mit § 84 Absatz 2 Satz 2 Zehntes Buch Sozialgesetzbuch (SGB X) dar. Auch war zum Zeitpunkt der Prüfung die Behebung des Gesetzesverstoßes nicht sicher absehbar. Im Zuge der Prüfung wurde auch bestätigt, dass die Software Cúram derzeit selbst keine Löschprozeduren anbietet, mit denen die im Sozialgesetzbuch festgeschriebenen datenschutzrechtlichen Anforderungen erfüllt werden können. Aus unserer Sicht erfüllt die Software Cúram damit eine wesentliche Anforderung nicht, die bei der Ausschreibung in der Leistungsbeschreibung explizit ausgewiesen war. Obwohl es laut Vorstudie von Dataport umfangreiche technische Fragestellungen zu klären gab, war nicht ansatzweise erkennbar, welche einzelnen Projektschritte geplant waren und wann die Implementierung der IT-Prozesse zum Löschen von Daten erfolgen sollte. Das

Projekt verfolgte offensichtlich über einen längeren Zeitraum eine Prioritätensetzung zu Lasten der Realisierung des Datenschutzes. Aus diesem Grund haben wir gemäß § 25 Abs. 1 Hamburgisches Datenschutzgesetz (HmbDSG) eine förmliche Beanstandung ausgesprochen. Das Projekt hat daraufhin die Aktivitäten zur Realisierung des Löschens intensiviert. Die Programmierung und die Funktionstests sind abgeschlossen und eine Löschung der Daten sollte zum 16.12.2013 erfolgen. Bei den Regressionstests im Dezember 2013 wurde jedoch ein Fehler der Schwere 2 „hoch" festgestellt, so dass eine Löschung nicht mehr vor Redaktionsschluss stattfand. Unsere Befürchtungen haben sich erneut bewahrheitet, dass eine Verschiebung der Regressionstests auf einen Termin kurz vor dem geplanten Echtlauf die eingeforderte Löschung in 2013 gefährden würde. Trotz aller Belastungen im Projekt ist nicht nachvollziehbar, dass damit nicht einmal innerhalb von 7 Monaten nach der Beanstandung die Löschung von Daten erfolgt ist, die zum Teil bereits in 2012 hätten gelöscht werden müssen.

Das Projekt JUS-IT ging seinerzeit auch an den Start, um eine „integrierte Sicht" im Rahmen der Sozialleistungen zu realisieren. Ziel war es, die Familie und ihre gesamten sozialrechtlich relevanten Probleme im Ganzen zu sehen. Es sollte nicht mehr so sein, dass das Jugendamt nicht weiß, was eine andere Jugendamts-Abteilung oder das Sozialamt machen. Dabei geht es um eine zielführende Zuschneidung der Hilfen für die Betroffenen, und zwar amtsübergreifend zwischen Jugendamt und Sozialamt ab dem Release 3, das Mitte 2015 produktiv werden soll, und darüber hinaus zu einem späteren Zeitpunkt auch mit der Wohngeldstelle. Aus Sicht des Projektes ist dafür eine gemeinsame Datenbasis zumindest für die Stammdaten eine wichtige Grundlage. Trotz dieser Sichtweise hat das Projekt im Berichtszeitraum aufgrund begrenzter Projektressourcen entschieden, dass mit Cúram zukünftig nicht alle Aufgaben der beiden Bereiche abgedeckt werden sollen, sondern die dafür bisher genutzte Software weiter verwendet werden soll. In diesen weitergenutzten Programmen ist jeweils eine eigene Stammdatenhaltung erforderlich. Dies führt dazu, dass nicht einmal im Bereich Soziales eine vollständige gemeinsame (Stamm-)Datenbasis gegeben sein wird.

Eine darüber hinausgehende gemeinsame Datenbasis für die unterschiedlichen Aufgabenbereiche Jugend und Soziales ist zudem nur zulässig, wenn die Voraussetzungen eingehalten werden, die das Sozialgesetzbuch dafür vorgibt. Dabei sind einerseits insbesondere §§ 67c, 67d, 69 und 79 SGB X zu beachten. Zentraldateien „können ohne bereichsspezifische Befugnisnorm nur insoweit als zulässig erachtet werden, als die Erforderlichkeit den Grad des unabweisbaren Notwendigen erreicht" (Rombach in Hauck/Noftz SGB X, § 69 Rn. 62, 64). Andererseits ist der Grundsatz der Datenerhebung beim Betroffenen zu berücksichtigen, wie er beispielsweise in § 67a Abs. 2 SGB X für die Datenerhebung im Sozialamt oder in § 62 Abs. 2 SGB VIII für das Jugendamt festgeschrieben ist. Abweichungen davon sind nur unter den gesetzlich genannten Voraussetzungen möglich. Ob die rechtlichen Grundlagen für eine gemeinsame Datenbasis und eine Dritterhebung gegeben sind, hat das Projekt noch nicht hinreichend aufgezeigt. Diese Fragestellungen sollen in einem Pilotbereich evaluiert werden. Erste

Zwischenergebnisse zeigen jedoch, dass zumindest der Anteil der Personen, die aus beiden Bereichen Hilfen beziehen, mit unter 0,5 Prozent sehr gering ist.

Da einerseits die Ergebnisse der Evaluierung nicht vorliegen und andererseits die weiteren Entwicklungsarbeiten auf einer sicheren Rechtsgrundlage erfolgen müssen, hat die Lenkungsgruppe des Projekts entschieden, bei der Ausgestaltung der Feinspezifikation für das „Release 3" von einem Modell der Mandantentrennung mit getrennter Stammdaten- und Falldatenverarbeitung für die Bereiche Jugend und Soziales auszugehen, das der folgenden Grafik entspricht. Wir haben diesen Beschluss begrüßt, da damit eine datenschutzgerechte Lösung angestrebt wird.

Logisches System JUS-IT

Wir haben darauf hingewiesen, dass auch bei einer getrennten Datenbasis und dieser mandantenfähigen Lösung einerseits positive wirtschaftliche Effekte durch die gemeinsame Infrastruktur genutzt werden können und andererseits die erforderlichen Informationsaustausche für eine integrierte Hilfe durch rechtlich zulässige Übermittlungen über standardisierte Schnittstellen ermöglicht werden können. Wir werden uns dafür einsetzen, dass die Anforderungen aus der Orientierungshilfe Mandantenfähigkeit (vgl. II. 1) eingehalten werden.

7. Schulwesen

7.1 Statistik in der Behörde für Schule und Berufsbildung

Mangels ausreichender gesetzlicher Grundlage sind die statistischen Tätigkeiten innerhalb der Behörde für Schule und Berufsbildung rechtswidrig; auch für die statistische Längsschnittuntersuchung, die bezüglich jeder Schülerin und jedes Schülers während der gesamten Schullaufbahn erstellt wird, fehlt die erforderliche gesetzliche Regelung.

Die grundlegende gesetzliche Regelung zu Statistiken im schulischen Bereich findet sich in § 98 Abs. 2 Hamburgisches Schulgesetz (HmbSG). Hiernach ist bei der Verarbeitung personenbezogener Daten zum Zwecke der Schulstatistik sicherzustellen, dass der Personenbezug außerhalb der staatlichen Schulen und der zuständigen Behörde nicht mehr herzustellen ist; ergänzend hierzu trifft § 6 Abs. 1 der Verordnung über

die Verarbeitung personenbezogener Daten im Schulwesen (Schul-Datenschutzverordnung) die allgemeine Regelung, dass alle in den §§ 1 und 5 Schul-Datenschutzverordnung genannten personenbezogenen Daten im Rahmen der Schulstatistik verarbeitet werden dürfen. Zwischen unserer Dienststelle und der Behörde für Schule und Berufsbildung bestand lange Zeit Uneinigkeit darüber, ob die gesetzlichen Regelungen den statistikrechtlichen Grundsätzen genügen. Die Besonderheit besteht dabei unter anderem darin, dass die Statistiken nicht – wie gewöhnlich üblich – durch eine externe Stelle erstellt werden, sondern durch organisatorisch zu der Behörde für Schule und Berufsbildung gehörende Abteilungen.

In seinem Volkszählungsurteil hat das Bundesverfassungsgericht die organisatorischen Voraussetzungen sowie Schutzmaßnahmen im Rahmen statistischer Erhebungen dargestellt. Ein Kernpunkt ist insoweit die gesetzlich abzusichernde Abschottung zwischen Statistik und Vollzug. Wurden Daten zu statistischen Zwecken erhoben, dürfen diese nicht zu Verwaltungsvollzugszwecken genutzt werden. Im schulischen Bereich Hamburgs werden die Statistiken – abgesehen von einzelnen Evaluationsdaten – aus den zunächst zu Verwaltungszwecken rechtmäßig erhobenen Daten erstellt. Solche Statistiken werden auch Geschäftsstatistiken genannt (vgl. § 8 Abs. 1 Hamburgisches Statistikgesetz - HambStatG). Während der gesamten Schullaufbahn der Kinder werden in der Behörde für Schule und Berufsbildung eine Vielzahl von Statistiken erstellt; zum Teil fallen hierunter auch Langzeituntersuchungen, die stetig mit neuen personenbezogenen Daten ergänzt werden und so ein umfassendes Profil der Kinder bilden. Hierin ist ein besonders starker Eingriff in das Grundrecht auf informationelle Selbstbestimmung zu sehen. Gerade in derartigen Konstellationen ist ein verfassungskonformer Ausgleich zwischen den statistischen Interessen auf der einen Seite und der Grundrechten der Betroffenen auf der anderen Seite zu schaffen. Auch wenn also – im Unterschied zur Situation im Volkszählungsurteil – die Daten primär nicht zu statistischen Zwecken erhoben werden, besteht das Erfordernis nach einer Abschottung und weiteren Schutzmaßnahmen auch hier, da die gegensätzlichen Interessenlagen vergleichbar sind. Um dem Grundrecht der Betroffenen auf informationelle Selbstbestimmung zu genügen, setzt ein internes statistisches Amt u.a. voraus, dass erstens nur erforderliche Daten erhoben werden dürfen, wobei auf solche Daten verzichtet werden sollte, die eine soziale Abstempelung befürchten lassen, dass zweitens primär anonyme Daten zu nutzen sind und dass drittens Löschung, Geheimhaltung und Abschottung gewährleistet sind.

Angesichts der diesbezüglichen Uneinigkeit wurde das Rechtsgutachten „Datenschutzrechtliche Bewertung spezifischer Fragen der Schulstatistik in Hamburg" von einem renommierten Rechtswissenschaftler eingeholt. Dieser beleuchtet in seinem Gutachten zwei Aspekte: Zum einen klärt er die – zwischen der Behörde für Schule und Berufsbildung und uns ebenso streitige – für die Beantwortung des Gutachtenauftrages vorgreifliche Frage, ob die staatlichen Schulen und die Behörde für Schule und Berufsbildung gemeinsam eine oder mehrere Daten verarbeitende Stellen sind;

bereits im letzten Tätigkeitsbericht hatten wir auch auf diese Uneinigkeit hingewiesen (vgl. 23. TB, III 8.4). Zum anderen betrachtet er die Voraussetzungen für eine eigene statistische Abteilung innerhalb der Behörde.

Der Gutachter kommt bzgl. der ersten, vorgreiflichen Frage zu dem Ergebnis, dass die Behörde für Schule und Berufsbildung gemeinsam mit den staatlichen Schulen nach den Vorschriften des HmbSG als eine Daten verarbeitende Stelle anzusehen ist. Er zieht zur Begründung Art. 2 d S. 1 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie) heran, nach dem der für die Verarbeitung Verantwortliche diejenige Behörde sei, „die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet." Diese Voraussetzungen sieht der Gutachter als erfüllt, da nach den speziellen schulrechtlichen Regelungen in Hamburg die staatlichen Schulen und die Behörde für Schule und Berufsbildung die gemeinsame Aufgabe haben, „schulische Bildung und Erziehung zu gewährleisten und hierfür ihre Leistungsfähigkeit zu messen und kontinuierlich zu verbessern, um den Anforderungen an das Schulwesen in einer sich ändernden Gesellschaft gerecht zu werden" (Seite 11 des Rechtsgutachtens). Im Hinblick auf diese speziell auf die Schulverwaltung in Hamburg anwendbare Gesetzeslage und weitere im Gutachten herausgearbeitete, individuelle Umstände konnten wir uns letztlich dieser Bewertung anschließen. Folge ist jedoch auch dann nicht, dass sämtliche personenbezogene Daten innerhalb der gesamten Schulverwaltung offen zugänglich sind; auch weiterhin ist z.B. der Grundsatz der Erforderlichkeit zu beachten, so dass die Daten den jeweiligen Abteilungen, Mitarbeitern usw. nur in dem Umfang bekannt sein dürfen, wie sie zur Erfüllung deren jeweiliger Aufgaben erforderlich sind.

Des Weiteren kommt der Gutachter in Bezug auf die statistische Tätigkeiten der Behörde für Schule und Berufsbildung zu dem Ergebnis im von uns vertretenen Sinne, dass die Behörde für Schule und Berufsbildung einer detaillierteren gesetzlichen Regelung bedarf, um selber Statistiken erstellen zu dürfen. Inhalt einer solchen, die Tätigkeiten eines statistischen Amtes rechtfertigenden Regelung müsse u.a. eine Aufgabenbestimmung und Zweckbindung, die Forderung nach ausreichender Datenaggregierung innerhalb des statistischen Amtes vor einer weiteren Übermittlung, die organisatorische, räumliche und personelle Abschottung sowie weitere formelle Anforderungen wie Speicherfristen sein. Gleichzeitig wurde hierbei bestätigt, dass auch für Langzeituntersuchungen angesichts deren erhöhten Gefährdungspotentials für das informationelle Selbstbestimmungsrecht eine konkrete und verhältnismäßige gesetzliche Grundlage zu schaffen ist.

Auf der Grundlage dieser Bestätigungen, dass sowohl die statistischen Tätigkeiten an sich wie auch konkret die Langzeituntersuchungen mangels rechtfertigender gesetzlicher Grundlage rechtswidrig sind, haben wir die Behörde für Schule und Berufsbildung

aufgefordert, diesen Zustand zu beseitigen. Bisher erfolgte ein erstes Gespräch, in dem seitens der Behörde für Schule und Berufsbildung erklärt wurde, entsprechende gesetzliche Regelungen zu entwerfen. Wir werden darauf achten, dass die Statistiken zukünftig auf einer entsprechenden Rechtsgrundlage erhoben werden, und im nächsten Tätigkeitsbericht darüber informieren.

7.2 Nutzung sozialer Netzwerke zu schulischen Zwecken

Die Behörde für Schule und Berufsbildung hält die derzeitige Gesetzeslage in Hamburg für ausreichend, um die Nutzung von Facebook und Co. durch die Lehrerschaft im schulischen Bereich auszuschließen, im Übrigen sollen Schulungen präventiv wirken.

Das Kultusministerium Baden-Württemberg hat im Jahr 2013 eine Handreichung herausgegeben, nach der von der Nutzung sozialer Netzwerke zu dienstlichen Kommunikationszwecken abzusehen ist. Hintergrund ist, dass die Verarbeitung personenbezogener Daten auf derartigen Plattformen unzulässig sein dürfte, da die Datenschutzstandards nicht mit deutschen Datenschutzstandards in Einklang stehen, wenn z.B. deren Server außerhalb des europäischen Wirtschaftsraumes betrieben werden.
Aus unserer Sicht ist die Nutzung von sozialen Medien zur Verarbeitung personenbezogener Daten zu dienstlichen Zwecken auf gesetzlicher Grundlage des Hamburgischen Datenschutzgesetzes (HmbDSG) verboten. Private Dienstanbieter für die Erhebung, Verarbeitung und Nutzung solcher Daten einzubeziehen, wäre für staatliche Schulen in Hamburg nur unter den Voraussetzungen des § 16 HmbDSG zulässig. Da aber die Datenschutzbestimmungen vor allem von Facebook die Verwendung der Daten auch zu eigenen Zwecken vorsieht, ist die gesetzliche Voraussetzung nicht erfüllt, dass der Empfänger die Daten nur zu dem Zweck verarbeiten darf, zu dem er sie erhalten hat.

Auf eine schriftliche Kleine Anfrage antwortete der Senat, dass eine Vorgehensweise wie in Baden-Württemberg nicht geplant ist. Hierneben wird auf Broschüren und auf folgende Maßnahmen verwiesen: Verankerung des Aufgabengebietes Medienerziehung im Rahmenplan, Hamburger Medienpass und Medienscouts. Die Behörde setzt somit auf präventive Schulungsmaßnahmen. Wir haben bereits im Jahr 2010 u.a. in Kooperation mit der Medienanstalt Hamburg/Schleswig-Holstein und dem Landesinstitut für Lehrerbildung und Schulentwicklung sowie der Schulbehörde die Broschüre „Meine Daten kriegt ihr nicht" herausgegeben. Ziel muss es insoweit sein, die Schülerinnen und Schüler einen verantwortungsbewussten Umgang mit sozialen Netzwerken zu lehren; dies setzt aber auch voraus, dass die Lehrerinnen und Lehrer ihrerseits entsprechend geschult sind, um fundiert Wissen vermitteln zu können.
Aus unserer Sicht ist daher Folgendes wichtig:

1. Die Nutzung von Facebook durch die Hamburger Lehrerschaft bei der Verarbeitung personenbezogener Daten zu dienstlichen Kommunikationszwecken ist allein aufgrund der gesetzlichen Befugnisnormen nicht zulässig.

2. Die in Schulen teilweise erfolgende Nutzung von Facebook zu dienstlichen Kommunikationszwecken auf der Grundlage einer Einwilligungserklärung der Betroffenen prüfen wir derzeit intensiv, insbesondere hinsichtlich der gesetzlichen Anforderungen an eine wirksame Einwilligung im Sinne eines informed consents.

3. Um der Schülerschaft die Funktionalitäten sozialer Netzwerke bieten zu können, prüfen wir derzeit eine alternative Plattformlösung, die den datenschutzrechtlichen Anforderungen genügt.

4. Medienkompetenz darf nicht nur im Rahmenplan verankert sein, sondern muss in der heutigen vernetzten Welt ein reguläres Unterrichtsfach werden, in dem auch die Datenschutzkompetenz von Schülerinnen und Schülern gefördert wird.

7.3 IServ

Die Einführung von IServ kann den Schülerinnen und Schülern die Möglichkeit bieten, den verantwortungsvollen Umgang mit Netzwerken im schuleigenen Netzwerk zu erlernen. Dies setzt jedoch eine datenschutzgerechte Ausgestaltung des Verfahrens an den Schulen voraus

Durch Eingaben wurden wir auf IServ und den Einsatz des Verfahrens an hamburgischen Schulen aufmerksam. IServ ist eine IT-gestützte Lern- und Kommunikationslösung für den Einsatz im pädagogischen Netzwerk von Schulen. Sie umfasst verschiedene Komponenten. Hierzu gehören Kommunikationsmöglichkeiten (E-Mail, Chat, Foren), Funktionen zur Schulorganisation (Kalender, Adressbuch, Infobildschirm), die Bereitstellung und der Abruf von Unterlagen vom Fileserver und der Zugang zum Internet. Der Zugriff über die Weboberfläche ist für die registrierten Nutzer nach Eingabe ihres Accounts und ihres Passwortes innerhalb des schuleigenen Netzes vorgesehen, kann jedoch in der Regel auch über das Internet von zu Hause aus erfolgen. Schüler und Lehrer können E-Mails austauschen sowie Daten, Referate und Präsentationen von zu Hause speichern und im Unterricht darauf zugreifen.

Die Einführung von IServ war an verschiedenen hamburgischen Schulen erfolgt, ohne dass wir zuvor beteiligt wurden. Wir haben das Thema daher unsererseits aufgegriffen. Der von der BSB erstellten und uns auf Anforderung übersandten Risikoanalyse und Verfahrensbeschreibung sowie der zur Abstimmung übersandten

Musternutzungsordnung für IT-Einrichtungen der Schule sind zu entnehmen, dass die BSB für IServ an hamburgischen Schulen grundsätzlich einen normativen und organisatorischen Rahmen vorgibt. Den Schulen werden hierbei bislang jedoch beispielsweise hinsichtlich der Entscheidung darüber, IServ-Funktionen auch für private Zwecke zu öffnen, den Nutzerkreis um Sorgeberechtigte zu erweitern, den Nutzern einen externen E-Mail-Verkehr zu ermöglichen sowie über konkrete Aufsichtsmaßnahmen für die Internetnutzung zu entscheiden, Gestaltungsfreiräume einräumt.
Wir haben problematisiert, dass Schulen durch entsprechende Entscheidungen sowohl zum Telekommunikationsanbieter als auch zu einem Telemediendienst-Anbieter nach § 3 Nr. 6 TKG/§ 11 TMG werden können und damit den Bestimmungen des TKG und des TMG unterliegen.
Die BSB hat uns daraufhin bestätigt, dass bis zur Klärung der daraus resultierenden offenen rechtlichen Fragestellungen die Schulen nur eine interne Kommunikation innerhalb des geschlossenen Benutzerkreises der Schule ermöglichen.

Neben den rechtlichen Fragestellungen wird bei der Bewertung des Verfahrens zu beachten sein, dass die dezentrale IT-Ausstattung, die Konfiguration und Organisation der Datenverarbeitung in den pädagogischen Netzen der Schulen unterschiedlich gestaltet ist.

Wir sehen das Potential, welches das Verfahren für Schulen im Rahmen der Medienerziehung bieten kann ebenso wie die Vorteile, den verantwortungsvollen Umgang mit Netzwerken in einem schuleigenen Netzwerk kennenzulernen. Es gilt jedoch die mit dem Verfahren verbundenen Risiken wirksam zu beherrschen. Wir prüfen unter welchen rechtlichen und technischen Voraussetzungen die datenschutzgerechte Ausgestaltung des Verfahrens an den hamburgischen Schulen realisiert werden kann.

7.4 Medienkompetenz – Hamburger Medienpass

Die Behörde für Schule und Berufsbildung geht auf dem Weg zum Bildungsziel „Medienkompetenz" mit dem Angebot „Hamburger Medienpass" einen weiteren Schritt voran.

Bereits vor einigen Jahren haben wir erkannt, wie wichtig es ist, die Medien- und die Datenschutzkompetenz der Schülerinnen und Schüler zu fördern. Schon im Jahr 2010 haben wir daher u.a. in Kooperation mit der Medienanstalt Hamburg/Schleswig-Holstein und dem Landesinstitut für Lehrerbildung und Schulentwicklung sowie der Schulbehörde die Broschüre „Meine Daten kriegt ihr nicht" herausgegeben. Die Nutzung dieser Handreichung, die den Lehrerinnen und Lehrern konkrete Vorschläge für eine Unterrichtseinheit bietet, erfolgt jedoch nur zögerlich.

Im Jahr 2013 initiierte die Behörde für Schule und Berufsbildung in Kooperation mit

dem Landesinstitut für Lehrerbildung und Schulentwicklung das Projekt „Hamburger Medienpass". Dieser besteht aus fünf Modulen zu je drei Doppelstunden und umfasst die Themen Computerspiele, soziale Netzwerke, Urheberrecht, Cyber-Mobbing und Smartphone. Wir haben angeboten, uns am Hamburger Medienpass zu beteiligen und ein Modul hierfür eigenständig zu entwickeln. Insoweit wurde vor wenigen Monaten eines der fünf Module in „Datenschutz und soziale Netzwerke" umbenannt. Wir haben uns daran gern beteiligt und dazu Unterrichtsmaterial erstellt, das sowohl die Medien- als auch die Datenschutzkompetenz der Schülerinnen und Schülern insbesondere anhand des Umganges mit sozialen Netzwerken nahebringen soll. Zwar wurde das Aufgabengebiet „Medienerziehung" im Rahmenplan verankert; die einzelne Schule ist jedoch frei darin, zur Erreichung dieses Bildungszieles den Medienpass zu nutzen. Bei deren Verwendung bestimmt die Schule ferner individuell, die Module auf die 5. bis zur 8. Jahrgangsstufe zu verteilen oder z.B. zusammenhängend als Projektwoche anzubieten. Verbesserungswürdig ist die fehlende Verbindlichkeit. Die Datenschutzkompetenzförderung sollte zu den verbindlichen Kerninhalten zählen, die allen Schülerinnen und Schülern hamburgweit angeboten werden. Die Schülerinnen und Schüler erhalten den Medienpass, in dem jedes absolvierte Modul eingetragen wird. Ist eine Schülerin oder ein Schüler jedoch z.B. aufgrund einer Erkrankung daran gehindert, das anstehende Modul zu bearbeiten, besteht keine Pflicht, dies nachzuholen; denkbar – so die verantwortlichen Initiatoren – könnte allenfalls die freiwillige Teilnahme zu späteren Zeiten innerhalb eines anderen Klassenverbundes sein. Auch die Abfrage und Überprüfung des Erlernten ist unseres Wissens nicht vorgesehen.

Die Einführung des Medienpasses ist ein weiterer Schritt in die richtige Richtung. Es bleibt dennoch abzuwarten, in welchem Ausmaß der Hamburger Medienpass genutzt werden wird und zu einer umfassenden Bildung der Jugendlichen beiträgt. Angesichts des geringen Grades an Verbindlichkeit des Hamburger Medienpasses muss das Fernziel aber weiterhin sein, alle Hamburger Schülerinnen und Schüler verpflichtend in Medien- und Datenschutzkompetenz zu bilden. Die Fähigkeit, mit den eigenen Daten verantwortungsvoll umzugehen und die Daten anderer respektvoll zu behandeln, ist eine wichtige Grundkompetenz für das Leben in der digitalen Gesellschaft.

7.5 Jugendberufsagentur – Datenschutzgerecht soll niemand verloren gehen

Die Ausgestaltung der Jugendberufsagentur wird erfolgreich datenschutzgerecht begleitet.

In der Jugendberufsagentur Hamburg (JBA) haben sich das Jobcenter team.arbeit.hamburg, die Stadt Hamburg und die Arbeitsagentur zusammengetan, um jungen

Menschen beim Einstieg in das Berufsleben zu helfen. Die drei Institutionen arbeiten dabei unter einem Dach, aber die JBA besitzt keine eigene Rechtsfähigkeit. Im Außenverhältnis bestehen die Rechtsbeziehungen der Kundinnen und Kunden der JBA daher weiterhin jeweils zu der leistungserbringenden Körperschaft.

Damit der Anspruch „Niemand soll verloren gehen" frühzeitig und umfassend eingelöst wird, werden bereits alle schulpflichtigen Schülerinnen und Schüler der Hamburger Schulabgangsklassen im Rahmen des berufsorientierenden Unterrichts erfasst und von der Berufsberatung der Arbeitsagentur beraten. Im Zuge der Berufsorientierung holt die Schule von den Jugendlichen bzw. deren Erziehungsberechtigten eine Einverständniserklärung ein. Mit einer Einverständniserklärung stimmen die Jugendlichen bzw. ihre Erziehungsberechtigten der Datenübermittlung an die Jugendberufsagentur zu, damit diese ihnen konkrete Dienstleistungen anbieten kann, um sie auch nach Verlassen der Schule zu beraten, zu vermitteln und zu fördern.

Das Konzept der JBA setzt auf die Freiwilligkeit der Inanspruchnahme der Leistung. Die JBA ist die zentrale Anlaufstelle für junge Menschen, die Beratung, Vermittlung und Unterstützung möchten bei:

- der Berufswahl und -vorbereitung
- der Suche nach einem geeigneten Ausbildungsplatz
- der Wahl geeigneter Bildungswege im berufsbildenden System
- der Wahl des passenden Studiums
- der Bewältigung schulischer Probleme

Wir haben den Aufbauprozess der JBA im Berichtszeitraum begleitet. Die datenschutzrechtlichen Anforderungen waren dabei insbesondere auf drei Ebenen zu beachten:

- Um eine tragfähige Rechtsgrundlage für das Wirken der Behörde für Schule und Berufsbildung (BSB) im Kontext der JBA zu ermöglichen, wurde der § 3 Abs. 7 Hamburgische Schulgesetz (HmbSG) eingefügt, wonach auch nach Erfüllung der Schulpflicht die Schulen mit den Trägern der beruflichen Bildung und den Sozialleistungsträgern kooperieren, um solche Schülerinnen und Schüler zu beraten und zu fördern, die noch keine Ausbildung abgeschlossen haben. Auch wurde durch eine Ergänzung in § 98 Abs. 1 HmbSG der Rahmen geschaffen, der für eine Nachsorge nach Beendigung der Schulpflicht bis zur Vollendung ihres 21. Lebensjahres die erforderliche Datenverarbeitung durch die BSB ermöglicht.
- Da die Datenübermittlung an die an der JBA beteiligten Institutionen eine datenschutzrechtliche Einwilligung erfordert, wurden entsprechende Erklärungen abgestimmt.
- Zahlreiche datenschutzrechtliche Einzelaspekte insbesondere des Einsatzes bestehender automatisierter Verarbeitung personenbezogener Daten wurden erörtert. Unsere Anforderungen an eine datensparsame Lösung wurden von der BSB

umgesetzt. Die gefundenen Lösungen setzen auf der getrennten Nutzung der IT-Prozesse der beteiligten Institutionen auf. Ein gemeinsames IT-Verfahren betreibt die JBA nicht.

Wir haben erfreut zur Kenntnis genommen, dass nach der datenschutzgerechten Realisierung der JBA in Hamburg das Konzept der JBA auch außerhalb Hamburgs aufgegriffen und auch dabei die Anforderungen des Datenschutzes explizit benannt wurden.

7.6 Landesmusikakademie Hamburg – Seminarverwaltung

Die Errichtung der Seminarverwaltung der Landesmusikakademie Hamburg steht derzeit vor grundlegenden offenen Fragen; das bisherige Konzept mit einer gemeinsamen Datei scheitert an § 11a Hamburgisches Datenschutzgesetz (HmbDSG).

Die Behörde für Schule und Berufsbildung hat für die ihr nachgeordnete staatliche Jugendmusikschule gemeinsam mit dem Hamburger Konservatorium und dem Landesmusikrat Hamburg e.V. einen Vertrag zur Bildung der Landesmusikakademie Hamburg geschlossen, deren Gegenstand die Kooperation der Fortbildungsabteilungen ist. Sie dient u.a. dem Zweck, eine Koordinierung der Angebote hinsichtlich des musikpädagogischen Bedarfs und des sich verändernden Schul- und Bildungssystems herbeizuführen; die Institute führen aber ihre eigenen Fortbildungen auf eigene Rechnung durch. Um dieses Ziel zu unterstützen, plant die Landesmusikakademie die Errichtung einer Seminarverwaltung, in der sowohl die staatliche Jugendmusikschule wie auch das Hamburger Konservatorium neben den angebotenen Kursen gemeinsam die Teilnehmerdaten personenbezogen verarbeiten sollen.

Die Landesmusikakademie legte uns eine Verfahrensbeschreibung und ein kurzes IT- und Sicherheitskonzept vor, das gleichzeitig die Risikoanalyse beinhaltet. Daher haben wir den Datenschutzbeauftragten der Behörde eingebunden und um eine behördeninterne Aufarbeitung der Unterlagen gebeten. Hierbei wiesen wir auf verschiedene kritische Punkte hin, u.a. die Fragen nach der Rechtsgrundlage, einer eventuellen Auftragsdatenverarbeitung und der Festlegung von Speicherfristen. Da das Hamburger Konservatorium eine nicht-öffentliche, die staatliche Jugendmusikschule aber eine öffentliche Stelle ist, gingen wir insbesondere auch auf die aus unserer Sicht dem Vorhaben grundlegend entgegenstehende gesetzliche Regelung des § 11a HmbDSG ein. Hiernach bedarf die Einrichtung einer automatisierten Datei, in der mehrere Daten verarbeitende Stellen personenbezogene Daten verarbeiten sollen, der ausdrücklichen Zulassung durch eine Rechtsvorschrift. Die gesetzliche Definition einer „Daten verarbeitenden Stelle" verweist auf § 2 Abs. 1 S. 1 HmbDSG; somit kommt die Errichtung einer gemeinsamen Datei nach dem HmbDSG nicht in

Betracht, sofern an dieser sowohl nicht-öffentliche wie auch hamburgische öffentliche Stellen beteiligt sein sollen. An dieser gesetzlichen Voraussetzung scheitert das Konzept derzeitig datenschutzrechtlich.

Die Landesmusikakademie steht somit bei ihrer Seminarverwaltung vor allem im Hinblick auf die personenbezogene Verarbeitung der Teilnehmerdaten vor durchgreifenden rechtlichen Bedenken. Derzeit ist die Behörde für Schule und Berufsbildung mit der Lösung befasst; hierbei steht auch die Frage nach der Rechtsform der Landesmusikakademie auf dem Prüfstand.

7.7 Bildungs- und Betreuungsangebote an Schulen

Wer für die Leistungen der Nachmittagsbetreuung an der Schule oder ein Mittagessen in der Schulkantine Ermäßigungen in Anspruch nimmt, muss Angaben über seine Sozialleistungsbezüge oder Einkommensverhältnisse machen und nachweisen.
Diese Informationen müssen besonders geschützt werden und dürfen ausschließlich für die Berechnung der Gebühr/des Zuschusses verarbeitet werden.

Mit der Umsetzung der ganztägigen Bildung und Betreuung (GBS) und des Ganztagsangebotes (GTS) wird in Hamburg ein umfangreiches Bildungs- und Betreuungsangebot für Kinder geschaffen. Neben kostenlosen Angeboten beinhaltet das Konzept kostenpflichtige Angebote wie z.B. die Betreuungsangebote in Randzeiten sowie die Möglichkeit zu einem kostengünstigen Mittagessen. Eine soziale Staffelung der Gebühren bzw. die Gewährung von Zuschüssen soll allen Schülerinnen und Schülern, deren Eltern dies wollen, unabhängig vom sozialen und wirtschaftlichen Status der Familie den gleichen Zugang zu den Angeboten ermöglichen. Eltern, welche eine Reduzierung der Gebühren für die ganztägige Bildung und Betreuung oder eine Bezuschussung für das Mittagessen benötigen, müssen zusammen mit einer Erklärung zu ihrem monatlichen Einkommen oder einem Nachweis darüber, dass sie nach dem Bildungs- und Teilhabepaket leistungsberechtigt sind, einen entsprechenden Antrag stellen. Die Antragsunterlagen werden in den Schulbüros entgegengenommen und sollen dort getrennt von der Schülerakte in einem verschlossenen Schrank aufbewahrt werden. Zugang soll nur die Schulsekretärin und die Schulleitung haben.

Für die Berechnung der von den Eltern zu leistenden GBS/GTS-Gebühren sowie die Abrechnung beteiligter Träger der Jugendhilfe wird den Schulen von der Behörde für Schule und Berufsbildung (BSB) eine Abrechnungsanwendung zur Verfügung gestellt. Die Verarbeitung der Einkommensdaten ist in der Schuldatenschutzverordnung nicht vorgesehen und basiert daher bislang auf der Einwilligung der Sorgeberechtigten.

Sowohl der behördliche Datenschutzbeauftragte der BSB als auch wir sind in dieses Verfahren eingebunden. Die datenschutzrechtliche Abstimmung zu diesem Verfahren konnte bislang jedoch noch nicht vollständig abgeschlossen werden.

Datenschutzrechtlich problematisch stellte sich die vorgesehene Organisation der Mittagessenausgabe und -abrechnung dar. Die Organisation obliegt grundsätzlich der jeweiligen Schule. Hierbei kann diese entweder selbst eine Kantine betreiben oder aber eine Kantine durch einen anderen Rechtsträger betreiben lassen. In der Regel bedienen sich die Schulen der Leistungen professioneller Anbieter für die Schulverpflegung (Caterer), welche das Bestell- und Abrechnungsverfahren wiederum häufig von entsprechend spezialisierten Abrechnungsunternehmen durchführen lassen. Grundlage für die Zusammenarbeit ist ein „Vertrag über eine Dienstleistungskonzession für Mittagsverpflegung in Schulen sowie ergänzender Leistungen".

Für die der Essensausgabe zugrunde liegenden Verfahren müssen Eltern ihr Kind in der Regel für eine gewünschte Teilnahme u.a. mit Vor- und Zunamen, Klasse und E-Mailadresse für ein Bestellsystem im Internet registrieren. Die Bezahlung erfolgt über ein persönliches Guthabenkonto, auf welches im Vorwege ausreichend Geld überwiesen worden sein muss, damit eine Bestellung - welche ebenfalls über das Internet erfolgt - möglich ist. Für Mittagessen, die bezuschusst werden, wird nur der verbleibende Eigenanteil der Eltern abgebucht. Die Essenausgabe erfolgt am Ausgabetresen in der Schulkantine, nachdem sich das Kind mittels eines von den Eltern bzw. von der Schule mit dem Caterer vereinbarten Identifizierungsverfahrens (elektronisch lesbarem Ausweis, Transponder, Fingerprint, Chipkarte o.ä.) ausgewiesen hat. Die gesamte Abrechnung liegt in der Verantwortung des Caterers. Über die tatsächlichen Zuschussbeträge erhält die Schule eine Gesamtabrechnung, in welcher der aufgelaufene Förderbetrag je Schüler ausgewiesen wird. Die für dieses Verfahren notwendigerweise erfolgende Übermittlung der prozentualen Höhe des bewilligten Zuschusses an den in der Regel privatrechtlich organisierten Caterer wurde von uns kritisiert, zumal es hierfür keine gesetzliche Grundlage gibt und Einwilligungserklärungen nicht eingeholt wurden.

Die BSB begründet das Verfahren damit, dass die Essensausgabe schnell und aus verschiedenen Gründen möglichst bargeldlos erfolgen soll. Gerade Kinder einkommensschwacher Familien sollen zudem nicht nur deshalb vom Mittagessen ausgeschlossen werden, weil die Eltern die Kosten nicht im Vorwege in voller Höhe bezahlen können. Zudem soll bei der Essensausgabe weder für Mitschüler, Lehrer oder Bedienstete in der Essensausgabe erkennbar sein, wer Vollzahler ist und wer einen Zuschuss erhält, um eine Stigmatisierung der Kinder zu vermeiden. Zuschüsse für Mittagessen können zudem nur für tatsächlich in Anspruch genommene Leistungen gewährt werden. Von uns alternativ vorgeschlagene Lösungen, die Abrechnung behördenintern vorzunehmen, so dass eine Übermittlung der Zuschusshöhe nicht erforderlich ist, wurden von der BSB aufgrund des hiermit verbundenen Verwaltungsaufwandes in den Schulen bisher als nicht realisierbar eingestuft.

Übereinkunft besteht inzwischen dahingehend, dass für eine Datenübermittlung an den Caterer und/oder Abrechnungsstellen eine Einwilligung der Betroffenen erforderlich ist, da die gesetzlichen Vorschriften keine Grundlage hierfür bieten. Muster für entsprechende Einwilligungserklärungen liegen uns inzwischen vor, welche zur Zeit inhaltlich abgestimmt werden. Wir werden uns weiter für eine datenschutzgerechte Ausgestaltung des Verfahrens einsetzen.

7.8 Mittagessen, Biometrie und Einwilligungserklärung

Die Schulen und die Behörde für Schule und Berufsbildung gemeinsam als eine Daten verarbeitende Stelle sind zwar datenschutzrechtlich nicht für die Erhebung biometrischer Daten von Kindern zum Zwecke deren Identifikation beim Schulmittagessen verantwortlich; sie übermittelten aber in diesem Zusammenhang ohne Rechtsgrundlage Daten an Caterer und deren zu Abrechnungszwecken hinzugezogenen Unternehmen.

Mehrere besorgte Eltern informierten uns darüber, dass im Zusammenhang mit dem Schulmittagessen biometrische Daten ihrer Kinder erhoben wurden, obwohl sie hierzu nicht ihre Einwilligung erteilt hatten. Wir haben hieraufhin umgehend Ermittlungen aufgenommen und festgestellt, dass ein Unternehmen mit Sitz in Schleswig-Holstein, das von einem Caterer zum Zwecke der Abrechnung der Mittagessen hinzugezogen wurde, mehrere Methoden anbietet, mit denen sich die Schulkinder bei der Mittagessensausgabe identifizieren können. Zu diesen Methoden gehört unter anderem die Identifikation mittels RFID-Karte oder mittels biometrischer Daten. Bei Letzterem wird zwar nicht der gesamte Fingerabdruck elektronisch eingelesen, gespeichert und zu Identifikationszwecken genutzt, sondern nur einige markante Merkmale des jeweiligen Fingerabdruckes; dennoch dient dieses elektronisch gespeicherte Fingertemplate zur Identifikation innerhalb der jeweiligen Schülerschaft, so dass darin ebenfalls personenbezogene Daten zu sehen sind. Da es sich auch bei diesem Fingertemplate um personenbezogene Daten handelt, greift deren Verarbeitung in das informationelle Selbstbestimmungsrecht des Betroffenen ein. Eine Verletzung dieses Rechtes liegt allerdings dann nicht vor, wenn eine wirksame Einwilligung erteilt wurde.

Verfahrenstechnisch wird zu Beginn der Fingerabdruck eines Kindes gescannt; dabei werden markante Punkte in einem Template zusammengefasst. Will sich ein Kind bei der Mittagessensausgabe identifizieren, so legt es seinen Finger auf, und die markanten Punkte werden erneut erhoben und mit den gespeicherten Templates verglichen. Liegt eine Übereinstimmung vor, so ist das Kind identifiziert, erhält das gebuchte Essen, und die finanzielle Abrechnung kann digital erfolgen.

Unsere weiteren Recherchen zur vertraglichen Ausgestaltung haben ergeben, dass die jeweilige Schule und der Caterer einen „Vertrag über eine Dienstleistungskonzession für Mittagsverpflegung in Schulen sowie ergänzende Leistungen" geschlossen haben. Hierin wird der Caterer verpflichtet, einerseits die datenschutzrechtlichen Bestimmungen nach dem Bundesdatenschutzgesetz einzuhalten und andererseits die finanzielle Abwicklung zu übernehmen; zu diesen Zwecken wurde in den konkreten Fällen von dem Caterer vertragsrechtlich eine IT-Firma mit Sitz in Schleswig-Holstein hinzugezogen. Ferner werden Verträge zwischen den Schülerinnen und Schülern bzw. deren gesetzlichen Vertretern und dem Caterer geschlossen. Eine vertragliche Beziehung zwischen der Schule und der Behörde für Schule und Berufsbildung einerseits und der IT-Firma andererseits besteht hingegen nicht.

Im Zuge unserer Ermittlungen hat sich auch bestätigt, dass die IT-Firma biometrische Daten auch von Kindern erhoben und verarbeitet hat, deren gesetzliche Vertreter hierzu nicht ihre Einwilligung erteilt haben. Da der Sitz dieser IT-Firma in Schleswig-Holstein liegt, haben wir das weitere Verfahren bzgl. der ohne Rechtsgrundlage erhobenen biometrischen Daten an die zuständige datenschutzrechtliche Aufsichtsbehörde, das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein abgegeben. Dennoch haben wir auch die Behörde angeschrieben und unter anderem die Frage gestellt, welche sonstigen personenbezogenen Daten an den Caterer und/oder die Abrechnungsfirma übermittelt werden; schon nach unserem damaligen Verständnis im August 2013 benötigt die Abrechnungsfirma schülerbezogene Daten wie z.B. Namen, Vornamen und jedenfalls auch die Tatsache der Leistungsberechtigung nach dem Bildungs- und Teilhabepaket des Bundes (BuT), um eventuelle Zuschüsse zum Mittagessen bzw. den elterlichen prozentualen Anteil an den Kosten zu berücksichtigen. Da nach unserer Ansicht als Rechtsgrundlage für eine solche Datenübermittlung von der Schule bzw. Behörde für Schule und Berufsbildung an private Stellen nur eine Einwilligung der Betroffenen in Betracht kommt, haben wir gleichzeitig auch um Zusendung einer entsprechenden Einwilligungserklärung gebeten.

Nachdem uns die Behörde für Schule und Berufsbildung zunächst widersprüchliche Auskünfte erteilt hatte, erklärte sie uns im November 2013, dass personenbezogene Daten (Vorname, Name, Geburtsdatum, Klasse, Anschrift und prozentualer Elternanteil der Essenszahlung) an die Abrechnungsfirma übermittelt wurden und dass hierfür keine Einwilligungen eingeholt wurden (vgl. auch III 7.7). Uns wurde daraufhin der Entwurf eines neuen Antragsformulars vorgelegt. Einige Anpassungen müssen aus unserer Sicht hierbei jedoch noch vorgenommen werden, damit von einer wirksamen Einwilligungserklärung ausgegangen werden kann. Wir haben dabei nochmals darauf hingewiesen, dass die Einwilligungserklärung sämtlicher Betroffener umgehend einzuholen ist.

Wir werden weiterhin genau darauf achten, dass die Behebung dieses rechtswidrigen Zustandes zeitnah zum Schutz des informationellen Selbstbestimmungsrechtes der Betroffenen erfolgen wird.

7.9 Protokollierung der Abrufe aus dem ZSR

Die Protokollierung der Abrufe aus dem Zentralen Schülerregister entspricht zwar noch der Ratio des Gesetzes; jedoch ist bisher ungeklärt, ob und inwieweit anhand dieser Protokollierung auch eine Überprüfung der Zulässigkeit der jeweiligen Abrufe erfolgt.

Wie im letzten Tätigkeitsbericht dargestellt, war zuletzt unklar, ob die gesetzlichen Anforderungen an den Inhalt der Protokollierung eines Abrufs erfüllt sind. § 10 Abs. 2 Satz 2 der Verordnung über die Verarbeitung personenbezogener Daten im Schulwesen (Schul-Datenschutzverordnung) bestimmt u.a., dass auch die Kennung des zum Abruf zugelassenen Datenendgerätes zu protokollieren ist. Auch weiterhin entspricht die derzeitige Protokollierung nicht dem Gesetzeswortlaut, da nur die zentrale IP-Adresse der Polizei protokolliert wird; Hintergrund ist, dass die Polizei mittels einer Firmenkennung über Hamburg-Gateway Zugriff auf das Zentrale Schülerregister nimmt, eine Übermittlung der IP-Adresse der jeweiligen Datenendgeräte dabei technisch aber nicht möglich ist. Organisatorisch ist aber geregelt, dass nur die Bediensteten des Führungslagedienstes der Polizei Zugriff auf das Zentrale Schülerregister nehmen und die Informationen an die anfragenden Bediensteten weitergeben.

Dies ist nach dem Gesetzeszweck ausreichend: Zweck der Protokollierung ist die nachträgliche Überprüfbarkeit der Zulässigkeit. Um diese Kontrolle ausüben zu können, ist es angesichts der arbeitsteiligen Organisation innerhalb der Polizei erforderlich, dass auch der den Abruf ursprünglich „verursachende" Bedienstete protokolliert wird. Dies erfolgt in der manuellen Dokumentation durch die Polizei. Mit den vorhandenen protokollierten Daten kann somit nachträglich zurückverfolgt werden, welcher Bedienstete aus welchem Grund einen konkreten Abruf verursacht hat, um die Zulässigkeit dieses Abrufes zu bewerten.

Als ungeklärt erwies sich hingegen die tatsächliche Überprüfung der protokollierten Abrufgründe durch die Behörde für Schule und Berufsbildung. § 10 Abs. 1 Satz 1 Schul-Datenschutzverordnung bestimmt, dass den Polizeivollzugsstellen, den Jugendämtern und den Gesundheitsämtern Daten nur „zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben" übermittelt werden dürfen. Wir haben im Zusammenhang mit unserer Prüfung auch eine Liste derjenigen Gründe angefordert, die für die jeweiligen Abrufe bisher protokolliert wurden. Bezüglich der Polizei waren als Gründe neben „Schulabsentismus" u.a. auch „Gefahrenabwehr" und „Strafverfolgung" protokolliert. Während ein Abruf im ersten Fall zu Schulzeiten erforderlich sein dürfte, haben wir hinsichtlich vieler anderer Gründe die Behörde für Schule und Berufsbildung zur Prüfung und Stellungnahme aufgefordert. Frage ist hierbei, inwieweit für diese Gründe eine Erforderlichkeit – als datenschutzrechtliche Grundvoraussetzung einer jeden Daten-

Übermittlung – zum Abruf gerade aus dem Zentralen Schülerregister gegeben ist. Die Behörde teilte uns mit, dass sie ebenso einen Anlass zu einer dringenden Rücksprache mit den abrufenden Dienststellen sieht und daher Anfang 2014 Gespräche mit der Polizeidienststelle und anschließend auch mit den anderen abrufenden Dienststellen führen wird, um diese Problematik datenschutzrechtlich zu klären. Wir werden im kommenden Tätigkeitsbericht hierüber weiter informieren.

7.10 ichblickdurch.de

Die Behörde für Schule und Berufsbildung ist nach intensiver Diskussion bereit, den Vorgaben des § 11a Hamburgisches Datenschutzgesetz (HmbDSG) zu entsprechen.

Im September 2012 teilte uns die Behörde die geplante Erweiterung der bestehenden Datenbank „ichblickdurch.de" mit, so dass eine informationelle Zusammenarbeit zwischen ihr und den Anbietern von Berufsbildungsmaßnahmen in einer gemeinsamen pseudonymisierten Datei eingerichtet werden sollte. Ziel ist u.a., dass sich Anbieter auch über den bisherigen Qualifikationsstand ihrer Teilnehmer zentral informieren können und dass der Behörde als Fördergeberin weiterhin eine Datengrundlage für Plausibilitätsprüfungen zur Verfügung steht.

Nach § 11a HmbDSG bedarf die Einrichtung einer gemeinsamen Datei der ausdrücklichen Zulassung durch eine Rechtsvorschrift; allerdings sind dessen Voraussetzungen nicht erfüllbar: Pseudonymisierte Daten sind zwar personenbezogen, da sie mittels des Pseudonyms einer bestimmten Person zugeordnet werden können. § 11a HmbDSG verbietet aber eine gemeinsame Datei zwischen öffentlichen und nicht-öffentlichen Stellen, da die gesetzliche Definition der „Daten verarbeitenden Stelle" in § 4 Abs. 3 HmbDSG auf § 2 Abs. 1 Satz 1 HmbDSG verweist, der wiederum grundsätzlich nur hamburgische öffentliche Stellen umfasst. Neben weiteren ungeklärten Fragen wiesen wir insbesondere auf diesen gesetzlichen Konflikt hin.

Anschließend versuchte die Behörde durch mehrere konzeptionelle Umstrukturierungen, einen gesetzeskonformen Zustand zu erreichen; allerdings blieb der vorgenannte Gesetzeskonflikt bestehen. Auch die Rechtsgrundlage für die Datenverarbeitungen der Anbieter war unklar. In einer Besprechung Mitte 2013 haben wir der Behörde einen konzeptionellen Weg aufgezeigt, der alle Interessen berücksichtigen dürfte; dies fassten wir anschließend wie folgt zusammen: Es soll eine gemeinsame Datei allein unter den privaten Anbietern mit einer Datenbankverwaltung durch das Sekretariat für Kooperation e.V. eingerichtet werden. Neben weiteren Voraussetzungen beruht die Eintragung der Teilnehmerdaten auf einer Einwilligung:
- in die Datenerhebung an sich,
- zur Speicherung in der gemeinsamen Datei,

- in die Bereitstellung der Daten für spätere Anbieter, falls der Teilnehmer auch dort qualifiziert werden will und
- zur Erhebung bereits in der Datei vorhandener Informationen.

Jede Stufe ist freiwillig und unabhängig von der nachfolgenden Stufe. Die letzte Stufe ist erforderlich, da ein Teilnehmer zum Zeitpunkt der dritten Stufe nicht schon wirksam in die zukünftige Datenweitergabe an andere, ihm ggf. noch gar nicht bekannte Träger einwilligen kann. Der Behörde werden aus der Datei lediglich anonyme bzw. aggregierte Daten übermittelt. Derzeit ist die Behörde mit allen Beteiligten dabei, die Datenbank nach unseren Vorgaben umzusetzen.

7.11 HBSC-Kids-Studie (UKE)

Bei der Studienaufklärung ist terminologisch zwischen pseudonymer und anonymer Befragung zu unterscheiden, wobei die Grenze zwischen personenbeziehbaren und faktisch anonymen Daten ggf. schwer zu ziehen ist; auch die Freiwilligkeit der Teilnahme muss gewährleistet sein.

Das Universitätsklinikum Eppendorf (UKE) führt an Hamburger Schulen erneut eine schriftliche Befragung zur Gesundheit durch. Diese Studie ist Teil der internationalen Vergleichsstudie „Health Behaviour in School-aged Children" (HBSC). Vor deren Durchführung wurden uns die Unterlagen übersandt. Geplant war, in ganz Hamburg 1.200 Schülerinnen und Schüler zu befragen. Es sollte darüber aufgeklärt werden, dass die Datenerhebung „anonym" erfolge. Abgefragt werden sollten zur Person u.a. das Geschlecht, die Klassenstufe (5. bis 9.), die Schulform sowie Geburtsmonat und –jahr; daneben sollte z.B. auch die Frage gestellt werden, ob eine chronische Erkrankung bestehe, die auch im Freitext hätte benannt werden können.

Gemäß § 4 Abs. 9 Hamburgisches Datenschutzgesetz (HmbDSG) sind Daten dann anonym, wenn die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Verteilt man aber 1.200 Teilnehmer auf 2 Geschlechter, 5 unterschiedliche Klassenstufen, 5 verschiedene Schulformen und rechnerisch linear auf 12 Geburtsmonate, so gibt es durchschnittlich z.B. nur 2 weibliche Befragte der 9. Klasse einer Realschule, die im Juli Geburtstag haben. Hinzukommt, dass rechnerisch nur ca. 2 Schulen je Schulform teilnehmen müssten, um die Zahl von 1.200 Teilnehmern erzielen zu können. Zusammen mit den übrigen Antworten, die z.T. auch als Freitext formuliert werden können, insbesondere auch der sensiblen Frage nach chronischen Erkrankungen, ist nach unserer Auffassung der Aufwand nur minimal, die z.T. sehr sensiblen Antworten einer konkreten natürlichen Person zuzuordnen.

Auf unsere Intervention hin änderte das UKE das Studiendesign. Zum einen wurde u.a. festgelegt, dass nur zwei Schulformen in die Studie einbezogen werden und dass hierbei auch nur 3 Klassenstufen befragt werden sollen. Um eine für die Anonymität hinreichend große Anzahl von Befragten zu erreichen, wurde zum anderen entschieden, von jeder Schulform 7 Schulen einzubinden. Dadurch sind rechnerisch nicht nur 2 Kinder in einer aus den Angaben zur Person zu bildenden Gruppe, sondern datenschutzkonform eine ausreichende Mindestanzahl. Da aber bei den international vorgegebenen Fragen immer noch eine Re-Identifizierung denkbar ist, wurde in der Aufklärung der Schülerinnen und Schüler bzw. deren Eltern der Hinweis aufgenommen, dass durch bestimmte Antwortkonstellationen eine Identifizierung möglich sein könnte. Gleichzeitig wurde auch der Hinweis auf die Freiwilligkeit der Teilnahme dahingehend ergänzt, dass es dem Befragten auch freisteht, einzelne Fragen nicht zu beantworten. Hierdurch und durch weitere Maßnahmen kann der Datenschutz auch bei dieser Studie gewahrt werden.

7.12 Hamburger Schulinspektion

Bei der Hamburger Schulinspektion bedarf eine Videoaufzeichnung einer wirksamen Einwilligung, und auch der Mitarbeiterdatenschutz ist zu beachten.

Aufgabe der Schulinspektion ist es, durch Evaluationen den Schulen eine Unterstützung bei der Verbesserung der Qualität zu bieten. § 85 Abs. 3 Hamburgisches Schulgesetz (HmbSG) bestimmt insofern, dass die Schulinspektion die Qualität des Bildungs- und Erziehungsprozesses an staatlichen Schulen untersucht. Im Vorfeld der Durchführung der Schulinspektion übersandte uns die Behörde für Schule und Berufsbildung die Unterlagen zur Stellungnahme. Die Schulinspektion beinhaltet nicht nur eine schriftliche Befragung, sondern auch u.a. Schulbesuche – während derer der Unterricht beobachtet wird – und Interviews der Beteiligten. Der Datenschutz der Schülerinnen und Schüler wird dadurch gewahrt, dass sowohl der Fragebogen als auch ein Interview nur mit ausdrücklicher schriftlicher Einwilligung erfolgen.

Die Interviews auch der Kinder sollten zur Unterstützung und Erleichterung der Arbeit der Inspektoren aufgezeichnet werden. Aus den ursprünglichen Informationen und Einverständniserklärungen ergab sich diese Aufzeichnung unseres Erachtens jedoch nicht mit ausreichender Präzision. Wir wiesen darauf hin, dass insbesondere die Fragen der Zugriffsberechtigungen, der Aufbewahrung und der Löschung dieser Videoaufzeichnungen zu thematisieren sind, damit die diesbezüglichen Einwilligungen auch wirksam sind.

Im Rahmen des Fragebogens für die Lehrkräfte sollten ursprünglich auch Fragen zur Schulleitung bzw. konkret zum Schulleiter/zur Schulleiterin gestellt werden. Soweit das Gremium „Schulleitung" aber nicht mindestens aus 3 Personen besteht, dürfte

eine Zuordnung der Antworten zu konkreten Personen leicht möglich sein; ohne weiteres gilt dies bei Fragen konkret zum Schulleiter/zur Schulleiterin. Daher sahen wir in diesem Fragenteil eine personenbezogene Datenerhebung. Es gibt zwar innerhalb der Hamburger Verwaltung das Gesprächsinstrument „Führungsfeedback"; dieses betrifft aber die Gesprächssituation direkt zwischen Vorgesetztem und Mitarbeiter. Für eine Mitarbeiterbefragung haben wir eine Empfehlung herausgegeben, in der es unter Ziffer 5.b. heißt:

„Auch Art und Inhalt der Fragestellungen können das Recht der Mitarbeiterinnen und Mitarbeiter auf informationelle Selbstbestimmung unzulässig einschränken. ... Problematisch können insbesondere folgende Komplexe sein: ... die Einschätzung von Vorgesetzten. Hierfür kommt allenfalls eine anonyme Befragung in Betracht. Außerdem müssen diejenigen, die eingeschätzt werden sollen, ohne jeden Zwang in Befragungen dieser Art einwilligen, wenn die Einschätzung personenbezogen erfolgt."

Neben einer Vielzahl weiterer Punkte haben wir die Behörde für Schule und Berufsbildung auch auf dieses Einwilligungserfordernis hingewiesen.

7.13 Kommunikation bei Schulkonflikten

An der Kommunikation im Falle von schulalltäglichen Konflikten sind viele unterschiedliche Personen mit verschiedenen Funktionen beteiligt. Wir haben ein Grundsatzpapier erstellt, in dem die Befugnisse, Daten bei den einzelnen Kommunikationsbeziehungen zu offenbaren, je nach Beteiligten differenziert betrachten werden.

Wir erhalten oft Eingaben von Eltern, die unterschiedliche Sachverhalte schildern, denen eines gemeinsam ist: Es geht um die Frage, ob personenbezogene Daten weitergegeben werden dürfen. Beteiligt an diesen Sachverhalten sind aber nicht nur die Lehrerinnen und Lehrer einerseits sowie die Schülerinnen und Schüler bzw. deren Eltern andererseits. Ebenso haben die Teilnehmer der verschiedenen Konferenzen, die Klasseneltemvertreter und die Elternratsvertreter jeweils in ihrer Funktion als Gremienvertreter sowie die Behörde für Schule und Berufsbildung im Rahmen ihrer Aufgaben datenschutzrechtliche Vorschriften zu beachten.

Aus diesem Anlass haben wir ein Grundsatzpapier erstellt, in dem die grundlegenden Kommunikationsbeziehungen datenschutzrechtlich betrachtet werden. Dabei sind als bereichsspezifische Normen das Hamburgische Schulgesetz (HmbSG) sowie die Verordnung über die Verarbeitung personenbezogener Daten im Schulwesen (Schul-Datenschutzverordnung), subsidiär aber auch das Hamburgische Datenschutzgesetz (HmbDSG) einschlägig.

Eine konfliktbasierte Kommunikation beginnt dabei nicht selten mit einer Beschwerde durch Eltern. Dies ist datenschutzrechtlich nicht bedenklich, da die Sorgeberechtigten nicht als Daten verarbeitende Stellen zu beurteilen sind; ihre Kommunikation ist als persönliche oder familiäre Tätigkeit im Sinne des § 1 Abs. 2 Nr. 3 Bundesdatenschutzgesetz (BDSG) zu bewerten, die nicht dem Datenschutz unterliegt. Grenzen ergeben sich jedoch dennoch in strafrechtlicher (z.B. üble Nachrede) oder zivilrechtlicher Hinsicht (Schadensersatz wegen Persönlichkeitsverletzung). Gleiches gilt für ein informelles Treffen der Eltern, um über Probleme auch personenbezogen zu diskutieren.

Die Schulleitung hat aufgrund einer Beschwerde zunächst die Möglichkeit, mit den betroffenen Eltern ein individuelles Gespräch zu suchen. Aus praktischer Sicht kommt auch ein „runder Tisch" zur Problemlösung in Betracht. Da die personenbezogenen Daten der betroffenen Eltern bzw. deren Kindes dem informationellen Selbstbestimmungsrecht unterliegen, ist ohne deren Zustimmung die Schulleitung nicht zu einem solchen Vorgehen berechtigt. Gegen oder ohne den Willen der Eltern bzw. deren Kindes ist eine Konfliktdiskussion auf Elternabenden ebenso unzulässig. Da die staatlichen Stellen auch für die Datenerhebung eine rechtliche Grundlage benötigen, dürfen deren Vertreter grundsätzlich ohne Zustimmung der betroffenen Personen auch in informellen Treffen keine Daten aufnehmen.

8. Forschung

8.1 Überblick über beratene Forschungsprojekte

Ein Arbeitsschwerpunkt unserer Dienststelle ist auch weiterhin die datenschutzrechtliche Betreuung von Forschungsprojekten. Der Aufwand nimmt dabei jedoch kontinuierlich zu, unter anderem da zum einen die Forschungsprojekte nationale und zum Teil auch internationale Ausmaße annehmen und zum anderen zunehmend auch Forschungsvorhaben außerhalb des medizinischen Bereiches vorgelegt werden.

Bisher meldeten sich forschende Institutionen bei uns mit der Bitte um datenschutzrechtliche Betreuung vorwiegend dann, wenn die Ethikkommission hierzu Anlass sah; mittlerweile treten Forscher auch immer häufiger an uns heran, um bereits im Vorfeld eines Antrages bei der Ethikkommission die datenschutzrechtlichen Aspekte absichern zu lassen. Kernpunkt ist dabei immer auch der *informed consent*; nur auf Grundlage einer umfassenden Aufklärung und einer hierauf beruhenden freiwilligen Einwilligungserklärung des Studienteilnehmers kann wirksam die Verarbeitung seiner Daten vorgenommen werden.

Oftmals müssen wir bei unseren Prüfungen feststellen, dass der Umfang der Datenverarbeitung unverhältnismäßig ist. Wir sehen anhand der Forschungsunterlagen, dass gerade im Bereich von personenbezogenen Forschungsvorhaben dem Grundrecht auf informationelle Selbstbestimmung die ebenfalls mit Verfassungsrang ausgestattete Wissenschafts- und Forschungsfreiheit gegenübersteht. Hier ist ein Ausgleich dieser zum Teil entgegenstehenden Interessen im Sinne einer praktischen Konkordanz erforderlich. So ist es immer wieder notwendig, daran zu erinnern, dass personenbezogene Daten auch zu löschen oder zu anonymisieren sind; die Fristen hierfür müssen dann individuell gefunden werden. Gerade hierzu gibt es neuere deutschlandweite Bestrebungen von Seiten der Wissenschaftler, die Aufbewahrungsfrist von personenbezogenen Daten grundsätzlich auf zehn Jahre festzusetzen. Wir sind jedoch der Meinung, dass eine solche generelle Festsetzung dem Schutz des informationellen Selbstbestimmungsrechtes nicht gerecht wird. Wie es auch im Hamburgischen Krankenhausgesetz (HmbKHG) niedergeschrieben ist, muss die Zuordnungsmöglichkeit zu einer bestimmbaren Person aufgehoben werden, sobald der Forschungszweck es erlaubt, spätestens mit Beendigung des Forschungsvorhabens. Maßstab ist somit der konkrete „Forschungszweck"; hieran muss sich auch die Aufbewahrungsfrist orientieren. Für diejenigen Fälle, in denen eine Kontrolle der guten wissenschaftlichen Praxis erforderlich ist, bietet das HmbKHG ebenfalls eine Regelung an, die eine personenbeziehbare Speicherung über das Ende des Vorhabens hinaus für Zwecke der internen Wissenschaftskontrolle zulässt, aber gleichzeitig eine pseudonymisierte Form vorschreibt und die zeitliche Grenze bei einem Zeitraum von bis zu zehn Jahren zieht.

Im Sommer 2011 kam es vor allem in Norddeutschland zu dem Ausbruch von EHEC. Da es sich weltweit um einen der größten Ausbrüche handelte, bietet er eine valide Grundlage für wissenschaftliche Forschungen. Nicht nur die norddeutschen Universitätsklinika, sondern auch das Robert-Koch-Institut sind hieran sehr interessiert. Zu Beginn des seinerzeitigen Ausbruches stand die Behandlung der Betroffenen im Vordergrund. Datenschutzrechtliche Belange, insbesondere die Voraussicht auf mögliche spätere Forschungsvorhaben, blieben in dieser „hektischen" Anfangsphase unberücksichtigt. Nunmehr sind wir in die Prüfung einbezogen worden, wie die vorhandenen Behandlungsdaten zu Forschungszwecken genutzt werden können. Im November 2013 hatten wir hierzu ein konstruktives Gespräch mit dem UKE, in dem die weitere datenschutzkonforme Vorgehensweise festgelegt wurde. So kann das UKE auch zweieinhalb Jahre nach Ausbruch der Krankheit den wissenschaftlichen Interessen gerecht werden.

Auch das Krankheitsbild HIV ist weiterhin intensiver Forschungsgegenstand. Um diese Erkrankung sowie deren Behandlung weiter zu erforschen, werden auch in Hamburg umfangreiche Studien initiiert, die vor allem im Hinblick auf den ggf. langandauernden Krankheitsverlauf auf viele Jahre ausgelegt sind. Entscheidend ist hierbei, dass die Vertraulichkeit der personenbezogenen Daten gesichert ist. Würden diese Daten unbefugt bekannt werden, führte dies zu einer erheblichen Beeinträchtigung jedenfalls der gesellschaftlichen Stellung der Betroffenen. Über ihn würden zusammengeführte

Gesundheitsinformationen bekannt werden, die das gesellschaftliche Ansehen stark beschädigen können. Neben der Erforderlichkeit, über Jahre hinweg neue Daten einem bestimmten Probanden zuordnen zu können, lag unser Fokus auch gerade auf diesem Sicherheitsaspekt.

Auch die Klinische Psychologie der Universität haben wir in diesem Zusammenhang beraten. So unterscheidet sich schon allein der Aufbau solcher Studien von denen einer medizinischen Beobachtungsstudie. Die Befragung unter Nutzung von Telekommunikationseinrichtungen ist einer der bevorzugten Wege zur Datenerhebung. Hierbei muss jedoch – soweit es sich um personenbezogene Daten handelt – sehr genau darauf geachtet werden, dass die Studienteilnehmer sich freiwillig und vor allem auch bewusst für die Teilnahme entscheiden können. Die Sicherstellung dieser Anforderungen an eine wirksame Einwilligung und die gemeinsame Erarbeitung einer Vorgehensweise gehörten ebenfalls zu unseren Aufgaben innerhalb des Berichtszeitraumes.

Wie bereits unter III 7.10 dargestellt wurde, finden Forschungsprojekte auch in anderen Zusammenhängen statt. Zu den datenschutzrechtlichen Problemen dieser internationalen Vergleichsstudie „Health Behaviour in School-aged Children" (HBSC) und der – angesichts des geplanten Studienumfanges berechtigten – Frage nach dem tatsächlichen Vorliegen einer „anonymen" Befragung verweisen wir auf den Beitrag unter III 7.10. Dies ist aber nur ein Beispiel dafür, dass gerade die Unterscheidung zwischen pseudonymisierten und anonymen Daten für die Anwender schwer nachzuvollziehen ist, für den Datenschutz aber eine der wesentlichen Differenzierungen darstellt, an die sich unterschiedliche Anforderungen anschließen.

9. Bauen, Wohnen, Umwelt

9.1 Luftbilder: Vereinbarung mit dem Landesbetrieb Geoinformation und Vermessung

Um die Probleme des Personenbezugs bei Luftbildern zu entschärfen, einigten wir uns mit dem Landesbetrieb Geoinformation und Vermessung (LGV) darauf, dass digitale Luftaufnahmen mit einer Pixelgröße von mindestens 20x20cm Bodenfläche grundsätzlich übermittelt und veröffentlicht werden dürfen.

Von Oktober 2010 bis Anfang 2012 hatten wir in einer Arbeitsgruppe mit dem LGV und der Rechtsabteilung der Stadtentwicklungsbehörde verschiedene datenschutzrechtliche Fragen der Geobasisdaten, der Vertriebswege zu ihrer Verbreitung, des Baulastenverzeichnisses und der Kaufpreissammlung sowie des Personenbezugs von Luftbildaufnahmen erörtert.

Zu letzterem hatten die Datenschutzbeauftragten vertreten, dass digitale Orthofotos (standardisierte Luftbilder, DOP) erst ab einer Pixelgröße von 40x40 cm (1 Pixel repräsentiert eine reale Bodenfläche von 40x40 cm) als nicht personenbezogen gelten und damit auch im Internet veröffentlicht werden können. Die bundesweite Praxis der Vermessungsbehörden und privaten Luftbildanbieter wich jedoch erheblich davon ab. Es wurden Luftbilder bis zu einer Genauigkeit von 10x10cm Pixelgröße vertrieben, ohne dass datenschutzrechtliche Beschränkungen berücksichtigt wurden.

Vor diesem Hintergrund haben wir die verschiedenen Bildschärfen von Orthofotos miteinander verglichen und daraufhin überprüft, ob auf ihnen Personen, Kfz-Kennzeichen oder Kfz-Modelle zu identifizieren sind. Dabei kamen wir zu der Überzeugung, dass grundsätzlich auch eine Veröffentlichung von DOP 20 (Digitale Orthofotos mit einer Pixelgröße von 20x20cm Bodenfläche) zu vertreten ist. Diese Auffassung haben wir in den Bund-Länder-Arbeitskreis Geodaten eingebracht und dort eine mehrheitliche Zustimmung erfahren.

In einer Vereinbarung mit dem LGV kamen wir danach überein, dass bereits bei DOP 20 mangels Identifizierungsmöglichkeit grundsätzlich keine „öffentlichen oder privaten Belange einer Übermittlung an jedermann entgegenstehen" (§ 10 Abs.3 Hamburgisches Vermessungsgesetz). Allerdings kann eine betroffene Person im Ausnahmefall – z.B. bei der Abbildung eines Krankenbettes in seinem hinteren Garten – eine Löschung dieser Bilddaten verlangen. DOP 10, also schärfere, detailliertere Luftbildaufnahmen, dürfen dagegen nur offline als Papierabzüge an die betroffenen Eigentümer und an andere Dienststellen der FHH abgegeben werden. Auch hier können Betroffene wegen ganz besonderer persönlicher Umstände eine Löschung von Bildausschnitten vor Weitergabe an andere Dienststellen verlangen.

Wir sind uns darüber im Klaren, dass diese Vereinbarung das Problem des Personenbezuges von Geodaten nicht löst. Angesichts der drängenden Praxisbedürfnisse wollten wir uns einer pragmatischen und für die öffentlichen Stellen handhabbaren Lösung jedoch nicht verschließen.

9.2 Kamerafahrten durch Hamburgs Straßen

Die Befahrung einiger Straßenzüge mit Kamera-Fahrzeugen am 7. März 2013 hat in der Bevölkerung einige Verunsicherung verursacht. Die Aufnahmen dienten einer technischen Machbarkeitsprüfung und sollten nicht veröffentlicht werden.

Durch Anfragen bei uns und durch Kleine Anfragen an den Senat wurden wir darauf aufmerksam gemacht, dass der Landesbetrieb für Geoinformation und Vermessung (LGV) Fahrten mit Kamerawagen in einigen Straßen der Stadt durchgeführt haben sollte. Unsere Recherchen haben dann ergeben, dass ein privater Auftragnehmer des LGV

(bzw. dessen Subunternehmer) am 7. März 2013 ca. 25 km Straßen im Hamburger Stadtgebiet abgefahren und 360° Panoramaaufnahmen angefertigt hatte.

Hintergrund war der Wunsch des LGV, ein Verfahren entwickeln zu lassen, mit dem sich 360° Panoramabilder aus der Fußgängerperspektive auf 3D-Gebäudemodelle übertragen lassen (sog. automatisierte Texturierung). Insofern ging es um die Klärung der technischen Machbarkeit. Dafür wurde der Firma virtualcitySystems GmbH aus Berlin im Rahmen eines größeren Gesamtauftrags ein optionaler Projektauftrag erteilt, ein Verfahren zur automatisierten Texturierung zu entwickeln. Die Aufnahmen bis hin zur Unkenntlichmachung von Gesichtern und Autokennzeichen wurden durch die Firma CycloMedia Deutschland GmbH als Subunternehmerin der Firma virtualcitySystems durchgeführt. Nach den Vertragsunterlagen und nach dem tatsächlichen Ablauf gehen wir davon aus, dass die Firma virtualcitySystems nicht als Auftragsdatenverarbeiter im Sinne des § 3 Hamburgisches Datenschutzgesetz (HmbDSG) für den LGV tätig wurde, sondern den Auftrag selbstständig und eigenverantwortlich durchführte.

Wir kamen zu dem Schluss, dass kein datenschutzrechtlicher Verstoß vorliegt. Zu den Aufgaben des LGV gehört es u. a., ein einheitliches geodätisches Bezugssystem einzurichten und vorzuhalten, § 1 Abs. 2 Hamburgisches Vermessungsgesetz (HmbVermG). Auch im Rahmen des Hamburgischen Geodateninfrastrukturgesetzes (HmbGDIG) hat der LGV die Aufgabe, am Ausbau und Betrieb der nationalen Geodateninfrastruktur mitzuwirken. Dazu gehört es nach unserer Rechtsauffassung auch, neue Darstellungssysteme zu entwickeln, etwa ein automatisiertes Texturierungsverfahren.

Anhaltspunkte für einen Verstoß der beauftragten Berliner Firma gegen das Bundesdatenschutzgesetz ergaben sich nach unserem ausführlichen Gespräch mit dem LGV und Einsicht in die Vertragsunterlagen nicht, so dass wir es nicht für erforderlich hielten, den Berliner Beauftragten für Datenschutz und Informationsfreiheit einzuschalten. Dem LGV wurden vom Auftragnehmer nur die Ergebnisse der Texturierungsversuche überlassen, in denen Personen und Kennzeichen nicht erkennbar waren. Dies sehen wir im Einklang mit § 13 HmbDSG und den Grundsätzen der Datensparsamkeit und der Verhältnismäßigkeit. Da das Ergebnis des Versuchs sich aus Sicht des LGV nicht für die Darstellung von 3 D-Gebäudemodellen eignete, wurden vom Auftragnehmer keine weiteren Daten an den LGV herausgegeben und die Firma virtualcitySystems sollte nach Abschluss des Auftrags die erhobenen Daten löschen.

Unbefriedigend bleibt letztlich, dass die Straßenbefahrung mit Kamerawagen offenbar einige Menschen beunruhigt hat. Sicher wird dies Erinnerungen an die Straßenaufnahmen von Google Street View geweckt haben. Für die Bürgerinnen und Bürger, die von den Aufnahmen betroffen waren, war nicht erkennbar, dass die Bilddaten zunächst nur zu Testzwecken erhoben wurden und nicht der Veröffentlichung dienten. Eine Pflicht zur Benachrichtigung besteht wegen der Vielzahl und mangels Identifizierbarkeit der Betroffenen nach dem Gesetz nicht; dennoch empfehlen wir,

nach Möglichkeit geeignete Verfahren zur Vorab-Information, z. B. über die Presse, zu suchen.

10. Finanzwesen

10.1 Kultur- und Tourismustaxe

Wir haben frühzeitig darauf hingewiesen, dass der Hotelgast, der nicht der Steuerschuldner ist, nicht verpflichtet werden kann, dem Hotelier Auskunft zum privaten oder beruflichen Anlass seiner Übernachtung zu erteilen.

Bereits im Jahr 2010 hatte die Kulturbehörde einen Gesetzentwurf für eine Kulturtaxe erarbeitet. Er machte den Hotelgast zum Steuerschuldner und verpflichtete ihn, gegebenenfalls die berufliche Veranlassung der Übernachtung nachzuweisen, die ihn von der Steuerlast befreite.

Im Mai 2012 legten die Wirtschafts-, Finanz- und Kulturbehörde einen neuen Gesetzentwurf vor. Dieser sah den Hotelier als Steuerschuldner vor und verzichtete auf eine Unterscheidung in private und berufliche Übernachtungsanlässe. Damit erübrigte sich auch eine Auskunftspflicht des Gastes. Wir stimmten diesem Gesetzentwurf zu.

Nach Gerichtsurteilen, die eine „Bettensteuer" bei beruflichem Übernachtungsanlass für unzulässig erklärten, wurde die Unterscheidung nach dem Anlass der Übernachtung in den Ausschussberatungen wieder in das Gesetz aufgenommen. Es blieb jedoch dabei, dass die Steuerpflicht den Hotelier trifft und der Gast damit nicht zu einer Auskunft verpflichtet werden kann. Er haftet jedoch für die entgangene Steuer, wenn er falsche Auskünfte bzw. Nachweise für einen beruflichen Übernachtungsanlass abgegeben hat.

Die fehlende Auskunftspflicht des Gastes haben wir nicht nur im Rahmen der Behördenabstimmung zum Gesetzentwurf deutlich gemacht, sondern auch in Stellungnahmen auf Anfragen des Hotel- und Gaststättenverbandes, des Bundes der Steuerzahler und der Presse. Wir vertraten ferner die Auffassung, dass der Gast auf die Freiwilligkeit einer Mitteilung über den Übernachtungsanlass hingewiesen werden muss, dass der Hotelier den Gast aber – mit diesem Hinweis – fragen darf. Denn von der Antwort hängt seine Steuerlast ab. Diesen für den Hotelier unbefriedigenden Konstruktionsfehler des Gesetzes kann er allerdings umgehen, wenn er seine Übernachtungspreise generell entsprechend anhebt und auf alle Übernachtungen – unabhängig vom Übernachtungsanlass – die Kulturtaxe abführt. Auch die gesetzlichen Aufzeichnungs-, Aufbewahrungs- und Meldepflichten können den Hotelier nicht zwingen, die Gäste über ihren Übernachtungsanlass zu befragen.

Abgelehnt haben wir einen einheitlichen Meldeschein, der sowohl die polizeiliche Anmeldepflicht des Gastes nach § 26 HmbMeldeG als auch die freiwillige Angabe über den Übernachtungsanlass nach dem Kultur- und Tourismustaxengesetz abdecken sollte. Sowohl die Zwecke als auch die Inhalte, Datenempfänger und Aufbewahrungsfristen sind für beide Datenoffenbarungen nach den Gesetzen unterschiedlich. So ist es z.B. nicht erforderlich und damit unzulässig, dass die Polizei mit der Meldung nach § 26 HmbMeldeG dann auch den Anlass für die Übernachtung erführe.

Den weiteren Verlauf der politischen und gerichtlichen Auseinandersetzungen über die Hamburger Kultur- und Tourismustaxe werden wir aus Datenschutzsicht aufmerksam verfolgen.

10.2 Ein Korruptionsregister zum Schutz des fairen Wettbewerbs

Mit dem Gesetz zur Einrichtung eines Registers zum Schutz fairen Wettbewerbs (GRfW) wurde eine Rechtsgrundlage für die Einrichtung einer zentralen Informationsstelle geschaffen, die Daten über unzuverlässige Unternehmen speichern darf, die von der Vergabe öffentlicher Aufträge ausgeschlossen werden sollen. Vor dem Abschluss eines Verwaltungsabkommens mit Schleswig-Holstein über den Betrieb eines gemeinsamen Registers steht eine vollständige Dokumentation der technisch-organisatorischen Maßnahmen und abschließende Beurteilung durch den HmbBfDI.

Am 12. September 2013 beschloss die Bürgerschaft das GRfW, das als Drucksache 20/7202 noch unter dem Titel „Hamburgisches Korruptionsregistergesetz (HmbKorrRegG)" auf den Weg gebracht worden war. Das Gesetz wurde am 1. Oktober 2013 verkündet und trat am 1. Dezember 2013 in Kraft. Ein Korruptionsregister hatte es in den Jahren 2004 bis 2006 schon in Hamburg gegeben; allerdings waren damals keine Eintragungen erfolgt (siehe BüDrs. 20/148 vom 12. April 2011).

Im Jahr 2011 hatte der Senat einen Anlauf unternommen, erneut ein Korruptionsregister zu schaffen. Damit sollten Unternehmen sowie natürliche und juristische Personen, die bestimmte wirtschaftliche Verfehlungen (z. B. Steuerhinterziehungen, Preisabsprachen) begangen hatten, von der Vergabe öffentlicher Aufträge ausgeschlossen werden.

Ein erster Entwurf war im November 2011 in die Behördenabstimmung gegangen, nachdem die Erwartung, dass es auf Bundesebene ein bundesweit geltendes, einheitliches Register für unzuverlässige Auftragnehmer geben würde, sich nicht erfüllt hatte. Auch ein einheitliches Vorgehen der norddeutschen Bundesländer war zu dem Zeitpunkt nicht zu erwarten.

Wir hatten zu einem Entwurf von Ende 2011 bereits Stellung genommen, ebenso wie zu einem geänderten Gesetzentwurf im Februar 2012 und im Juli 2012. Der Gesetzentwurf wurde dann jedoch ausgesetzt, weil mit Schleswig-Holstein über ein gemeinsames Korruptionsregister verhandelt wurde. Schließlich erfolgte dann im Februar 2013, nachdem man sich auf ministerialer Ebene mit Schleswig-Holstein auf übereinstimmende landesgesetzliche Regelungsentwürfe verständigt hatte, erneut ein Abstimmungsverfahren, in dessen Rahmen wir erneut Stellung nahmen.

Positiv ist aus unserer Sicht, dass es nun ein gemeinsames Register geben soll, an dem Hamburg und Schleswig-Holstein beteiligt sind, und das weiteren Bundesländern offen stehen soll. Denn bei einem Alleingang eines Bundeslandes würden Zweifel bestehen, ob die Regelung mit dem verfassungsrechtlichen Gleichheitsgrundsatz vereinbar ist, wenn keine allgemeine Meldepflicht für alle bundesweit tätigen Unternehmen besteht.

Wir sehen in datenschutzrechtlicher Hinsicht die Wirkung einer Eintragung in das Korruptionsregister als einen besonders tiefen Eingriff in die Rechte Betroffener an, da sie diese in ihrer wirtschaftlichen Existenz bedrohen kann – zumal die zentrale Informationsstelle Vergabesperren aussprechen kann. Viele Änderungsvorschläge und Anregungen aus unseren Stellungnahmen fanden Berücksichtigung.

Einige Anregungen blieben leider unberücksichtigt. Für erläuterungsbedürftig hielten wir den Begriff der „schweren Verfehlung" (§ 2 Abs. 2 Satz 1 GRfW), die zu einem Registereintrag führen soll. Kritisiert hatten wir im Hinblick auf den schwerwiegenden Eingriff durch eine Eintragung die Möglichkeit einer Aufnahme in das Korruptionsregister anhand „weicher" Daten (§ 2 Abs.2 Satz 2 Nr. 4 GRfW „vergleichbar schwere Verfehlungen, insbesondere vorsätzliche oder grob fahrlässige Falscherklärungen ...") und hatten gefordert, dass es einen abschließenden Katalog von Verfehlungen im Gesetz geben müsse, die zu einer Eintragung führen können. Problematisch ist wegen der Schwere des Eingriffs durch eine Eintragung unserer Meinung nach auch, dass eine „schwere Verfehlung" selbst dann als nachgewiesen gilt, wenn im Falle staatsanwaltschaftlicher Ermittlungen gegen Betroffene eine endgültigen Einstellung des Verfahrens gemäß § 153a Strafprozessordnung (StPO) mangels öffentlichen Interesses erfolgt (§ 2 Abs. 3 GRfW). Kritisch mit Blick auf die rechtsstaatliche Unschuldsvermutung sehen wir zudem, dass im Einzelfall vor einer rechtskräftigen Verurteilung bzw. vor rechtskräftigem Bußgeldbescheid eine Registereintragung möglich sein soll. Wir haben uns vergeblich dafür eingesetzt, dass Speicherfristen maximal denen in Bundesregistern entsprechen und Löschungen sofort erfolgen, wenn die Tilgung im Register erfolgt.

Auf unser Betreiben wurde in § 10 GRfW die Vorschrift über ein gemeinsames Register so gefasst, dass die Vorschriften anderer teilnehmender Länder über die Art der aufzunehmenden und abzurufenden Daten, den Zweck des Abrufs und die Vorschriften über

Aufnahme in das und Löschung aus dem Register mit dem GRfW übereinstimmen müssen und im Verwaltungsabkommen die technisch-organisatorischen Maßnahmen und die Datenschutzkontrolle näher geregelt sein müssen. Wichtige datenschutzrechtliche Unterlagen wurden erst im November 2013 geliefert. Ob die Risiken für die verarbeiteten Daten auf ein vertretbares Maß reduziert werden, kann der HmbBfDI erst dann einschätzen, wenn eine vollständige Darlegung der umzusetzenden technischen und organisatorischen Maßnahmen erfolgt ist. Diese müssen dem hohen Schutzbedarf der Daten gerecht werden.

Im Laufe der Abstimmungsverfahren hatten wir zunächst eine Klarstellung in § 10 GRfW gefordert, welcher Landesdatenschutzbeauftragte für die Kontrolle des gemeinsamen Registers zuständig sei. Letztlich hat das GRfW eine Regelung (gemeinsames Register bei einer Landesbehörde, aber getrennte landeseigene zentrale Informationsstellen) vorgesehen, die diese Festlegung überflüssig gemacht hätte. Deshalb hatten wir, wie auch die Behörde für Justiz und Gleichstellung, diese Bestimmung in § 10 Abs. 5 Satz 1 und 2 GRfW als obsolet angesehen; dies wurde jedoch am Ende des Abstimmungsverfahrens leider nicht mehr geändert. Letztlich halten wir die Regelung für unschädlich; die Umsetzung wird sich in der Praxis einspielen.

10.3 VoSystem zur Organisation der Vollstreckung in der Steuerverwaltung

Durch die Einführung des automatisierten Datenverarbeitungssystems VoSystem soll die Arbeit in den Vollstreckungsdienststellen der Steuerverwaltung erleichtert und beschleunigt werden. Ob das IT-Verfahren, das in Kooperation mit Dataport und Schleswig-Holstein durchgeführt werden soll, den datenschutzrechtlichen Anforderungen genügt, lässt sich derzeit noch nicht abschließend beurteilen, weil uns die notwendigen Unterlagen noch nicht vorliegen.

Anfang 2013 wurden wir von der Steuerverwaltung darüber in Kenntnis gesetzt, dass die Bearbeitung von Vollstreckungsfällen in der Steuerverwaltung zukünftig automatisiert werden solle. Im Programmierverbund „KONSENS" steht das auf der Grundlage des § 20 Abs. 2 Finanzverwaltungsgesetz (FVG) eingerichtete VoSystem seit 2006 allen Bundesländern zur Verfügung und wird bislang in den Finanzämtern in Bayern, Brandenburg, Bremen, Mecklenburg-Vorpommern, Nordrhein-Westfalen, Rheinland-Pfalz und Sachsen angewendet. In Hamburg wurde das Verfahren bislang nicht eingesetzt, weil Fachwissen und Personal dafür nicht vorhanden gewesen sind. Deshalb soll die Verfahrensbetreuung durch das Amt für Informationstechnik Schleswig-Holstein (AIT) erfolgen, insbesondere werden die PC-Arbeitsplätze der Anwender hinsichtlich der Einführung, Weiterentwicklung, Wartung und bei Störungen der neuen Vollstreckungs-Software und der technischen Infrastruktur unterstützt. Das VoSystem wird auf Servern bei Dataport im Data Center Steuern (DCS)

betrieben; Dataport sorgt für die Netzwerkanbindung.

Mit der Automatisierung der Vollstreckungsaufgaben sollen die Arbeitsplätze der Vollstreckungsstellen technisch unterstützt werden: Beispielsweise werden durch automatische Wiedervorlagen Zahlungs- und sonstige Fristen überwacht und systemseitig im Einzelfall Maßnahmen vorgeschlagen. VoSystem wird die erforderlichen Vordrucke zur Verfügung stellen. Alle für die Vollstreckungsfälle erforderlichen Daten werden in elektronischen Akten vorgehalten. Dies führt vor allem zu einer erheblichen Einsparung an Papier und an Zeit.

Die wesentlichen Rechtsfragen wurden bereits auf Länderebene anlässlich der Konstruktion des Verfahrens VoSystem erörtert. Datenschutzrechtlich ist vorrangig die Abgabenordnung (AO) einschlägig (§§ 30, 85, 88 und 88a), die nur wenig Raum für eine ergänzende Geltung des Hamburgischen Datenschutzgesetzes (HmbDSG) lässt. Eine Besonderheit ist, dass die hamburgische Steuerverwaltung im Wege der Auftragsdatenverarbeitung das AIT mit der Einführung und Betreuung betraut. Insofern gehen wir von der Anwendbarkeit des HmbDSG, insbesondere § 3, aus. Dies ergibt sich aus § 2 Abs. 1 Satz 1 Nr. 1 HmbDSG. Ferner sind von der Finanzbehörde nach unserer Rechtsauffassung eine Risikoanalyse gemäß § 8 Abs. 4 und eine Verfahrensbeschreibung gemäß § 9 HmbDSG anzufertigen.

Risikoanalyse und Verfahrensbeschreibung dokumentieren die Eigenschaften des Verfahrens (z.B. Berechtigungskonzept und IT-Konzept), den Schutzbedarf der Daten, die zu betrachtenden Risiken, die getroffenen technischen und organisatorischen Maßnahmen für ein tolerierbares Restrisiko, Regelungen zur Auftragsdatenverarbeitung, Test und Freigabe des Verfahrens und mehr. Ohne diese Unterlagen ist die Einschätzung, ob das Verfahren datenschutzgerecht betrieben wird, nicht zu leisten. Sie sind in diesem Fall besonders wichtig, weil es viele Mitwirkende und viel Technikeinsatz über Ländergrenzen hinweg gibt.

Wir haben die Steuerverwaltung darauf hingewiesen, dass im Falle eines hohen Schutzbedarfs der personenbezogenen Daten zusätzliche Maßnahmen geprüft werden müssten, mit denen die spezifischen Risiken des Fachverfahrens ggf. reduziert werden können. Dazu gehört auch ein Secure Service Level Agreement (SSLA, das die Finanzbehörde als datenschutzrechtlich verantwortliche Stelle anstelle des sonst üblichen SLA mit Dataport abschließen sollte. Auch ist darauf zu achten, dass das AIT, soweit es seinerseits das DCS beauftragt, ebenfalls entsprechend hohe Schutzmaßnahmen mit Dataport vereinbart.

Neben den Risiken, die mit der Auftragsdatenverarbeitung und mit dem automatisierten Verfahren an sich verbunden sind, sehen wir auch datenschutzrechtliche Vorteile in dem Verfahren. Durch eine stark am individuellen Aufgabenbereich der Vollstreckungssachbearbeiter orientierte Beschränkung der Zugriffsrechte wird vermieden,

dass Sachbearbeiter Einzelangaben aus verschiedenen Papier-Sachakten heraussuchen müssen, die auch nicht benötigte Daten enthalten. Dadurch, dass das Verfahren es ermöglicht, zukünftig Vollstreckungssachen unter der Steuernummer des Betroffenen zu führen, werden weitere Fehlerquellen, z. B. ein Versand von Angaben über dritte Steuerpflichtige aufgrund versehentlich falscher Zuordnung, vermieden.

Allerdings sind wir, nach einer Präsentationsveranstaltung Ende Februar 2013 und Beantwortung unserer im Februar gestellten Fragen im August, leider nicht über den Fortgang der technisch-organisatorischen Umsetzung informiert worden, wie es im Februar 2013 abgesprochen worden war.

Vor der beabsichtigten Pilotierung Anfang Februar 2014 – von der wir kürzlich erfuhren – müssen die o.g. Unterlagen fertig gestellt sein; daneben könnte noch ein erläuterndes Gespräch notwendig werden. Wir hoffen, dass sich dann nicht noch Änderungsbedarf aus datenschutzrechtlicher Sicht ergibt.

10.4 Technische Überwachung der Spielbank Hamburg

Technische Maßnahmen zur Überwachung der Spielbank Hamburg für Zwecke der Spiel- und Steueraufsicht dürfen nicht unverhältnismäßig in die Rechte der Besucher und der Mitarbeiter eingreifen. Sollen bestimmte Bereiche laufend überwacht werden, ist die Erforderlichkeit von Bilddaten besonders sorgfältig zu prüfen.

Über die Intentionen, die personalintensive Überwachung der Spielbank Hamburg für Zwecke der Spielaufsicht und der Steuerüberwachung durch Videoüberwachung zu entlasten, haben wir bereits berichtet (22.TB, III 15.3).
Angedacht war seinerzeit, die Überwachung der Eingangs-, Spiel-, Kassen- und Abrechnungsräume sowie der Außenbereiche bis zu zwei Stunden vor Öffnung und nach Schließung zu betreiben. Darauf sollten alle Spielzüge und alle beteiligten Personen erkennbar abgebildet sein. Dazu wollte man die vorhandene Anlage der Spielbank Hamburg nutzen, die diese für eigene Zwecke nach § 6b des Bundesdatenschutzgesetzes (BDSG) betreibt. Die Automatenprotokollierung sollte parallel dazu sämtliche Spielzüge, Einsätze und Auszahlungen der Automaten festhalten.

Wir hatten seinerzeit erhebliche Bedenken u.a. gegen eine Nutzung im Rahmen einer gemeinsamen Datei nach § 11 a des Hamburgischen Datenschutzgesetzes (HmbDSG) geäußert, in der jede beteiligte Stelle für ihre Zwecke Zugriff auf die Daten nimmt, da das HmbDSG eine solche Konstruktion nicht erlaubt.

Im Berichtszeitraum wurden mit der Finanzbehörde die rechtlichen Möglichkeiten ausgelotet, eine Videoüberwachung allein zu steuerrechtlichen Zwecken und ohne den Aufbau einer gemeinsamen Datei mit der Spielbank auszugestalten. Dabei sollte auch unnötige doppelte Kameraführung vermieden werden. Unser Vorschlag ging dahin, dass die Finanzbehörde die Datenverarbeitung für ihre Zwecke vollständig und verantwortlich betreiben solle. Soweit davon Daten auch für die Spielbank für deren Zwecke erforderlich wären, könnten diese nach den allgemeinen Übermittlungsvorschriften zur Verfügung gestellt werden.
Bei dieser Lösung wäre grundsätzlich auch eine Auftragsdatenverarbeitung in Betracht gekommen, wenn die Spielbank die Technik auf einem mandantenfähigen System zur Verfügung gestellt hätte, damit eine Vermischung der Daten ausgeschlossen wäre.

Die Finanzbehörde ist diesem Vorschlag letztlich nicht gefolgt, sondern hat sich für eine Lösung entschieden, wonach sie die abgabenrelevanten Zählvorgänge in den Abrechnungsräumen der Spielbank durch eine eigene Anlage überwacht und im Übrigen die Spielbank gesetzlich verpflichtet wird, den Spielbereich in eigener Verantwortung so detailliert aufzunehmen, dass die spielaufsichtlichen und steueraufsichtlichen Belange durch Übermittlung an die Aufsichtsbehörden abgedeckt werden. Auf diese Daten soll anlassbezogen oder im Rahmen von Stichprobenkontrollen zurückgegriffen werden können.
Daneben sollten die mittlerweile bauseits gesetzlich vorgeschriebenen Automatenprotokollierungen elektronisch zusammengeführt und im Wege des automatisierten Abrufs der Steuerverwaltung zur Verfügung gestellt werden.

Leider hatte der ursprünglich vorgelegte Entwurf dies noch nicht hinreichend widergespiegelt. Wir waren deshalb an der Formulierung der Regelungen intensiv beteiligt, um die jeweils nach Aufgaben getrennten Eingriffe in die Rechte der Betroffenen auf das erforderliche Maß zu beschränken. So dürfen an das zuständige Finanzamt für Kontrollzwecke nur die Spielzüge, nicht aber die handelnden Personen erkennbar übermittelt werden. Erst bei hinreichenden Verdachtsmomenten auf ein Vergehen oder eine Straftat dürfen diese von der zuständigen Stelle einzelfallbezogen abgefordert werden. Auch die Spielaufsicht braucht keinen jederzeitigen Zugriff auf die Daten, sondern wie bisher nur bei Anhaltspunkten für Verstöße gegen das ordnungsgemäße Spiel, die durch die Spielbank als dazu verpflichteter Stelle nicht hinreichend unterbunden wurden.

Zur Angemessenheit gehört auch, dass die an sich nicht personenbezogenen, laufend an die Steueraufsicht zu übermittelnden Automatenprotokollierungen für steuerliche Zwecke nicht anlasslos mit den Daten aus der Videoüberwachung zusammengeführt werden dürfen.
Im Verlauf des Abstimmungsverfahrens haben wir auch erreicht, dass auf die Überwachung von Kassenräumen mit Publikumsverkehr verzichtet wird.

11. Behördliche Datenschutzbeauftragte

11.1 Entwicklung

Die Entwicklung hat sich verstetigt. In einigen Bereichen stellt sich die Frage nach flankierenden Maßnahmen für die Beauftragten.

Über die Bestellung behördlicher Datenschutzbeauftragter, die Umsetzung des Konzepts Behördliche Datenschutzbeauftragte in der Kernverwaltung und die Zusammenarbeit haben wir wiederholt berichtet (21 .TB, 3; 22. TB. III 1.1; 23. TB, III 1.1)

Die Entwicklung hat sich in den einzelnen Bereichen verstetigt. Erfreulich ist, dass die Behörde für Inneres und Sport zum 01.01.2013 auch einen Beauftragten mit 100% Stellenkapazität bestellt hat. Damit haben alle Behörden der Kernverwaltung nun ihren bestellten Datenschutzbeauftragten; bei den Gerichten fehlen bisher das Sozial- und das Landessozialgericht.

In unerwartet hohem Maße gibt es Fluktuation, insbesondere bei den Gerichten. Aber auch dort, wo die Aufgaben mit einem Stellenanteil wahrgenommen werden, scheint die Aufgabe weniger der Person als der Stelle zugeordnet zu werden. Daraus resultiert zum einen ein kontinuierlicher Schulungsbedarf, zum anderen scheint so eine angemessene Betreuung der jeweiligen Stellen nur eingeschränkt möglich.

Der Vielgestaltigkeit der Bestellungen entsprechend ist auch der Eindruck der Zusammenarbeit. Insgesamt kann gesagt werden, dass die Kontakte zu den behördlichen Beauftragten umso intensiver sind, je größer der Stellenanteil der Bestellung ist. Die Mehrzahl der bestellten Beauftragten hat eine juristische Vorbildung, so dass regelmäßige Beratungsbedarfe insbesondere im technischen Bereich bestehen, was bei der gegebenen Ausstattung der Dienststelle leider zunehmend nicht mehr in jedem Fall gewährleistet werden kann. Auch fehlt in den meisten Fällen ein bestellter Vertreter, so dass bei Urlaub oder längeren Vakanzen keine Bearbeitung erfolgen kann.

Um die Bedarfe und Entwicklungen besser einschätzen zu können, beabsichtigen wir, im nächsten Berichtszeitraum eine Erhebung zu den Rahmenbedingungen in den einzelnen Stellen und den Bedürfnissen ihrer Beauftragten durchzuführen.

Auch in diesem Berichtszeitraum haben wir im Rahmen unserer Kapazitäten neben den laufenden Beratungen die jährlichen Datenschutztreffen sowie Fortbildungen zur Einführung, zum Personaldatenschutz, zur Vorabkontrolle und zu sozialen Medien durchgeführt. Anfragen zur Fortbildung in Technikfragen liegen vor.
Mit anlassbezogenen Rundschreiben haben wir u.a. auf unsere überarbeiteten Musterformulare zu Risikoanalyse und Verfahrensbeschreibung, zu den Orientierungshilfen Mandantenfähigkeit und Soziale Netzwerke und insbesondere auf die neu gefassten Erläuterungen zum Hamburgischen Datenschutzgesetz hingewiesen.

12. Verkehr

12.1 Projekt Deutschland online Kfz

Die Einschaltung privater Stellen bei der KFZ-Ummeldung begegnet letztlich keinen datenschutzrechtlichen Bedenken, da der ermessensweise anzufordernde Nachweis einzelner registerrelevanter Daten keinen Identitätsnachweis beinhaltet und daher die KFZ-Zulassung nicht notwendig von der Sichtprüfung des Personalausweises abhängig gemacht werden muss.

Das Projekt hatten wir schon im letzten Bericht behandelt (23. TB III 14.3). Dabei geht es um die Möglichkeit, auf der Grundlage des geltenden Rechts online-unterstützt KFZ-Ummeldungen zu erleichtern. Schon frühzeitig hatten wir mit dem Landesbetrieb Verkehr (LBV) die Einbindung privater Stellen bei der Aushändigung der Unterlagen und Kennzeichen sowie der Einziehung alter Dokumente und Kennzeichen diskutiert und waren uns zunächst einig, dass dies aufgrund des ermessensweise, aber ausnahmslos geforderten Identitätsnachweises durch Vorlage des Personalausweises problematisch sei.

Nach der mit den Datenschutzbeauftragten des Bundes und der Länder abgestimmten Auslegung der Auftragsdatenverarbeitung sind nur technische Unterstützungsleistungen von der Regelung umfasst. Die Betrauung mit (Teil-) Aufgaben, die eine Ermessensentscheidung erfordern, bedürfen einer Funktionsübertragung im Wege der Beleihung. Die Auftragsdatenverarbeitung ist somit der Spezialfall einer Verwaltungshelferschaft mit Verarbeitung personenbezogener Daten.
Bis auf die regelmäßige Prüfung des Personalausweises waren die erforderlichen Tätigkeiten unstreitig im Wege der Verwaltungshelferschaft als rein technische Ablaufunterstützung des LBV einzuordnen. Mit der Sichtprüfung eines Ausweises und der Entscheidung, ob die Identität nachgewiesen ist oder nicht, wird regelmäßig ein Beurteilungsermessen ausgeübt. Dies gilt auch im positiven Fall.

Wir haben unsere Bedenken nach Produktivsetzung des Pilotprojekts letztlich zurückgestellt aufgrund folgender Überlegungen:
Wenn auch der LBV bisher ausnahmslos die Vorlage von Ausweisen sowohl der Halter als auch etwaiger Bevollmächtigter verlangt, um die Aushändigung der Zulassung tatsächlich nur an den, den es angeht, zu bewirken, ist eine Gleichbehandlung aller KFZ-Zulassungen weder rechtlich noch aus Datenschutzgründen erforderlich.
§ 6 Abs. 1 Satz 1 der Fahrzeugzulassungsverordnung (FZV) bestimmt lediglich, welche Halterdaten zur Speicherung im Fahrzeugregister angegeben und auf Verlangen nachgewiesen werden müssen (Familienname, Geburtsname, Vorname, Ordens- oder Künstlername, Datum und Ort der Geburt, Geschlecht und Anschrift des Halters), er verlangt aber keinen Identitätsnachweis.

Der Nachweis der Daten liegt somit sowohl im Entschließungs- als auch im Auswahlermessen des LBV. Dies geschah bisher zwar typischerweise und sehr umfänglich durch Vorlage des Personalausweises oder einer sonstigen Identifikationsurkunde. Zu Dokumentationszwecken wurden z.B. Ausweise von Bevollmächtigten nicht nur eingesehen, sondern auch in Kopie zum Vorgang genommen. Diese Art der Ermessensausübung beinhaltet aber weder eine Ermessensbindung dergestalt, dass der Nachweis immer durch die Vorlagen eines Ausweises erfolgen muss, noch dass damit alle für einen Identitätsnachweis zu überprüfenden Daten zweifelsfrei festgestellt werden müssten.
So sind nach § 6 Abs. 1 FEV weder der Nachweis eines Lichtbildes nach § 6 Abs. 1 FEV noch der Unterschrift erforderlich. Auch ist für den Antrag Schriftform gesetzlich nicht vorgeschrieben.

Angesichts der bei der Ummeldung ohnehin vorzulegenden alten Fahrzeugpapiere und der bestehenden und regelmäßig vom LBV genutzten Möglichkeit, die aktuelle Meldeadresse durch einen Melderegisterabgleich schon bei der Vorbereitung der Zulassung zu verifizieren, kommt der Vorlage des Ausweises keine rechtsgestaltende Wirkung dergestalt zu, dass erst nach erfolgreichem Identitätsnachweis die Zulassungspapiere ausgehändigt und die Zulassung damit rechtlich bekannt gegeben wird. Auf eine ermessensweise Entscheidung, ob Lichtbild und Unterschrift die des Fahrzeughalters sind, kommt es daher rechtlich nicht an. Vielmehr reicht es aus, dass sich aus der Gesamtschau der Umstände mit hinreichender Sicherheit darauf schließen lässt, dass Papiere und Kennzeichen an den richtigen Antragsteller ausgehändigt werden.

Leider hat es in diesem Zusammenhang eine weniger erfreuliche Entwicklung in der bisher guten Zusammenarbeit mit dem LBV gegeben:

Nach Redaktionsschluss des 23. TB erreichte uns die Mitteilung, dass die Einschaltung privater Stellen gutachtlich geprüft werden solle. Unserer Bitte unter Hinweis auf § 23 Absatz 5 des Hamburgischen Datenschutzgesetzes (HmbDSG), uns das Gutachten vor Produktivsetzung zur weiteren Prüfung zukommen zu lassen, ist der LBV nicht nachgekommen. Vielmehr wurde angekündigt, dass das Thema auch Gegenstand einer anstehenden Veröffentlichung des Gutachters sein solle. Im April 2012 ging das Projekt in Echtbetrieb. Erst im August 2013 wurde uns das Gutachten nach Androhung einer Beanstandung übermittelt. Ausdrücklich wurde darauf hingewiesen, dass man unsere Rechtsauffassung zu § 23 Absatz 5 HmbDSG nicht teile, da das Gutachten eine rechtliche Einschätzung praktischen Verwaltungshandelns beinhalte.

Diese Auffassung können wir nicht teilen:

Nach § 23 Absatz 5 HmbDSG sind die der Aufsicht unserer Dienststelle unterliegenden Stellen verpflichtet, uns bei der Erfüllung unserer Aufgaben zu unterstützen. Unsere Frage- und Einsichtsrechte sind nicht auf konkrete Datenverarbeitungsprozesse be-

schränkt. Die Vorschrift beinhaltet ausdrücklich, Auskunft zu erteilen sowie Einsicht zu gewähren in alle Unterlagen und Akten, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen.

Zu den Aufgaben unserer Dienststelle gehört neben der Beratung der Behörden auch die Prüfung von Risikoanalysen und Verfahrensbeschreibungen im Rahmen der Vorabkontrolle von automatisierten Anwendungen. Dazu gehört angesichts des geltenden Gesetzesvorbehalts für Eingriffe in das informationelle Selbstbestimmungsrecht selbstverständlich auch die Prüfung hinreichender Rechtsgrundlagen.

Es war daher sachgerecht und erforderlich, das gerade wegen der im Übrigen bundesweit bestehenden Rechtsunsicherheit erstellte Gutachten anzufordern, um es im Sinne des LBV in unsere Prüfung einbeziehen zu können.

Leider hat das Gutachten, das sich ausführlich mit älteren und neueren Diskussionsständen zur Abgrenzung von Verwaltungshelferschaft und Beleihung befasst hat, inhaltlich wenig zur Beförderung der damit verbundenen datenschutzrechtlichen Fragestellungen beigetragen.
Die dort noch ausdrücklich unterstellte Identitätsprüfung ist weder als personenbezogene Datenverarbeitung noch hinsichtlich ihrer ermessensabhängigen Rechtswirkung innerhalb eines hoheitlichen Verfahrens problematisiert worden, sondern als ein kognitiver Vorgang auf einfache Übereinstimmung reduziert worden, der keine Prüfung darstelle. Dabei wurde unterstellt, dass dieser Vorgang keinen Einfluss auf die Verwaltungsentscheidung habe. Tatsächlich ist aber wenigstens die Bekanntgabe der KFZ-Zulassung durch Aushändigung der Papiere und gesiegelten Kennzeichen von der „Einschätzung" des Identitätsnachweises durch die beauftragte Stelle abhängig.

12.2 Handyparken

Mit dem Neuabschluss von Verträgen mit Systemanbietern zum Handyparken bietet sich die Gelegenheit, das Verfahren datenschutzkonform auszugestalten.

Das Handyparken nach § 13 Abs. 3 der Straßenverkehrsordnung soll es den Betroffenen ermöglichen, Parkgebühren bequemer und minutengenau entrichten zu können. Auf Seiten der Verwaltung wird mit Vereinfachungen und Einsparungen bei gleichzeitigen Mehreinnahmen gerechnet.

Dazu haben sich zwei grundlegend verschiedene Ansätze entwickelt:
Immer muss zwischen der Behörde und dem Betroffenen ein Systemanbieter zwischengeschaltet werden, der den Teilnehmer registriert, für die Abbuchung der Gebühren sorgt und für Kontrollen Auskunft darüber erteilt, ob der Betroffene zum Zeitpunkt

der Kontrolle zur Gebührenzahlung angemeldet ist. Die dafür erforderliche Plattform kann entweder von der Gemeinde oder dem Systembetreiber betrieben werden.
Nach dem einen Ansatz handeln die Systemanbieter im Auftrag der Verwaltung. Die personenbezogene Datenverarbeitung erfolgt von der Registrierung über die Gebührenerhebung bis zum Einzug von Bußgeldern auf einer städtischen Plattform und bleibt vollumfänglich in der Hand der Verwaltung.

Nach dem anderen Ansatz schließen die Systemanbieter zwar auch Verträge mit den Kommunen, um ihr System auf einer kommunalen Plattform elektronisch anbieten zu können; hinsichtlich der einzelnen Gebührenentrichtung handeln sie aber namens und im Auftrag der Betroffenen. Dies hat den Vorteil, dass der Betroffene sich nur einmal bei einem Anbieter seiner Wahl anmelden muss, um dann in verschiedenen Kommunen, in denen sein Anbieter vertreten ist, bargeldlos zahlen zu können. Parallel dazu verpflichtet sich der Anbieter gegenüber der Gemeinde typischerweise zum monatlichen Abführen der Einnahmen und unterzieht sich zudem einer gewissen Kontrolle durch die jeweilige Gemeinde.

Bereits 2007 waren wir durch die Behörde für Stadtentwicklung und Umwelt (BSU) zu laufenden Gesprächen mit einem Systemanbieter geladen worden. Wir hatten uns seinerzeit darauf beschränkt, auf die grundlegenden Schwierigkeiten des gemeindeübergreifenden Modells hinzuweisen, und dringend das Modell der Auftragsdatenverarbeitung empfohlen. Dieser Empfehlung ist die BSU seinerzeit nicht gefolgt. Sie hat 2008 das Handyparken nach einem Mustervertrag, der mit der Stadt Köln abgeschlossen worden war, eingeführt. Danach wurden auf einer Plattform die Angebote mehrerer Anbieter eingestellt.

Im Frühjahr 2013 bat die BSU vor Verlängerung des Vertrages um einen Termin zur datenschutzrechtlichen Beratung. Dabei war auch angedacht, die Plattform durch Dataport betreiben zu lassen. Da der Mustervertrag mit der Stadt Köln und auch der später vorgelegte Entwurf keine der genannten Varianten erkennbar und zutreffend abdeckte, haben wir nochmals auf die grundlegenden Unterschiede und deren datenschutzrechtlichen Anforderungen hingewiesen.

Zuletzt wurde uns mitgeteilt, dass ein privates Konsortium die erforderliche Plattform eigenverantwortlich betreiben und es Betroffenen anbieten soll, gegenüber allen angebotenen Gemeinden in ihrem Namen das Handyparken abzuwickeln (Vergabe von Kennzeichnungen, Nachweis der Registrierung eines Parkvorgangs gegenüber der Parkraumüberwachung sowie das Abführen der Parkgebühren an die zuständige Gemeinde).

Grundsätzlich hat die Freie und Hansestadt Hamburg bei der Umsetzung die Vorschriften des Hamburgischen Datenschutzgesetzes zu beachten. Dazu gehören vor allem die Datenerhebung beim Betroffenen, die Erforderlichkeit, die Zweckbindung und die

Datensparsamkeit. Darauf ist auch beim Vertragsabschluss mit einem Dritten zu achten. Andererseits müssen die Daten es ermöglichen, die Gebührenschuldner erforderlichenfalls auch verfolgen zu können.

Wir haben uns daher für die weiteren Hinweise auf eine datenschutzgerechte Ausgestaltung der Kommunikation mit dem Anbieter beschränkt:

Die Parkraumüberwachung sollte nur passwortgeschützt Anfragen verschlüsselt und unter Angabe des Zeitpunkts und des Kennzeichens zur Frage stellen können, ob eine Gebührenanmeldung für diesen Zeitpunkt besteht, hilfsweise, ob sie für diesen Tag einmal bestanden hat. Die Antwort sollte nicht den konkreten Standort, sondern nur die Parkzone beinhalten, um Profilbildungen auszuschließen.

Den Gebühreneinzugsstellen sollte zu Kontrollzwecken ein Zugriff im Wege des automatisierten Abrufs auf die Abrechnungsvorgänge auf Hamburgischen Parkflächen tagesaktuell unter Angabe eines verkürzten Kennzeichens, des Datums, des Beginns und des Endes sowie der Parkzone ermöglicht werden.

Für die laufenden monatlichen Abrechnungen sollte auf die Angabe des verkürzten Kennzeichens verzichtet werden.

Abfragen der Parkraumüberwachung und Kontrollen der Gebühreneinzugsstellen sind zu protokollieren. Die datenschutzgerechte Anbindung aller beteiligten Stellen ist durch Vorabkontrolle nach § 8 HmbDSG sicherzustellen. Ebenso ist sicherzustellen, dass neben dem Handyparken weiterhin die datensparsame Variante der bargeldlosen Gebührenzahlung angeboten wird.

Schließlich haben wir empfohlen, vertraglich zu regeln, dass die Betroffenen umfassend über die zwischen dem Konsortium und der FHH stattfindenden Datenflüsse informiert werden.

12.3 Verkehrslenkung durch Videoüberwachung

Wird zur Verkehrslenkung und -leitung Videoüberwachung eingesetzt, sind Übersichtsaufnahmen ausreichend und personenbezogene Daten unkenntlich zu machen. Werden für Zwecke der Gefahrenabwehr Übersichtsaufnahmen gezoomt und ist dabei die Verarbeitung personenbezogener Daten nicht ausgeschlossen, bedarf es einer Erlaubnisnorm für die Verarbeitung.

Seit langem betreibt die Polizei in der Verkehrsleitzentrale Videoüberwachung für Zwecke der Verkehrslenkung und Verkehrsleitung. Dazu benutzt sie Anlagen, deren schwenk- und neigbare Kameras auch gezoomt werden können für Fälle, in denen ein

Ereignis beobachtet wird und zur Gefahrenabwehr die Art des Hindernisses für die Einleitung der erforderlichen Maßnahmen festgestellt werden muss. Dabei werden teilweise auch personenbezogene Daten wie Kennzeichen und Reklameschriftzüge von Kleingewerbetreibenden erkennbar.
Daneben wird die Anlage in erforderlichem Umfang auch anderen Polizeidienststellen im Einzelfall zur Lagebeurteilung zur Verfügung gestellt.

In der Vergangenheit sind wir wiederholt beteiligt worden, als es um die Übermittlung von Aufnahmen an den Fernsehsender Hamburg1 ging und um den Austausch von Aufnahmen mit dem HVV. Seit 2011 werden Aufnahmen auch an die Hamburg Port Authority zum dortigen Verkehrsleitsystem übermittelt.

Man war seinerzeit übereingekommen, dass dagegen dann keine datenschutzrechtlichen Bedenken bestehen, wenn die Übertragung für die Dauer des Zoomvorgangs unterbrochen wird. Die Videoüberwachung selbst wurde als eine Art der Datenerhebung gewertet, die seit 2001 in analoger Anwendung von § 6b des Bundesdatenschutzgesetzes (BDSG) beurteilt wurde. Danach ist auch die Videoüberwachung zur Unterstützung der Aufgabenwahrnehmung zulässig. 2007 hat das Bundesverfassungsgericht zu einer gemeindlichen Videoüberwachung entschieden, dass die Videoüberwachung grundsätzlich einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen darstellt und jedenfalls in dem zur Entscheidung stehenden Fall einer hinreichend normenklaren Regelung durch den Gesetzgeber bedarf. Ein Rückgriff auf die Inhalte des § 6b BDSG bei fehlender landesrechtlicher Regelung scheidet aus Rechtsgründen aus.

Im Jahre 2013 hatten wir die Gelegenheit, die lange geplante, modernisierte Verkehrsleitzentrale zu besichtigen. Wegen der zwischenzeitlichen Bestellung eines behördlichen Datenschutzbeauftragten waren wir an den vorbereitenden Verfahren nicht beteiligt, mussten dann aber erfahren, dass eine Vorabkontrolle nicht durchgeführt worden war. Die Polizei hat dazu die Meinung vertreten, dass bei Übersichtsaufnahmen zur Verkehrslenkung keine personenbezogenen Daten verarbeitet würden und für die bei den Zoomvorgängen erfassten personenbezogenen Daten kein Erhebungswille bestehe und damit für die Verarbeitung eine Rechtsgrundlage nicht erforderlich sei.

Wir halten die Auffassung der Polizei vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts für nicht mehr zutreffend und haben unsere Auffassung im Zusammenhang mit der Modernisierung der Verkehrsleitzentrale gegenüber der Polizei und dem behördlichen Datenschutzbeauftragten nochmals betont. Nachdem der Hamburgische Gesetzgeber 2010 die Regelung in § 30 Hamburgisches Datenschutzgesetz (HmbDSG) auf Fälle des Hausrechts beschränkt hatte, hatten wir uns, wie berichtet (23.TB, III 1.2.2), im Arbeitskreis Verkehr der Konferenz der Datenschutzbeauftragten des Bundes und der Länder dafür eingesetzt, für den Verkehrsbereich auf eine bereichsspezifische bundesrechtliche Regelung zu drängen. Dies ist aus verschiedenen

Gründen bisher ohne Ergebnis geblieben. So waren eine Reihe von Fallkonstellationen nach ihren Eigenheiten zu betrachten, und nicht in allen Ländern besteht dasselbe Regelungsinteresse, da vielfach, wie in § 6b BDSG, in den dortigen Regelungen die Videoüberwachung auch zur Unterstützung der Aufgabenwahrnehmung zulässig ist.

Die Rechtmäßigkeit personenbezogener Datenverarbeitung ist nach § 10 HmbDSG zu jedem Zeitpunkt der Verarbeitung zu gewährleisten. Betroffen sind davon auch Passanten, die insbesondere an Kreuzungen bei entsprechenden Zoom-, Schwenk- und Neigungswinkeln erkennbar erfasst werden.

So wird in anderen Ländern, in denen die Verkehrslenkung und –leitung nicht bei der Polizei angebunden ist und keine gleichzeitige Nutzung zu Zwecken der konkreten Gefahrenabwehr erfolgt, selbst bei der Videoüberwachung zu Zwecken der Seitenstreifenfreigabe auf Autobahnen bzw. Schnellstraßen die Verpixelung personenbezogener Daten gefordert, da der Personenbezug für die Aufgabenwahrnehmung nicht erforderlich ist. Entsprechende technische Mittel stehen zur Verfügung. Angesichts der fortgeschrittenen technischen Möglichkeiten der Bildbearbeitung muss auch bei Verfahren, die grundsätzlich nur Übersichtsaufnahmen benötigen, durch eine Vorabkontrolle sichergestellt sein, dass auch bei Zusammenspiel aller Komponenten ein unzulässiger Personenbezug ausgeschlossen ist.

Auch Wirtschaftlichkeitserwägungen können hier nicht eingewendet werden. Das Datenschutzrecht kennt sie nur bei der Datensicherung im Zusammenhang mit dem Schutzbedarf. Die Rechtmäßigkeit der Verarbeitung bleibt davon unberührt.

Auf den Erhebungswillen kommt es spätestens seit der Entscheidung des Bundesverfassungsgerichts nicht mehr an, zumal die Vorschriften über die Videoüberwachung nicht auf den Begriff der Erhebung zurückgreifen, sondern mit dem Begriff der Beobachtung abweichende Voraussetzungen geschaffen haben. Zur Beobachtung gehört auch schon die nicht gezielte Sichtbarmachung. Für diese Auffassung sprechen auch die Regelungen im Polizei- und Versammlungsrecht, die die Aufnahmen Dritter ausdrücklich erlauben, wenn sie unvermeidbar sind.

Ist die Verarbeitung von Daten mit Personenbezug technisch nicht auszuschließen und soll auf die Verpixelung gleichwohl verzichtet werden, bedarf es daher einer hinreichenden Verarbeitungsermächtigung. Da damit in absehbarer Zeit auf Bundesebene nicht gerechnet werden kann, haben wir empfohlen, eine Rechtsgrundlage in das Gesetz über die Datenverarbeitung der Polizei (PolDVG) aufzunehmen, da auch die Verkehrsleitzentrale spätestens mit der einzelfallbezogenen Anwendung der Zoomfunktion im Bereich der Gefahrenabwehr datenschutzrelevant beobachtet.

12.4 Kamerafahrten zu Zwecken der Straßenunterhaltung

Kamerafahrten mit dreidimensionaler, auf Laservermessung beruhender Erfassung des Straßenraums sind zu Zwecken der Straßenunterhaltung selbst bei ausschließlicher Nutzung für diese Zwecke nur dann zulässig, wenn die dabei erhobenen personenbezogenen Daten zuverlässig und frühzeitig unkenntlich werden. Es reicht nicht, zum Schutz der Betroffenen die Verwendung durch Verwaltungsverfügung auf die Straßenunterhaltung zu beschränken.

Dem Landesbetrieb Straßen, Brücken und Gewässer (LSBG) obliegt die Unterhaltung der Straßen einschließlich der Beschilderung und der Ausstattung mit Lichtsignalanlagen. Im Sommer 2013 teilte uns der LSBG mit, dass er plane, ähnlich der Befahrung durch Google Street View, aber nur für eigene Zwecke, auf allen Hauptverkehrsstraßen und Autobahnabschnitten innerhalb des Staatsgebiets den Zustand der Straßen durch Kamerafahrten georeferenziert zu erfassen, und zwar ohne die dabei anfallenden personenbezogenen Daten zu verpixeln. Die Vorgehensweise werde auch durch das Bundesverkehrsministerium befürwortet, sei aber unabhängig von den Vorhaben des Landesbetriebs Geoinformation und Vermessung (LGV),vgl. dazu III 9.2; vielmehr habe dieser bereits Interesse an den Aufnahmen angemeldet. Der LGV ist für die Erfassung und Veröffentlichung bzw. Abgabe von Vermessungs- und geodatenbezogenen Produkten zuständig.

Die Vorstellung des Vorhabens durch den Systemanbieter ergab, dass nicht nur der eigentliche Straßenkörper mit einer bodenwärts gerichteten Kamera gefilmt und georeferenziert werden soll, sondern dass zwecks Erfassung der Infrastruktur wie Schilder und Leuchtsignalanlagen auch Rundum-Panoramaaufnahmen erforderlich sind. Damit vergrößert sich die Zahl der Betroffenen gegenüber der bloßen Erhebung des Straßenbelags und gelegentlich einzelner KFZ-Kennzeichen erheblich.

Die zuständige Behörde will aus Kostengründen von der Verpixelung Abstand nehmen und hält sie im Übrigen nicht für erforderlich, da eine öffentliche Aufgabe wahrgenommen werde, die Daten den Verwaltungsbereich nicht verlassen würden und nicht für Erwerbszwecke genutzt würden. Personenbezogene Daten würden nur als Beiwerk erfasst. Man halte die Daten für hinreichend geschützt, wenn Verwendungszweck und Speicherdauer verwaltungsintern festgelegt sowie die Weitergabe an Dritte ausgeschlossen würden.

Wir hatten kurzfristig vor der Vorstellung schon nach kursorischer Prüfung darauf hingewiesen, dass eine Verarbeitung der dabei erfassten personenbezogenen Daten wie Kfz-Kennzeichen und Gesichter, aber etwa auch Reklameschriftzüge von Kleingewerbetreibenden und Einzelkaufleuten nur dann zulässig sei, wenn dafür eine hinreichende Rechtsgrundlage gegeben sei oder die Daten durch Verpixelung für eine

weitere Verarbeitung hinreichend unkenntlich gemacht würden. Die Beeinträchtigung gegenüber der bloßen Bilderfassung wird durch die Georeferenzierung deutlich erhöht. Durch die weit in die Tiefe gehenden seitlichen Aufnahmen sind neben KFZ-Kennzeichen zumindest alle Passanten in ihren Rechten betroffen, ohne dass diese Daten zu irgendeinem Zeitpunkt für die Aufgabenwahrnehmung des LSBG erforderlich sind. Wir haben daher eine Verpixelung zumindest dieser Daten für unverzichtbar gehalten und uns dabei von folgenden Überlegungen leiten lassen:

Der LSBG ist bei der personenbezogenen Datenverarbeitung an Recht und Gesetz gebunden und darf die Daten nur soweit verarbeiten, wie dies für seine Aufgabenwahrnehmung erforderlich ist. Dies gilt für jede Phase der Verarbeitung.
Zur Aufgabenwahrnehmung benötigt der LSBG zwar Informationen über den Straßenzustand, die Beschilderung und die Lichtzeichenanlagen, nicht aber die erfassten personenbezogenen Daten.

Auch wenn man unterstellt, dass die Daten bei Bilderfassung unvermeidbar aufgenommen werden, so sind sie als nicht erforderliche Daten nach § 19 Abs. 3 des Hamburgischen Datenschutzgesetzes (HmbDSG) doch zu löschen, im Falle einer Bilderfassung also schnellstmöglich zu verpixeln. Demzufolge muss technisch sichergestellt sein, dass die Verpixelung umgehend nach der Aufnahme erfolgt. Hinreichende technische Verfahren stehen zur Verfügung.

Auf die Verpixelung kann auch nicht aus Kostengründen verzichtet werden. Das Gesetz sieht eine Wirtschaftlichkeitsabwägung nur bei einzusetzenden Maßnahmen der Datensicherheit vor, und zwar vorbehaltlich der Rechtmäßigkeit der Datenverarbeitung.
Der Gedanke des Beiwerks ist dem Kunsturhebergesetz entnommen und kann hier nicht weiterhelfen. Es verfolgt als Schutzzweck die Sicherung der künstlerischen Betätigung und privilegiert dazu nur die Veröffentlichung, also Übermittlung, selbst wenn Personen als Beiwerk erscheinen. Hier geht es jedoch schon um die rechtmäßige Erhebung der Daten. Sie richtet sich für den LSBG nach dem HmbDSG.

Die geplante verwaltungsinterne Verwendungsbegrenzung ist als untergesetzliche Vorschrift zum Schutz der Betroffenen weder geeignet noch ausreichend. Die personenbezogene Datenverarbeitung steht unter dem materiellen Gesetzesvorbehalt. Das HmbDSG bestimmt die Voraussetzungen und Grenzen einer Zweckänderung und möglicher Übermittlungen. Die Erfahrung zeigt, dass vorhandene Daten immer Begehrlichkeiten wecken, und weitere Verwendungsmöglichkeiten wären unschwer vorstellbar.

Von der Verpixelung kann schließlich auch nicht abgesehen werden, weil die personenbezogenen Daten mit den erforderlichen Daten in den Bildaufnahmen fest verbunden sind. Dieses Privileg kennt das Gesetz nur bei der Aktenführung in Papierform. Werden Daten automatisiert verarbeitet, ist in jeder Phase ihrer Verarbeitung deren Rechtmäßigkeit sicherzustellen (§ 10 HmbDSG).

Daneben sind auch die georeferenzierten Hausfassaden in Bezug auf ihre Eigentümer und Bewohner als personenbeziehbare Daten geschützt, vgl. 22. TB IV 3.3 zur parallelen Problematik bei Google Street View. Die Prüfung zu diesem Komplex ist noch nicht abgeschlossen. Wir haben dies zum Anlass genommen, die Fragestellung in den Arbeitskreis Verkehr der Datenschutzbeauftragten des Bundes und der Länder einzubringen.
Wie wir erfahren haben, hat auch in Brandenburg bei entsprechender Sachlage die unverpixelte Verarbeitung zu Beanstandungen geführt.

Zu Redaktionsschluss teilte uns die zuständige Behörde mit, dass die Prüfung unserer Argumente noch nicht abgeschlossen sei.

12.5 Videoüberwachung des Schiffsverkehrs

Für die Videoüberwachung zur Sicherung des Schiffsverkehrs im Hamburger Hafen sollte eine bereichsspezifische landesrechtliche Regelung im Hafen- und Schifffahrtsgesetz getroffen werden.

Die Hamburg Port Authority (HPA) ist eine der Stellen, die zu Verkehrssicherungszwecken umfänglich Videoüberwachung betreibt. So wurde auch der Bedarf für eine Videoüberwachung des Schiffsverkehrs durch die Verkehrszentrale der HPA zur Verbesserung der maritimen Verkehrssicherung gesehen und eine entsprechende Anlage installiert. Dabei können auch personenbezogene Daten anfallen.

Im Jahre 2012 wurde uns die bestehende Anlage vorgeführt. An der Sinnhaftigkeit und Erforderlichkeit bestanden keine Zweifel. Die radargestützte Technik des durchaus nicht fehlerfreien automatischen Identifikationssystems mittels Transponder in der Seeschifffahrt (AIS) ist nicht auf allen Wasserfahrzeugen vorgeschrieben und erkennt daher Kleinfahrzeuge nicht, erzeugt Fehlechos, insbesondere im Bereich der Liegeplätze, und kann keine Daten zu Nebelverhältnissen liefern. Dementsprechend wird Videoüberwachung bereits vom Bund und anderen Ländern zur ergänzenden Überwachung von Wasserstraßen nach den jeweils einschlägigen Vorschriften eingesetzt.

Die Aufgabe der Verkehrssicherung, -regelung und -information auf der Bundeswasserstraße Elbe obliegt im Bereich des Hamburger Hafens nicht der Bundesverwaltung, sondern nach § 45 Abs. 5 des Bundeswasserstraßengesetzes und § 3 Abs. 1 Nr. 3 des Gesetzes über die Hamburg Port Authority (HPAG) der HPA. Sie handelt insoweit als Gefahrenabwehrbehörde zwar auf einer Bundeswasserstraße, unterliegt damit aber, soweit personenbezogene Daten anfallen, den Vorschriften des Hamburgischen Datenschutzgesetzes (HmbDSG).

Wie in anderen Bereichen auch, war die Videoüberwachung zunächst als eine Form der Datenerhebung betrachtet worden, die auch vom Hamburgischen Datenschutzbeauftragten früher in analoger Anwendung von § 6b des Bundesdatenschutzgesetzes (BDSG) beurteilt worden war. § 6b BDSG kennt auch die Videoüberwachung zur Unterstützung der Aufgabenwahrnehmung. Nachdem das Bundesverfassungsgericht eine analoge Anwendung ausgeschlossen hatte und für den Bereich der Videoüberwachung normenklare spezifische Regelungen gefordert hatte, hat der Hamburgische Gesetzgeber sich im HmbDSG auf die Regelung zu Hausrechtszwecken beschränkt und fachspezifische Anforderungen einer Regelung in Fachgesetzen vorbehalten.

Wir haben daher empfohlen, die Videoüberwachung des Hafens zu Zwecken der Verkehrssicherung, -regelung und –information landesrechtlich im Hafenverkehrs- und Schifffahrtsgesetz zu regeln. Ein erster Entwurf eines zweiten Gesetzes zur Änderung des Hafen- und Schifffahrtsgesetzes ist auf Arbeitsebene mit uns abgestimmt und an die Fachbehörde zur weiteren Veranlassung weitergereicht worden.

13. Hochschulwesen

13.1 Novellierung des Hamburgischen Hochschulgesetzes

Bei der Weiterentwicklung des Hochschulrechts wurde eine Auskunftspflicht von ehemaligen Studierenden zu Gründen eines Studienabbruchs eingeführt. Wir konnten erreichen, dass Gründe aus dem persönlichen, insbesondere gesundheitlichen und familiären Bereich davon ausgenommen und nur auf freiwilliger Basis mitgeteilt werden.

Im Mai 2013 erreichte uns ein umfangreicher Drucksachenentwurf zur Neuordnung des Hamburgischen Hochschulrechts. Mit dem Ziel, die Qualität in Studium und Lehre zu verbessern, verpflichtete § 3 des Gesetzentwurfs zum Hamburgischen Hochschulgesetz (HmbHG) die Hochschulen, die Gründe für eine Studienbeendigung ohne Abschluss zu untersuchen. § 111 Abs.2a HmbHG-E ermächtigte die Hochschulen, in einer Satzung auch ehemalige Studierende zu verpflichten, über „Gründe für Studienverlauf und –ergebnis" Auskunft zu geben. § 118 Abs.3 Ziff.3 HmbHG-E qualifizierte einen Verstoß gegen diese Auskunftspflicht als Ordnungswidrigkeit.

Mit unserer Stellungnahme schlugen wir vor, in § 111 Abs.2 a HmbHG die Befragungsziele durch eine Insbesondere-Regelung zu konkretisieren, um sie stärker auf den Gegenstand der in § 3 HmbHG-E eingefügten Untersuchungspflicht der Hochschule zu beschränken. Vor allem aber drängten wir darauf, nähere Angaben über gesundheitliche, familiäre oder (hochschul-)politische Gründe für einen Studienabbruch oder Hoch-

schulwechsel von der Auskunftspflicht auszunehmen und insoweit ausdrücklich eine Belehrung der Befragten über die Freiwilligkeit dieser Angaben im Gesetz vorzusehen. Ferner regten wir an, die Verpflichtung der externen Berufungsausschuss-Mitglieder auf das Datengeheimnis in § 14 Abs.2 S.5 HmbHG aufzunehmen.

Die Anfang Juni 2013 versandte überarbeitete Entwurfsfassung berücksichtigte unsere Vorschläge und Formulierungsangebote vollständig.

Auch die weitere Fassung des Gesetzentwurfs, die die Behörde für Wissenschaft und Forschung aufgrund von Prüfaufträgen des Senats und einem Beteiligungsverfahren mit den Spitzenorganisationen im Dezember 2013 vorlegte, behielt die von uns angeregten Änderungen bei. § 111 Abs.2a HmbHG-E geht nun sogar noch darüber hinaus und bindet die Auskunftspflicht für die ehemaligen Studierenden generell an die weitergehende Bedingung „sofern keine überwiegenden berechtigten Belange der Befragten entgegenstehen".

13.2 Projekt Hochschulübergreifendes Identitätsmanagementsystem eCampus-IDMS

Nach der Regelung auf Gesetzesebene erforderte die Erstellung einer Mustersatzung weitere intensive Beratungen.

Wir haben schon früher ausführlich über das Projekt eines hochschulübergreifenden Identitätsmanagementsystems und seine Umsetzung berichtet (22.TB, III 11.1, 23.TB III 11.2). Ziel des Projekts ist es, zur Umsetzung der immer engeren Kooperationen der Hamburgischen Hochschulen untereinander eine übergreifende Infrastruktur zur Verwaltung aller Hochschulangehörigen zu gewährleisten. So soll jeder Hochschulangehörige über nur noch eine Kennung sich für alle für ihn freigeschalteten Verfahren anmelden können, egal an wie vielen Hochschulen er studiert oder beschäftigt ist. Dafür sollen in einem kaskadierenden Ansatz die Personendatensätze aus 59 Einzelangaben in ein Meta Directory eingespeist und darin, mit einem Identifikationsmerkmal versehen, konsolidiert und zu einer einzigen hochschulübergreifenden Kennung verarbeitet werden. Wie uns das Projekt im Verlauf des Berichtszeitraums mitteilte, wurde zwischenzeitlich von dem Ziel, allen Studierenden einen E-Mail-Account zur Verfügung zu stellen, abgesehen. Ebenso wurde davon Abstand genommen, dass jede beteiligte Stelle, soweit sie fachlich Kontakt zu einem Betroffenen unterhält, Aktualisierungen des Personendatensatzes vornehmen kann. Ursprünglich hatte man sich erhofft, insbesondere über die beteiligte Staats- und Universitätsbibliothek zeitnaher Aktualisierungsmeldungen verarbeiten zu können.

Nachdem schon in der letzten Berichtszeit die gesetzliche Grundlage für das System

in § 111 Abs. 4 Hamburgisches Hochschulgesetz (HmbHG) gelegt worden war, haben wir in mehreren Durchläufen die erforderlichen Inhalte der Mustersatzung weiter diskutiert und die Vorabkontrolle mit Risikoanalyse und Verfahrensbeschreibung nach § 8 f des Hamburgischen Datenschutzgesetzes (HmbDSG) begleitet.

Bei der Mustersatzung kam es weiterhin darauf an, die Verantwortlichkeiten der beteiligten Stellen, ihre Befugnisse, den erforderlichen Verarbeitungsumfang und insbesondere die notwendige Protokollierung der überwiegend voll automatisierten Datenverarbeitung abzubilden. Denn die Verantwortung für die Richtigkeit dieses Prozesses, der vor Ort in der einzelnen Hochschule Einfluss auf die Anwendungen (z.B. richtige Zuordnung von Kennungen bei der Berechtigungsvergabe für einzelne Anwendungen) und auf den Status der Betroffenen hat (richtige Konsolidierung von Mehrfachmeldungen, automatische Löschung nach systembedingt vorgegebenen Löschroutinen), trägt die für das Verfahren verantwortliche Stelle. Daher ist es erforderlich, dass die ändernden Zugriffe auf den Personendatensatz dauerhaft nachvollzogen werden können, wie dies sonst im Rahmen einer herkömmlichen Aktenführung schriftlich dokumentiert würde. Diese Zugriffe sind deshalb nach der für die Datenschutzkontrolle üblichen Frist von sechs Monaten zu sperren und bis zum Ausscheiden der Betroffenen vorzuhalten.

Diese Protokollierungsanforderung geht über die übliche Sechsmonatsfrist für Datenschutzkontrollzwecke deutlich hinaus. Da im Verlauf der Umsetzung mitgeteilt wurde, dass nur noch die Hochschule, an der ein Studierender immatrikuliert bzw. ein Mitarbeiter beschäftigt ist, wirksam Änderungen am Personendatensatz vornehmen können sollte, war auch eine Notwendigkeit, allen beteiligten Stellen Zugriff auf die Protokollierung zu gewähren, nicht begründbar und die Zugriffsrechte entsprechend zu beschränken.

Mit der jetzigen Ausgestaltung hat unsere Forderung, die Sicherungsmaßnahmen an einem hohen Schutzbedarf auszurichten, ausdrücklich Eingang in die Regelung gefunden. Vor diesem Hintergrund besteht im Rahmen der Vorabkontrolle des Verfahrens beim vorgesehenen Betrieb im Rechenzentrum der Hochschule für angewandte Wissenschaften noch weiterer Diskussionsbedarf.

14. Wirtschaftsverwaltung

14.1 Videoüberwachung im Jagdwesen

Der Einsatz von Wildbeobachtungskameras durch Jäger der Jagdgenossenschaften richtet sich nach den Vorschriften des öffentlichen Rechts. Mangels hinreichender Rechtsgrundlagen ist zur Zeit nur ein Einsatz im Rahmen von wissenschaftlichen Forschungsvorhaben denkbar.

Kameras, die zur Videoüberwachung eingesetzt werden können, werden immer kleiner und leistungsfähiger. Sie können so in den unterschiedlichsten Bereichen eingesetzt werden. Der Einsatz sogenannter Wildkameras wird in Jagdkreisen daher intensiv diskutiert. Wiederholt hat es Berichterstattungen gegeben über Betroffene, die durch Wildkameras zum Teil empfindlich in ihren Rechten verletzt wurden.

Wir haben verschiedene Presseberichte zum Anlass genommen, uns bei der Jagdaufsichtsbehörde nach dem Sachstand in Hamburg zu erkundigen. Uns wurde mitgeteilt, dass ein Interesse bestehe, mit Wildkameras insbesondere an den Landesgrenzen die Wanderung von Schwarzwild zu beobachten und Wildschäden zu verhüten.

Das Jagdwesen ist im Bundesjagdgesetz (BJagdG) und im Hamburgischen Jagdgesetz (HmbJagdG) geregelt.

Das Jagdrecht steht dem Eigentümer auf seinem Grund und Boden zu; auf Flächen, an denen kein Eigentum begründet ist, steht das Recht den Ländern zu. Das Jagdrecht darf nur in Jagdbezirken (Eigenjagdbezirke bei alleinigem Eigentum oder gemeinschaftliche Jagdbezirke) ausgeübt werden. Eigentümer, deren Grundflächen zu einem gemeinsamen Jagdbezirk gehören, bilden eine Jagdgenossenschaft. Der Jagdgenossenschaft steht das Jagdrecht zu. Sie nutzt es in der Regel durch Verpachtung. Nach § 10 Abs. 1 BJagdG kann sie die Verpachtung auf den Kreis der Jagdgenossen beschränken. Verpachtet werden dabei nicht die Grundstücke, sondern das Recht zur Jagdausübung. Nach Auskunft der Aufsichtsbehörde seien die Hamburgischen Jagdbezirke ausschließlich in Jagdgenossenschaften organisiert. Diese verpachteten nahezu ausschließlich an ihre Mitglieder.

Nach § 5 HmbJagdG sind Jagdgenossenschaften Körperschaften des öffentlichen Rechts. Sie unterliegen bei der personenbezogenen Datenverarbeitung daher den Vorschriften des Hamburgischen Datenschutzgesetzes (HmbDSG).

Wir haben deshalb folgende Hinweise gegeben:
Wird das Jagdrecht unter Nutzung von Wildbeobachtungskameras ausgeübt, hat es sich folglich nach den Vorschriften des HmbDSG zu richten. Da weder im HmbJagdG noch im HmbDSG eine hinreichende Rechtsgrundlage für die Videoüberwachung zur Wildschadensverhütung getroffen wurde, wäre eine Überwachung derzeit unzulässig.

Als Körperschaften des öffentlichen Rechts können die Jagdgenossenschaften nur diejenigen Rechte verpachten, die sie selbst besitzen. Die Pächter übernehmen damit als abgeleitetes Recht die öffentlich-rechtlichen Rechte und Pflichten des Jagdrechts der Genossenschaft, wie sie schon als Mitglieder daran gebunden sind. Es umfasst neben der Aneignung als Nutznießung auch die Hege und Pflege als Gefahrenabwehr.

Wie in anderen Ländern diskutiert, kommt nach Hamburgischem Recht zur Zeit ledig-

lich eine Überwachung zu Forschungszwecken in Betracht. Dabei ist jedoch sicherzustellen, dass es sich nicht nur um von der Aufsichtsbehörde beauftragte statistische Erhebungen handelt, sondern dass es sich nach § 27 HmbDSG um wissenschaftliche Forschung handeln muss.
Hierauf haben wir hingewiesen. Dazu teilte die Aufsichtsbehörde mit, dass eine Nutzung durch die Pächter nicht mehr geplant sei, dass aber mittelfristig geplant sei, einen Forschungsauftrag an eine deutsche Hochschule zu vergeben.

Bei der Ausarbeitung des Auftrags haben wir unsere Unterstützung angeboten.

15. Parlamentsangelegenheiten, Wahlen und Volksabstimmungen

15.1 Änderungen des Volksabstimmungsrechts

Bei der Änderung des Gesetzes und der Verordnung zu Volksabstimmungen konnten wir einige datenschutzrechtliche Verbesserungen erreichen.

Im Mai 2012 wurde uns der Entwurf eines Gesetzes zur Änderung des Volksabstimmungsgesetzes zugesandt. Ziel der Änderung war die Anpassung an Art.50 der Hamburger Verfassung, der unter anderem eine Zusammenlegung von Volksabstimmungen mit Bürgerschafts- oder Bundestagswahlen vorsieht. Zu den sehr ausdifferenzierten Verfahrensbestimmungen des Gesetzentwurfs nahmen wir im Juni 2012 Stellung. Wir regten im Wesentlichen an,

- bei den Beratungen der Initiatoren durch die Abstimmungsleitung auch ausdrücklich die Einbeziehung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit vorzusehen, wenn Datenschutz- oder Informationsfreiheitsfragen berührt sind,
- in die Verordnungsermächtigung auch die Ausgestaltung des (obligatorischen) elektronischen Eintragungsverzeichnisses aufzunehmen,
- für eine elektronische Beantragung einer Briefeintragung (analog zur Briefwahl) eine verschlüsselte Übertragung der Antragsdaten im Internet vorzusehen.

Am 20. August 2012 übersandte die Behörde für Inneres den geänderten Gesetzentwurf. Er nahm unsere Vorschläge auf und setzte sie um. Die Verschlüsselung von elektronischen Anträgen auf Briefeintragung wird in der Gesetzesbegründung ausdrücklich erwähnt, im Gesetzestext wird allgemeiner auf ein „zugelassenes elektronisches Verfahren" Bezug genommen. Das Gesetz wurde so im Oktober 2012 verabschiedet.

Ein Jahr später haben wir auch die vom Volksabstimmungsgesetz vorgesehene Verordnung begleitet. In unserer Stellungnahme vom Mai 2013 regten wir folgende Änderungen an:

- eine gesetzliche Grundlage oder zumindest eine entsprechende Zuständigkeitsanordnung des Senats für die Zentralisierung der Gültigkeitsprüfung durch nur ein Bezirksamt,
- eine Beschreibung konkreter Inhalte für die bisher zugelassenen Freitextfelder („Bemerkungen") im Abstimmungsverzeichnis,
- den Schutz der bei Straßensammlungen erstellten, aber noch nicht der zuständigen Behörde ausgehändigten Unterschriften- und Eintragungslisten vor unbefugtem Zugriff,
- die Ergänzung „datenschutzgerecht" für die Vernichtung nicht abgegebener Unterschrifts- und Eintragungslisten durch die Initiatoren.

  Zu den beiden erstgenannten Punkten teilte uns die Innenbehörde mit, dass eine entsprechende Fassung der Zuständigkeitsanordnung geplant sei und für das Freitextfeld „Bemerkungen" technische Vorgaben bestünden, die eine beliebige Eintragung ausschließen. Die am 19.Juli 2013 beschlossene Volksabstimmungsverordnung setzt unsere beiden letztgenannten Vorschläge wörtlich um.

15.2 Vordrucke für die Beantragung von Briefwahlunterlagen

Durch die Umstellung der Vordrucke zur Beantragung von Briefwahlunterlagen und die damit verbundene Versendung im geschlossenen Umschlag konnte der Datenschutz der Wählerinnen und Wähler endlich verbessert werden.

In der Vergangenheit hatten wir mehrfach die datenschutzrechtlich unerfreuliche Praxis behandelt, dass die Vordrucke zur Beantragung von Briefwahlunterlagen im Postkartenformat mit vorgedruckter Adresse der zuständigen Wahldienststelle ausgegeben wurden (22.TB, III 13.1, 23.TB, III 13.1). Das führte dazu, dass die Antragsteller verleitet wurden, ihre Anträge mit allen erforderlichen personenbezogenen Daten, zum Teil einschließlich der Angabe von Kommunikationsdaten, vor Einsehbarkeit durch Dritte ungeschützt zu versenden. Zum Teil verstieß diese Praxis gegen bestehende Bundesvorschriften.

Zuletzt war uns, wie berichtet, zur vorgezogenen Bürgerschaftswahl 2011 mitgeteilt worden, dass eine datenschutzfreundliche Gestaltung wegen der gebotenen Eile nicht mehr rechtzeitig habe umgesetzt werden können, dass eine datenschutzfreundliche Ausgestaltung aber unverändert vorgesehen sei.

Dies ist bei der vergangenen Bundestagswahl auch umgesetzt worden:

Schon im September 2012 hat uns das Landeswahlamt das für die Bundestagswahl 2013 vorgesehene Antragsformular zur Abstimmung vorgelegt. Im Bundesrecht ist die Gestaltung durch Muster weitgehend vorgegeben und war schon früher im DIN A4-Format vorgesehen.

Diese Vorgabe ist übernommen worden. Die Ansprache war weniger förmlich gewählt worden, und die persönlichen Angaben sollten als Erleichterung bereits aus dem Melderegister übernommen werden.

Hiergegen bestanden im Ergebnis keine Bedenken. Die Übersendung erfolgte in einem geschlossenen Umschlag, so dass die Daten auf dem Transportweg hinreichend gesichert waren.

Im Juli 2013 wurde uns auf Anfrage mitgeteilt, dass auch die Wahlbenachrichtigung zur anstehenden Europa- und Bürgerschaftswahl analog zu der Wahl- und Abstimmungsbenachrichtigung gestaltet werde.

16. Bezirke

16.1 Datenverarbeitung bei der Ausschussarbeit der Bezirksversammlungen

Auch bei der Ausschussarbeit sind die Regelungen des Hamburgischen Datenschutzgesetzes zu beachten, soweit nicht das Bezirksverwaltungsgesetz vorrangige Regelungen trifft. Weitergehende Regelungen zugunsten der Bürgerschaft sind auf die Bezirksverwaltung nicht anwendbar.

In der Berichtszeit sind wir mit verschiedenen datenschutzrechtlichen Fragestellungen bei der Arbeit der Bezirksversammlungen und ihrer Ausschüsse befasst worden. Dabei ist insbesondere beachtlich, dass Bezirksversammlungen keine echten Parlamente, sondern Verwaltungsausschüsse sind. Ihre Rechte und Pflichten ergeben sich aus dem Bezirksverwaltungsgesetz (BezVG) und, soweit dieses keine spezifischen datenschutzrechtlichen Regelungen trifft, aus dem Hamburgischen Datenschutzgesetz (HmbDSG).

16.1.1 Öffentliche Behandlung von Eingaben

Jeder Einwohner kann sich, ähnlich wie an die Bürgerschaft und den Bundestag, zu allen persönlichen und öffentlichen Belangen mit Eingaben auch an die Bezirksversammlung oder ihre Ausschüsse wenden. Dabei sind die unterschiedlichen rechtlichen Voraussetzungen beachtlich.

§ 20 BezVG bestimmt zu Eingaben lediglich, dass sie nach Maßgabe der Geschäftsordnung der jeweiligen Bezirksversammlung zu behandeln sind. Die Geschäftsordnungen sind nicht einheitlich. Die Regelungen reichen von der analogen Anwendung der bürgerschaftlichen Vorschriften – und damit der nicht-öffentlichen Behandlung – über ausschließlich interne Verfahrensregelungen bis zur Nichtregelung.

So enthält die Geschäftsordnung der Bezirksversammlung Altona in den Paragrafen 10 und 16 neben internen Verfahrensregelungen keine Regelung zur öffentlichen oder nicht-öffentlichen Behandlung von Eingaben. In der Bezirksversammlung Altona wurde daher erwogen, Eingaben künftig grundsätzlich öffentlich zu behandeln. Zu dem dazu entworfenen Konzept hat uns die behördliche Datenschutzbeauftragte 2012 um Stellungnahme gebeten.
Die Betroffenen sollten sich vorab unter Fristsetzung zu folgenden Varianten erklären:
öffentliche Behandlung in den Ausschüssen mit Veröffentlichung im Internet,
öffentliche Behandlung in den Ausschüssen mit Veröffentlichung im Internet bei Schwärzung konkret anzugebender personenbezogener Daten oder Behandlung in nichtöffentlicher Sitzung ohne Veröffentlichung.

Ohne fristgerechte Rückmeldung sollte die zweite Variante angewendet werden. Seitens des Ältestenrates war erwogen worden, auf die Auswahlmöglichkeit der nichtöffentlichen Behandlung gänzlich zu verzichten.

Hierzu haben wir auf folgendes hingewiesen:
Die öffentliche Behandlung von Eingaben stellt datenschutzrechtlich eine Übermittlung an Stellen außerhalb des öffentlichen Bereiches dar. Aufgrund des im Datenschutzrecht geltenden Verbots mit Erlaubnisvorbehalt bedarf es hierfür einer gesetzlichen Grundlage.
§ 14 BezVG regelt zwar die Öffentlichkeit von Sitzungen, verpflichtet die oder den Vorsitzenden bzw. die Bezirksamtsleitung aber gleichzeitig, bestimmte Themen in nichtöffentlicher Sitzung zu behandeln. Diese Regelung ist auch bei der Ausgestaltung der Eingabenbearbeitung beachtlich. Dabei genügt schon, dass berechtigte Interessen Einzelner dies erfordern. Eine Abwägung berechtigter Interessen mit dem Allgemeinwohl ist hier nicht vorgesehen.

Für die Frage, ob bei der öffentlichen Behandlung von Eingaben berechtigte Interessen Einzelner betroffen sind, können die Regelungen von Bürgerschaft und Bundestag vergleichend herangezogen werden. Dort werden Eingaben ausdrücklich nicht-öffentlich behandelt und lediglich der Bürgerschaft bzw. dem Bundestag in anonymisierter Form berichtet. Zudem dürfte es auch den Erwartungen der Betroffenen entsprechen, dass ihre Anliegen wie in Bund und Ländern nicht vor einer breiten Öffentlichkeit behandelt werden.
Dasselbe ergibt sich nach § 7 HmbDSG, wonach die Bezirksversammlungen und ihre Ausschüsse als Teil der Verwaltung das Datengeheimnis zu wahren haben.

Da verschiedene Anliegen denkbar sind, die nicht nur die Petenten selbst betreffen, haben wir eine abgestufte Vorgehensweise empfohlen:

Bei ausschließlich persönlichen Belangen nicht-öffentliche Behandlung, bei Belangen, die (auch) Dritte angehen können, Behandlung ohne Nennung des Petenten. Ist eine

öffentliche Behandlung unter Einbeziehung der Betroffenen sinnvoll oder beinhaltet die Eingabe ausschließlich allgemeine Vorschläge, kann eine informierte Einwilligung erfragt werden. Sie muss dann den Anforderungen des § 5 Absatz 3 HmbDSG entsprechen.

16.1.2 Weitergabe personenbezogener Daten an Ausschüsse

2013 hat sich das Bezirksamt Eimsbüttel aufgrund entsprechender Beschlüsse mit folgenden Fragen beschäftigt und dazu auch die behördliche Datenschutzbeauftragte um unsere Beteiligung gebeten: Können jeweils regelhaft die Namen von Eigentümern leer stehender Wohnungen und der nicht berücksichtigten Bieter in Vergabeverfahren den jeweils zuständigen Ausschüssen mitgeteilt werden?

Das Gutachten kam zu dem Ergebnis, dass mangels konkreter Erforderlichkeit für den Einzelfall eine regelhafte Weitergabe nicht möglich sei. Dabei stellt es auf § 19 Absatz 2 BezVG ab, wonach die Bezirksversammlung die Arbeit des Bezirksamtes kontrolliert. Wir haben verschiedene Hinweise gegeben und teilen das Ergebnis, dass in beiden Fallkonstellationen eine regelhafte Weitergabe nicht zulässig ist.

Ohne spezifische gesetzliche Regelung kann die Weitergabe nur nach den allgemeinen Datenschutzregelungen erfolgen. Als Verwaltungsausschüsse sind auch die Bezirksversammlungen und ihre Ausschüsse an die Regelungen des HmbDSG gebunden. Dazu gehören u.a. der Grundsatz der Erforderlichkeit, der in §§ 12 ff HmbDSG für die Erforderlichkeit, bezogen auf den Einzelfall und auf die spezifische Aufgabenstellung der einzelnen Ausschüsse, auf den Zeitpunkt der Verarbeitung abstellt, und der Grundsatz der Datensparsamkeit (§ 5 Absatz 4 HmbDSG).

Zutreffend hat das Gutachten betont, dass das Bezirksamt seine Aufgaben nach Recht und Gesetz und ohne Ansehen der Person wahrnimmt. Sind die Betroffenendaten grundsätzlich nicht entscheidungserheblich, sind sie auch für die Kontrolltätigkeit grundsätzlich nicht erforderlich. Die Weitergabe von Namen Betroffener im Rahmen einer Kontrolle nach § 19 Absatz 2 BezVG wäre danach nur bei Umständen oder Anhaltspunkten sachgerecht, die deren Kenntnis im Einzelfall bedürften. Daneben wäre auch eine stichprobenhafte Kontrolle bestimmter Vorgänge oder Zeiträume denkbar, die aus der Natur der Sache heraus aber ebenfalls ohne Ansehen der Person zu erfolgen hat und daher nach dem Grundsatz der Datensparsamkeit ebenfalls ohne die listenweise Weitergabe der Namen der Betroffenen zu erfolgen hätte.

Im Ergebnis kann auch eine Beurteilung nach § 19 Absatz 1 BezVG, wonach das Bezirksamt über Angelegenheiten von grundsätzlicher Bedeutung zu informieren hat, nicht zu einer regelhaften Namensweitergabe führen. Ob eine Angelegenheit grundsätzliche Bedeutung hat, ergibt sich oft erst im Einzelfall. Erscheinen einzelne Verwal-

tungsaufgaben per se von grundsätzlicher Bedeutung, ist es angemessen, diese vorab gemeinsam mit der Bezirksverwaltung festzulegen. Auch dann kann die Weitergabe der Namen der Betroffenen nur einzelfallbezogen geprüft werden.

Weitergehende Kontrollbefugnisse hinsichtlich der Namen der Betroffenen können sich im Einzelfall aus besonderen Umständen oder konkreten Anhaltspunkten ergeben oder auf der Grundlage einer informierten Einwilligung der Betroffenen. Sie lösen dann aber gleichwohl regelmäßig die Prüfung nach § 14 BezVG aus, ob berechtigte Interessen der Betroffenen es erfordern, den Vorgang nicht-öffentlich und vertraulich zu behandeln, um das Datengeheimnis der Betroffenen hinreichend zu schützen. Dabei ist insbesondere auch beachtlich, dass die Protokolle zu in öffentlicher Sitzung behandelten Vorlagen bisher auch in das Ratsinformationssystem eingestellt und allgemein zugänglich gemacht werden. Dies wäre gegebenenfalls sachgerecht zu modifizieren.

Wir haben die Anfrage auch zum Anlass genommen, nochmals darauf hinzuweisen, dass die Ausschuss- und Fraktionsmitglieder nicht nur der Verschwiegenheit nach §§ 7 und 11 BezVG unterliegen, sondern bei der Verarbeitung personenbezogener Daten dem weiter reichenden Datengeheimnis nach § 7 HmbDSG.

Die Regelungen des BezVG gelten nicht nur für Vorgänge mit Personenbezug, sondern auch für allgemeine Vorgänge und nehmen offenkundige Tatsachen, abschließend beratene Angelegenheiten und Angelegenheiten, die ihrer Natur nach keiner Geheimhaltung mehr bedürfen, ohne weitere Differenzierung von der Verschwiegenheitspflicht aus. Daher ist daneben § 7 HmbDSG beachtlich, der personenbezogene Daten ausnahmslos auch über die Dauer des Beschäftigungsverhältnisses hinaus durch das Datengeheimnis schützt, und zwar unabhängig vom Beratungsstand und der vermeintlichen Belanglosigkeit einzelner Angaben.

16.1.3 Personenbeziehbarkeit bei der Beantwortung Großer und Kleiner Anfragen

Eine Kleine Anfrage der Bezirksversammlung Eimsbüttel betraf ausschließlich die Mitglieder der Bezirksversammlung und ihrer Ausschüsse. Sie warf gleich mehrere grundsätzliche datenschutzrechtliche Fragen auf. Zum einen ging es um die Frage, ob einzelne personenbezogene oder personenbeziehbare Auskünfte für die eigentliche Fragestellung erforderlich sind, zum anderen, ob Antworten auch personenbezogen erteilt werden können, und in diesem Zusammenhang, wann Angaben hinreichend anonymisiert sind und welche Möglichkeiten der Reidentifizierung dabei beachtet werden müssen.

Inhaltlich ging es um die Frage, ob allen Ausschussmitgliedern die Möglichkeit hinreichend bekannt sei, für die Teilnahme an Sitzungen Kinderbetreuungskosten beantra-

gen zu können. Dazu wurde u.a. gefragt, in welcher Weise das Bezirksamt Antragsberechtigte auf diese Möglichkeit aufmerksam mache. Es wurde aber auch gefragt, wie oft die Regelung in den Jahren 2011 bis Mai 2013, aufgelistet nach Monaten, Anzahl der gezahlten Entschädigungen pro Kind sowie Status und Geschlecht der/des Beantragenden, in Anspruch genommen worden sei.

Die erbetene tabellarische Beantwortung listete ohne Namensnennung die Inanspruchnahmen pro Kind pro Monat, einschließlich Status und Geschlecht des Elternteils, auf. Sie wurde turnusmäßig an den Fragesteller, das Präsidium, die Fraktionsbüros und Fraktionsvorsitzenden und an alle Mitglieder der Bezirksversammlung versandt. Üblicherweise erfolgt auch eine Veröffentlichung im Internet über das Ratsinformationssystem unter Beachtung der Datenschutzvorschriften. Auch Ausschussprotokolle werden darin veröffentlicht, soweit in öffentlicher Sitzung getagt wurde.
Die Antwort auf diese Anfrage wurde zunächst ohne die Tabelle veröffentlicht, da uns dazu eine Anfrage eines Mitglieds der Bezirksversammlung erreichte:

Schon die Formulierung der Anfrage lasse erkennen, dass es ein unzureichendes Wissen zu hinreichender Anonymisierung gebe. Es sei ihm anhand der Angaben ohne Schwierigkeiten möglich, seinen Fraktionskollegen auf den Kopf zuzusagen, wo sie in der Tabelle zu finden seien; aufgrund der öffentlich zugänglichen Ausschussprotokolle dürfte dies auch mit wenig Aufwand für die gesamte Tabelle gelten.

Diese Auffassung teilen wir im Ergebnis:
§ 24 BezVG regelt das Recht der Mitglieder der Bezirksversammlung, Große und Kleine Anfragen zu stellen. Nach Absatz 2 hat eine Beantwortung zu unterbleiben, soweit gesetzliche Vorschriften oder berechtigte Interessen Einzelner entgegenstehen. Diese sind regelmäßig schon dann betroffen, wenn Datenschutzregelungen nicht eingehalten werden. Dies ist auch dann der Fall, wenn die Antwort keinen Personenbezug erfordert und die an sich unter das Datengeheimnis fallenden personenbezogenen Angaben nicht hinreichend anonymisiert werden.

Die Frage, ob den Ausschussmitgliedern die Möglichkeit, Betreuungskosten geltend zu machen, hinreichend bekannt ist, kann auch ohne die vollumfängliche Bewilligungspraxis seit 2011 beantwortet werden. Die Bezirksverwaltung hat zu prüfen, ob unter dem Aspekt der Datensparsamkeit auf personenbezogene und personenbeziehbare Angaben verzichtet werden muss. Dies geschieht typischerweise durch Verzicht auf die Namensnennung und durch Aggregierung von Fallzahlen auf drei und größer, reicht aber nicht in jedem Falle aus.
Wie der Petent im vorliegenden Fall eindrücklich beschrieb, sind die berechtigten Interessen der Betroffenen nicht schon dadurch gewahrt, dass die Fragen ohne Namensnennung beantwortet wurden. Denn je kleiner der Betroffenenkreis ist, je mehr Einzelaussagen getroffen werden und je mehr Zusatzwissen erreichbar ist, desto eher sind Rückschlüsse auf konkrete Personen und damit eine Reidentifizierung möglich.

Dies ist besonders beachtlich bei einer Veröffentlichung im Internet, da darüber eine nicht überschaubare Anzahl von Adressaten mit erreicht wird.

Zu einem anderen Ergebnis führt auch nicht § 13 Abs. 2 Nr. 8 HmbDSG, der eine Verarbeitung für andere Zwecke zulässt, wenn sie der Beantwortung von Eingaben sowie von Kleinen und Großen Anfragen dient. Die Vorschrift ist von der Bürgerschaft für eigene Zwecke eingeführt worden und dient zunächst nur der Auswertung vorhandener Daten und Übermittlung der – auch personenbeziehbaren – Ergebnisse vom Senat an die Bürgerschaftsverwaltung. Die weitere Verarbeitung erfolgt nach dortigen bereichsspezifischen Vorschriften und in dortiger Verantwortung. Zur Stärkung des echten parlamentarischen Kontrollrechts der Bürgerschaft regeln § 7 der Datenschutzordnung der Bürgerschaft und § 13 Abs. 2 Nr. 8 HmbDSG abweichend von § 24 BezVG, dass Verarbeitung und Veröffentlichung erst dann zu unterbleiben haben, wenn überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen.

Wir haben daher gebeten, die Bezirksversammlungsmitglieder dahingehend zu sensibilisieren, die berechtigten Interessen der Betroffenen zu berücksichtigen und schon bei der Formulierung der Anfragen auf unnötige Detaillierungen zu verzichten, und die Bezirksverwaltung, stärker auf mögliche Reidentifizierungsmöglichkeiten zu achten. Dabei haben wir nochmals darauf hingewiesen, dass die der Bürgerschaft zustehenden weitergehenden Frage- und Veröffentlichungsrechte auf die Bezirksversammlung und ihre Ausschüsse nicht anwendbar sind.

16.2 Online-Übertragungen aus Sitzungen der Bezirksversammlungen

Soll die Öffentlichkeit von Sitzungen der Bezirksversammlungen und ihrer Ausschüsse durch Online Übertragungen unterstützt werden, bedarf es hierfür entsprechender Ermächtigungen im Bezirksverwaltungsgesetz. Bis dahin ist die wirksame Einwilligung aller Betroffenen erforderlich. Die Einrichtung des Verfahrens ist einer Vorabkontrolle zu unterziehen. Sie kann nicht dadurch umgangen werden, dass die einzelnen Abgeordneten ihre Beiträge zur Veröffentlichung bestimmen.

Bereits seit längerem werden Bedarfe nach moderneren Kommunikationsformen von den Gemeindeverwaltungen kommuniziert und von den Datenschutzbeauftragten bundesweit begleitet. Dies gilt besonders für die Übertragungen von Gemeinderatssitzungen im Internet. Dabei kann es sich um sog. Live-Streams handeln, bei denen Sitzungen in Echtzeit übertragen werden, oder aber um gespeicherte Aufnahmen, die der Allgemeinheit jederzeit zum Abruf zur Verfügung stehen.

Uns hatte schon 2011 eine Anfrage der behördlichen Datenschutzbeauftragten der Be-

zirksämter erreicht, unter welchen Voraussetzungen eine entsprechende Übertragung von Sitzungen der Bezirksversammlungen durch die Bezirksverwaltung möglich sei.

Die Rechtsprechung zur Rundfunk- und Pressefreiheit im Verhältnis zu Persönlichkeitsrechten der Betroffenen ist umfänglich und hat u.a. ergeben:
Der Unbefangenheit des gesprochenen Wortes kommt für den politischen Meinungsbildungsprozess eine hohe Bedeutung zu (Bundesverwaltungsgericht, Urteil vom 03.08.1990, BVerwGE 85, 283; NJW 1991, 118). Es ist anerkannt, dass Ton- und erst recht Bildaufzeichnungen des gesprochenen Wortes die Betroffenen in ihren Persönlichkeitsrechten berühren (Bundesverfassungsgericht (BVerfG), Beschluss vom 14.07.1994, http://connect.juris.de/jportal/portal/t/gec/page/jurisw.psml?pid=Dokumentanzeige&showdoccase=1&js_peid=Trefferliste&documentnumber=1&numberofresults=2&fromdoctodoc=yes&doc.id=KVRE253519401&doc.part=L&doc.price=0.0&doc.hl=1#focuspoint, Urteil vom 24.01.2001, RN 80 ff, http://www.bundesverfassungsgericht.de/entscheidungen/rs20010124_1bvr262395.html).

Dies gilt nach der Rechtsprechung auch für Mitglieder von Gemeinderäten und ist unter Wahrung des Verhältnismäßigkeitsgrundsatzes mit der Rundfunk- und Pressefreiheit abzuwägen (zuletzt Oberverwaltungsgericht des Saarlandes, Beschluss vom 30.08.2010, unter Verweis auf das o.a. Urteil des BVerfG, http://connect.juris.de/jportal/portal/t/32gd/page/jurisw.psml?pid=Dokumentanzeige&showdoccase=1&js_peid=Trefferliste&documentnumber=1&numberofresults=2&fromdoctodoc=yes&doc.id=MWRE100002498&doc.part=L&doc.price=0.0&doc.hl=1#focuspoint). Betroffen sind darüber hinaus auch Mitarbeiter und Besucher.

Entscheidungen über die Anforderungen eines eigenen Online-Angebots der Verwaltung liegen bisher nicht vor.

Die Bezirksversammlung ist nach § 3 des Bezirksverwaltungsgesetzes (BezVG) Teil des Bezirksamtes und damit Teil der Exekutive. Sie kann damit den Grundsatz der Öffentlichkeit nicht in demselben Umfang für sich reklamieren wie Bundes- und Landesparlamente (Jarass/Pieroth, Grundgesetz für die Bundesrepublik Deutschland, Artikel 20 RN 13), sondern unterliegt als Verwaltungsausschuss bei der Wahrnehmung ihrer Aufgaben den datenschutzrechtlichen Bestimmungen des Bezirksverwaltungsgesetzes (BezVG) und ergänzend denen des Hamburgischen Datenschutzgesetzes (HmbDSG). Die Übertragung ins Internet stellt rechtlich eine Übermittlung an Stellen außerhalb des öffentlichen Bereiches dar. Da das BezVG bisher keine hinreichenden Regelungen trifft, sind die Möglichkeiten und Grenzen des HmbDSG zu beachten.

Die Übertragung von Sitzungen der Bezirksversammlungen als verwaltungseigenes Angebot kommt daher zur Zeit nur mit vorheriger informierter schriftlicher Einwilligung der Betroffenen in Betracht. Die Teilnahme zumindest von Besuchern muss auch möglich sein, wenn sie in eine Übertragung nicht einwilligen. Dies kann durch Beschrän-

kung der Kameraführung auf das Rednerpult geschehen oder durch Ausweisen von Plätzen außerhalb des Aufnahmewinkels. Soweit Aufnahmen längerfristig abrufbar sein sollen, ist auch zu gewährleisten, dass ein Widerruf der Einwilligung datenschutzgerecht umgesetzt werden kann.

Eine Anfrage der Bezirksversammlung Altona aus dem Jahre 2012 haben wir entsprechend beantwortet und ergänzend auf die erforderliche Vorabkontrolle nach § 8 HmbDSG hingewiesen. Die Bezirksversammlung berief sich anschließend auf § 2 Abs. 6 HmbDSG und machte geltend, dass das Gesetz keine Anwendung finde, da die Redeaufzeichnungen von den Betroffenen zur Veröffentlichung bestimmt worden seien.

Diese extensive Auslegung würde bedeuten, dass die gegenwärtige Bestimmung den Betroffenen jede Möglichkeit nimmt, auch für künftige Zeiten und Zusammenhänge Einfluss auf die Datenverarbeitung zu nehmen. Darüber hinaus wären auch technisch-organisatorische Maßnahmen zur Datensicherung nicht zu treffen, und den Betroffenen stünde die Anrufung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit nicht zur Verfügung.

Wir konnten diese Auffassung nicht teilen:

Zum einen sind auch Mitarbeiter und Besucher betroffen, letztere zumindest, wenn sie sich an öffentlichen Fragestunden beteiligen. Über ihre Rechte können die Mitglieder der Bezirksversammlung nicht wirksam verfügen.

Maßgeblich ist jedoch, dass die aus dem Jahre 1990 stammende Regelung gegen die Anforderungen der EG-Datenschutzrichtlinie aus 1995 verstößt, die mit der Novellierung 2001 umzusetzen war:

Für den hier betroffenen Fall bestimmt die Richtlinie, dass nur die ausschließlich für private oder familiäre Tätigkeiten bestimmte Datenverarbeitung nicht unter ihren Anwendungsbereich fällt. Diese Grenze ist mit der Ausübung eines öffentlichen Ehrenamtes und den Intentionen der Abgeordneten, mehr Bevölkerungsnähe zu erreichen und den Bekanntheitsgrad bei der vorgeschriebenen Direktwahl zu erhöhen, ersichtlich überschritten. Eine richtlinienkonforme Auslegung führt daher zur Anwendung des HmbDSG.

Eine Umfrage in den Ländern, die eine ähnliche Regelung noch enthalten, hat ergeben, dass die Vorschrift dort auch nicht mehr angewendet wird; in Hessen wurde vielmehr parallel eine ausdrückliche Regelung zur Übertragung von Gemeinderatssitzungen im Internet geschaffen.

Aber auch die ursprüngliche Gesetzesbegründung stützt die weite Auslegung durch die Bezirksversammlung nicht:

Danach soll die Verarbeitung nur insoweit erleichtert werden, als Daten bereits allgemein zugänglich sind und privilegiert damit letztlich nur die Erhebung durch Behörden. Sobald Daten in Verwaltungsvorgänge Eingang gefunden haben, gilt für sie das Hamburgische Datenschutzgesetz. Als Anwendungsbereiche werden Zeitungen, Adress- und Telefonbücher benannt, und als vergleichbar werden veröffentlichte Interviews angesehen. Diese werden jedoch typischerweise vor ihrer Veröffentlichung von den Betroffenen freigegeben.

Darüber hinaus stellt Live-Streaming eine unmittelbare, nicht korrigierbare Herausgabe von Informationen dar und verfügt über eine besondere Qualität, die über sonstige Veröffentlichungen hinausgeht und irreversibel ist. Der Abschirmung vor möglichen Beeinträchtigungen des Persönlichkeitsrechts, insbesondere durch technisch-organisatorische Maßnahmen, dient das HmbDSG mit der geforderten Einwilligungslösung.

Im Ergebnis befürworten wir eine bereichsspezifische Regelung im BezVG.
Bis zu ihrem Erlass kann eine Übertragung der Sitzungen der Bezirksversammlungen aufgrund einer Einwilligungslösung erfolgen. Dies würde zum Beispiel bedeuten, dass bei fehlender Einwilligung technisch eine jederzeitige Aussetzung der Übertragung bzw. Aufnahme möglich ist und dass Aufzeichnungen im Falle eines Widerrufs der Einwilligung umgehend gelöscht werden.

16.3 Videoüberwachung in öffentlichen Toiletten

Die Videoüberwachung öffentlicher Toiletten ist kein geeignetes Mittel, die Sicherheit des dort eingesetzten Reinigungspersonals zu erhöhen. Die Aufnahme von Toilettenbereichen berührt die Intimsphäre der Betroffenen und ist daher unzulässig.

Im Sommer 2013 haben wir durch eine Eingabe erfahren, dass in einer öffentlichen Toilette, die vom Bezirksamt Mitte betrieben wurde, Videoüberwachung stattfinde.

Die Videoüberwachung dort und in fünf anderen Toilettenanlagen wurde damit begründet, dass das vor Ort beschäftigte Personal einer beauftragten Firma in der Vergangenheit tätlichen Angriffen ausgesetzt gewesen sein solle, was in einem Fall sogar zur Schließung der Toilettenanlage geführt habe. Alle Kameras seien auf die Drehkreuze im Eingangsbereich gerichtet, zeichneten nicht auf und seien nicht mit einer Alarmanlage verbunden. Die Übertragung erfolge in den Mitarbeiterraum. Handele es sich um Kinder, die das Drehkreuz übersteigen oder ähnlich harmlose Vorfälle, könne das Personal einschreiten; in gefährlicheren Situationen mit gewaltbereitem Klientel oder bei zu erwartenden Beleidigungen könne das Personal zu seinem Schutz im Aufenthaltsraum verbleiben.

Wir haben uns alle Anlagen angesehen und mussten feststellen, dass einige Kameras nicht nur den Eingangsbereich und die Drehkreuze, sondern zum Teil auch Toilettenräume, Stehbecken und die Handwaschbecken beobachteten.

Nach weiteren Erörterungen haben wir das Bezirksamt gebeten, die Videoüberwachung insgesamt einzustellen.

Die Überwachungsmaßnahmen an sich waren angesichts der konkreten Arbeitssituation und der konkreten Ausgestaltung der Überwachung nicht geeignet, den Schutz der Mitarbeiter zu erhöhen, und sie waren vor allem sowohl hinsichtlich der Aufnahme der Toilettenräume unverhältnismäßig angesichts des Eingriffs in die Intimsphäre der Betroffenen und hinsichtlich der Aufnahme der Drehkreuze angesichts der Tatsache, dass es möglich ist, das Umgehen der Zahlung durch bauliche Mittel zu unterbinden.

Die Überwachung von öffentlich zugänglichen Umkleide-, Dusch- und Toilettenräumen berührt regelmäßig die Intimsphäre der Betroffenen. Damit werden in besonderem Maße die schutzwürdigen Interessen der Betroffenen berührt. Sie ist daher grundsätzlich unzulässig.

Auch bei Ausrichtung der Kameras auf den Eingangsbereich erscheint eine Videoüberwachung für den angegebenen Zweck ungeeignet: Tatsächlich gestaltet sich die Arbeitssituation so, dass die Mitarbeiter vor allem mit der Reinigung der Toiletten beschäftigt sind und sich daher wenig im Mitarbeiterraum aufhalten und den Monitor beobachten können. In der überwiegenden Zeit sind sie also gar nicht in der Lage, durch die Videobeobachtung eventuelle Übergriffe oder Belästigungen zu erkennen, geschweige denn ihnen zu entgehen.

Die Zielrichtung der Kameras und auch die gemeldeten Vorfälle ließen vielmehr darauf schließen, dass damit in erster Linie die Gebührenzahlung überwacht werden soll. Videoüberwachung ist aber grundsätzlich nur dann zulässig, wenn sie verhältnismäßig ist und insbesondere keine milderen Mittel zur Erreichung des verfolgten Zwecks zur Verfügung stehen. In den Anlagen waren jedoch Drehkreuze installiert, durch die normal gebaute Personen sich ohne Schwierigkeit hindurchzwängen können, wie auch vom Reinigungspersonal demonstriert wurde. Zur Vermeidung von Gebührenverlusten in dieser Größenordnung ist es daher zumutbar, auf mildere Mittel wie manipulationssichere Drehkreuze zurückzugreifen, wie sie in anderen Toilettenanlagen privater Betreiber bereits eingesetzt werden.

Die Überlegung, dass Toiletten in Tiefgeschossen eine tendenziell größere Gefährdung für die Beschäftigten bedeuten und mit der bloßen Beobachtung ein relativ geringer Eingriff in die Rechte der Betroffenen verbunden ist, führt zu keinem anderen Ergebnis. Selbst bei einer baulichen Veränderung der Drehkreuze und einer Beschränkung der Kameras auf den Eingangsbereich wäre die Gefährdung nicht wesentlich verringert,

ist doch die Tendenz, in unbewachte Bereiche auszuweichen, auch aus anderen Verwendungszusammenhängen hinreichend bekannt.

Schließlich mussten wir dem Bezirksamt auch mitteilen, dass eine Videoüberwachung durch die Mitarbeiter einer beauftragten Firma als Auftragsdatenverarbeitung bewertet werden muss und diese schon aus rechtlichen Grüßen nicht zulässig ist.

Bis Dezember 2013 sind alle Überwachungsanlagen stufenweise abgebaut worden.

17. Statistik

17.1 Registergestützte Volkszählung – Zensus 2011

Noch sind nicht sämtliche Hilfsmerkmale gelöscht. Wir setzen uns weiterhin für die frühestmögliche Löschung dieser Daten ein.

Wir haben die Volkszählung von Anfang an intensiv und kritisch begleitet (vgl. 21. TB, 5.2, 23. TB, III 19.1). In einer eigens für den Zensus 2011 einberufenen Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder wurden Datenschutzaspekte diskutiert und datenschutzrechtliche Forderungen gegenüber dem Gesetzgeber und der amtlichen Statistik erhoben, welchen - wie berichtet - nicht allen nachgekommen wurde. Nach Vorgaben der EU soll im Jahr 2021 die nächste Volkszählung durchgeführt werden. Anlässlich der Veröffentlichung der ersten Zensusergebnisse und Bekanntgabe der ermittelten Bevölkerungszahlen am 31. Mai 2013 wurde vom Bundesbeauftragten für Datenschutz und Informationsfreiheit ein Eckpunktepapier mit datenschutzrechtlichen Forderungen im Hinblick auf einen Zensus 2021 veröffentlicht. In dieses sind die Ergebnisse der in der Bund-Länder-Arbeitsgruppe diskutierten Fragestellungen und Erfahrungen zum Zensus 2011 eingeflossen. Das Eckpunktepapier kann unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/EckpunktepapierZensus2021.html?nn=408908 eingesehen werden.

Mit dem Zensusstichtag, dem 09. Mai 2011, hatte die Phase der Datenerhebung begonnen. Zu diesem Stichtag übermittelten nicht nur Verwaltungsbehörden, wie etwa die Meldebehörden oder die Bundesagentur für Arbeit ihre Datensätze an die Statistischen Ämter, sondern auch die Befragungen der Bürger begannen an diesem Tag. Im Rahmen der Gebäude- und Wohnungszählung wurden sämtliche Eigentümer und Verwalter von Gebäuden und Wohnungen postalisch befragt. In der ergänzenden Haushaltsstichprobe erfolgte in Hamburg die Befragung von etwa 62.500 Bürgern. Außerdem wurden direkt vor Ort die Daten der Bewohner von Gemeinschaftsunterkünften und der Insassen von Justizvollzugsanstalten erhoben. Im Frühsommer 2012 waren die Erhebungen einschließlich aller Rückfragen und vorgesehenen Wieder-

holungsbefragungen abgeschlossen und die Erhebungsstellen wurden geschlossen. Während der Erhebungsphase haben sich viele Bürger mit Fragen und Eingaben an uns gewandt, weil sie durch die Befragungen ihr Recht auf informationelle Selbstbestimmung verletzt sahen. Über während der Erhebungsphase aufgetretene Probleme und Fragestellungen, wie etwa den unberechtigten Versand von Erinnerungsschreiben und uneinheitliche Auskunftsansprüche hatten wir bereits im letzten Tätigkeitsbericht informiert. Gravierende datenschutzrechtliche Mängel konnten durch uns hier jedoch nicht festgestellt werden. Nach Abschluss der Erhebungen haben die Statischen Ämter des Bundes und der Länder mit der Aufbereitung und Auswertung der Zensusdaten begonnen. Dabei kamen nach dem Zensusgesetz einzelnen Statistikämtern im Rahmen des sogenannten Statistischen Verbundes besondere Aufgaben zu. So oblag etwa dem Statistischen Bundesamt der Aufbau einer Referenzdatenbank. Andere Statistikämter waren für die Entwicklung und Bereitstellung von Software und Auswertungsdatenbanken für bestimmte Zensusbereiche zuständig.

Nach Abschluss der Erhebungsphase liegt aus datenschutzrechtlicher Sicht besonderes Augenmerk auf der Einhaltung der gesetzlichen Löschfristen, insbesondere für die Hilfsmerkmale. Hilfsmerkmale sind Angaben, die der technischen Durchführung der Statistik dienen, wie beispielsweise der Name und die Anschrift einer Person. Diese sind zum frühestmöglichen Zeitpunkt von den eigentlichen, dauerhaft gespeicherten statistischen Daten, den sogenannten Erhebungsmerkmalen, zu trennen. Sie müssen gelöscht werden, sobald die Überprüfung der Erhebungsdaten auf ihre Vollständigkeit und Schlüssigkeit hin erfolgt ist und sie für die Durchführung und Kontrolle der Erhebungen nicht mehr benötigt werden. Die Löschung der Hilfsmerkmale und Erhebungsunterlagen hat nach § 19 Zensusgesetz 2011 spätestens vier Jahre nach dem Berichtszeitpunkt (09. Mai 2011) zu erfolgen. Zentrale Frage ist dabei, ab wann die Hilfsmerkmale für die Durchführung und Kontrolle der Erhebungen nicht mehr erforderlich sind. Wir haben vom Statistischen Amt für Hamburg und Schleswig-Holstein ein Löschkonzept angefordert, um Klarheit über das Verfahren zur Löschung der Hilfsmerkmale zu erhalten und diese überwachen zu können. Das Statistische Amt hat eine Übersicht über den Stand der Datenlieferungen, Datenbestände und Löschungen erstellt, anhand derer der jeweils aktuelle Stand der Löschungen festgestellt werden kann. Leider kam es u.a. aufgrund von verspätet fertig- und bereitgestellten Softwareprogrammen im Statistikverbund immer wieder zu Verzögerungen bei der Aufbereitung der Zensusdaten. Daher konnte insbesondere der mit den Datenschutzbeauftragten vereinbarte frühzeitige Löschtermin (31.Dezember 2011) für die Hilfsmerkmale bei den Erhebungen in den sensiblen Sonderbereichen nicht eingehalten werden. Die Löschung erfolgte erst im Spätsommer 2012.

Wir stehen seit Beginn des Zensus 2011 mit dem Statischen Amt in engem Kontakt. Dabei haben wir in vielen Gesprächen datenschutzrechtliche und technische Fragestellungen bei der Durchführung des Zensus 2011 behandelt. Wir lassen uns regelmäßig über den aktuellen Sachstand bezüglich der Löschungen der Hilfsmerkmale

unterrichten und werden den Fortgang der Löschungen auch weiterhin überwachen. Bei den Erörterungen zum Zensus 2011 zeigte das Statistische Amt erfreulicherweise insgesamt ein hohes Maß an Sensibilität für die Belange des Datenschutzes. Noch nicht abgeschlossen werden konnten Erörterungen hinsichtlich zusätzlicher Sicherungsmöglichkeiten des Zugangs zu zentralen Zensusanwendungen (Filterung der zugriffsberechtigten FHH-Nutzer). Hier sehen wir auch im Hinblick auf zukünftige Anwendungen noch Optimierungsbedarf.

17.2 Landesinformationssystem (LIS)

Das Statistische Amt für Hamburg und Schleswig-Holstein hat unsere datenschutzrechtlichen Bedenken aufgegriffen und mit dem Aufbau eines Sicherheitsmanagements einen richtigen Weg eingeschlagen.

Im letzten Tätigkeitsbericht (23. TB, III 19.2) hatten wir ausführlich über die geplante Einführung eines Landesinformationssystems (LIS) durch das Statistische Amt für Hamburg und Schleswig-Holstein berichtet. Das LIS ist ein datenbankgestütztes, statistisches Informationssystem zur zentralen Speicherung und Auswertung von Statistikdaten, welches verschiedenen Nutzergruppen die individuelle Auswertung von Statistikdaten mittels einer grafischen Benutzeroberfläche ermöglichen soll. Die Daten werden in die „LIS-Kernapplikation" aus Anwendungen der amtlichen Statistik übernommen. Der Zugriff der Mitarbeiter erfolgt über Clients im Statistikamt an den Standorten Kiel und Hamburg. Darüber hinaus werden aggregierte Daten für die Öffentlichkeit in einer sogenannten „LIS-Onlinedatenbank" zum Abruf bereitgestellt. Unsere datenschutzrechtlichen Bedenken insbesondere hinsichtlich der Konzeption der Datenbereitstellung im Internet wurden durch das Statistische Amt aufgegriffen und führten zu konzeptionellen Veränderungen des Verfahrens dahingehend, dass

- für die Online-Datenbank eine vom Kern-LIS getrennte Datenbank vorgesehen ist, in welche nun nur explizit vom Fachgebiet freigegebene Daten (selektive Replikation) für die Veröffentlichung übernommen werden.
- die Online-Datenbank ausschließlich aggregierte Daten enthält.
- vor Einstellung in die Online-Datenbank die vom Fachbereich selektierten Daten vom Fachbereich erneut hinsichtlich der Gewährleistung der statistischen Geheimhaltung überprüft und ggf. weitere erforderliche Aggregationen oder Löschungen vorgenommen werden.
- die übergreifende Prüfung von Einzelfreigaben auf die Einhaltung von Datenschutz und statistische Geheimhaltung durch die Fachliche Leitstelle erfolgt.
- der zusätzliche Einsatz von Geheimhaltungstools zur Gewährleistung der statistischen Geheimhaltung geplant ist.
- die Verantwortlichkeiten, Zuständigkeiten und Abläufe für die jeweiligen Verfahrensschritte festgelegt und dokumentiert wurden.

Das für das Verfahren LIS erstellte Sicherheitskonzept orientiert sich am IT-Grundschutz des Bundesministeriums für Sicherheit in der Informationstechnik (BSI). Diese Orientierung soll beibehalten und für weitere Verfahren des Statistikamtes übernommen werden.

Das Statistische Amt für Hamburg und Schleswig-Holstein beauftragte das Unabhängige Landeszentrum für Datenschutz (ULD) mit der Erstellung eines Gutachtens zu Datenschutz und Datensicherheit des Verfahrens Landesinformationssystem (LIS) auf der Basis des IT-Grundschutzstandards des Bundesamtes für Sicherheit in der Informationstechnik. Die Begutachtung umfasste die Prüfung der Dokumentation nach den Anforderungen des Grundschutzstandards, die Vorort-Prüfung über den ordnungsgemäßen Einsatz des LIS beim Statistikamt Nord, die Überprüfung des Auftragnehmers Dataport im Rahmen der Auftragsdatenverarbeitung (Begutachtung der Dokumentation und die stichprobenartige Prüfung der Umsetzung von Grundschutzmaßnahmen vor Ort) sowie die datenschutzrechtliche Bewertung des Verfahrens, welche gemeinsam mit dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit erfolgte. Das Gutachten kam zu dem Ergebnis, dass die Anforderungen des Grundschutzstandards dahingehend erfüllt werden, dass das Sicherheitsmanagement beim Statistischen Amt und bei Dataport aktiv ist. Zuständigkeiten und Verantwortlichkeiten für den sicheren Betrieb des Verfahrens sind auf Seiten des Statistischen Amtes und Dataport festgelegt. Diese werden praktisch umgesetzt und die eingesetzten IT-Komponenten nach den Grundschutzanforderungen betrieben.

Im Oktober 2012 erfolgte die Produktivsetzung des Verfahrens „LIS-Online". Die Planung des Extranets, über welches die Bereitstellung statistischer Einzeldatensätze für andere Behörden erfolgen sollte, hat das Statische Amt aufgrund unserer rechtlichen Hinweise zurückgestellt.

Positiv hervorzuheben ist auch, dass das Statistische Amt durch weitere Maßnahmen (wie z.B. die Durchführung von Penetrationstests) zeigt, dass die Sicherheitsproblematik als Aufgabe erkannt und wahrgenommen wird. Solche Maßnahmen können zur Aufdeckung von Schwachstellen führen, die dann umgehend abgestellt werden können und auch sollten. Wir werden diesbezüglich weiter mit dem Statistischen Amt im Gespräch bleiben.

18. Personenstandswesen

18.1 Elektronisches Personenstandsregister

Bei der gemeinsamen Nutzung einer IT-Infrastruktur durch verschiedene Daten verarbeitende Stellen muss eine rechtlich zwingend erforderliche Trennung der Daten durch technische Maßnahmen konsequent umgesetzt werden.

Durch das in Kraft getretene modernisierte Personenstandsgesetz (PStG) und die Verordnung zur Ausführung des Personenstandsgesetzes (PStV) wurden im Personenstandswesen die Grundlagen für den Wechsel von der papiernen zur elektronischen Registerführung gelegt. Die elektronische Registerführung ist bereits seit 2009 erlaubt und ab 2014 für die Standesämter verbindlich vorgeschrieben. Wie im 23. Tätigkeitsbericht (III 17.2) dargestellt, hat Hamburg gemeinsam mit Schleswig-Holstein und Bremen den Dienstleister Dataport ländertübergreifend mit der Entwicklung und dem Betrieb des Verfahrens Elektronisches Personenstandsregister beauftragt. Die uns vorgelegte Konzeption sah für die drei Bundesländer keine getrennten Verfahren, sondern die gemeinsame Nutzung einer Infrastruktur und eines Verfahrens in einem Rechenzentrumsbetrieb vor. Die personenstandsrechtlich vorgeschriebene zwingende Trennung der Standesamtsdaten der beteiligten Bundesländer, aber auch der einzelnen Standesämter eines Landes, sollte durch mandantenorientierte, technische und organisatorische Regelungen umgesetzt werden. Hierzu haben wir folgende Auffassung vertreten: Eine Datenverarbeitung verschiedener Daten verarbeitender Stellen muss nicht zwingend in getrennten Verfahren durchgeführt werden. Auch die Verarbeitung in einem mandantenfähigen System kann grundsätzlich datenschutzgerecht und gesetzeskonform erfolgen, jedoch setzt dies voraus, dass die zwingende Datentrennung durch ausreichende technische Maßnahmen gewährleistet ist. Das bedeutet z.B., dass rechtlich nicht zulässige übergreifende Zugriffe technisch ausgeschlossen sind und nicht nur über organisatorische Maßnahmen gewährleistet werden. Im Dezember 2011 teilten wir den Auftraggebern und dem Projekt gemeinsam mit den Datenschutzbeauftragten der Länder Bremen und Schleswig-Holstein mit, dass die vorgelegte Konzeption die an die gesetzlich vorgegebene Datentrennung zu stellenden Anforderungen nicht erfüllt und forderten diese auf, anhand der von uns schriftlich dargelegten Kriterien zur Mandantenfähigkeit darzustellen, wie diese umgesetzt werden sollen.

Ohne dass zuvor auf die von den Landesdatenschutzbeauftragten geäußerten datenschutzrechtlichen Bedenken hinsichtlich der technischen Konzeption des Verfahrens inhaltlich eingegangen wurde, wurde das IT-Verfahren im Januar 2012 in den hamburgischen Standesämtern ausgerollt und produktiv gesetzt. Daraufhin haben wir in einem gemeinsamen Gespräch mit dem Staatsrat der Behörde für Inneres und Sport (BIS) sowie den zuständigen Amtsleitungen bzw. Fachamtsleitungen der BIS, der Finanzbehörde und des Bezirksamtes Nord die Vorgänge im Vorfeld der Produk-

tivschaltung erörtert und eine rechtskonforme Gestaltung des IT-Verfahrens eingefordert. Es wurde vereinbart, auf Arbeitsebene anhand einer Gegenüberstellung der von den Datenschutzbeauftragten aufgestellten Anforderungen und der vom Projekt geplanten Maßnahmen die Frage der Mandantenfähigkeit und darauf aufsetzend der Rechtmäßigkeit des Verfahrens zu vertiefen, um daraus die notwendigen noch zu treffenden technischen und organisatorischen Maßnahmen abzuleiten. Vor diesem Hintergrund wurde von der Einleitung einer förmlichen Beanstandung gem. § 25 Abs. 2 HmbDSG abgesehen.

Im Rahmen dieser Erörterungen wurde deutlich, dass es weder ein einheitliches Verständnis des Begriffs Mandantentrennung gab, noch dass detaillierte, allgemeingültige Vorgaben für eine datenschutzgerechte Ausgestaltung von mandantenfähigen Systemen schriftlich fixiert waren. Aus diesem Grunde wurde von den Datenschutzbeauftragten des Bundes und der Länder die „Orientierungshilfe Mandantenfähigkeit" erarbeitet (s. II 1.), welche im Oktober 2012 vom AK Technik einstimmig verabschiedet und im November 2012 von der Datenschutzkonferenz zustimmend zur Kenntnis genommen wurde.

Im Hinblick auf das Verfahren Elektronisches Personenstandsregister wurde das Erfordernis einer technischen Änderung in Bezug auf die Vergabemöglichkeiten standesamtsübergreifender Berechtigungen erkannt. Die Einrichtung unzulässiger übergreifender Zugriffsmöglichkeiten darf nicht nur durch organisatorische Maßnahmen verhindert, sondern muss auch technisch durch das System ausgeschlossen werden. Für eine entsprechende Systemänderung wurde ein Change Request erstellt und für die Ländertrennung umgesetzt.

Im Oktober 2013 ist die Hamburgische Verordnung über ein zentrales Personenstands- und Sicherungsregister (HmbzPSRVO) in Kraft getreten, mit der nunmehr die gemeinsame Verarbeitung der Daten der hamburgischen Standesämter in einem zentralen Register legitimiert ist. Damit ist eine Mandantentrennung bezüglich der hamburgischen Standesämter untereinander nicht mehr erforderlich.

Während der Abstimmungsprozesse haben wir wiederholt daraufhin hingewiesen, dass der Verfahrensdokumentation nicht immer deutlich zu entnehmen ist, welche Einstellungen für welches Land vorgesehen und umgesetzt sind, und um Übersendung angepasster Unterlagen gebeten. Diese angeforderten Unterlagen liegen bislang nicht vor.

Eingefordert haben wir zudem eine frühzeitige Beteiligung bei der Erarbeitung einer Konzeption für die Umsetzung der nach § 26 PStV vorgesehenen Suchfunktion für Standesämter anderer Bundesländer. Auch hier müssen die Ausgestaltungsmöglichkeiten und -grenzen einer Suchfunktion in mandantenfähigen Systemen berücksichtigt werden. Da eine Umsetzung durch die Erteilung von übergreifenden Zugriffsrechten die erforderliche Mandantentrennung zwischen den Bundesländern aufheben würde,

muss eine andere technische Umsetzung der Abfragen abfrageberechtigter Standesämter beispielsweise über die Clearingstelle/Brokerdienste erfolgen.

18.2 Prüfung der Standesamtlichen Registerstelle mit dem Generalregister der Hamburgischen Standesämter

Wir haben kritisiert, dass bei der Zweitbuchführung aufgrund von Sparmaßnahmen datenschutzrechtliche Qualitätseinbußen in Kauf genommen wurden. Für das historisch gewachsene Verfahren Generalregister muss eine rechtskonforme Lösung gefunden werden.

Wie im letzten Tätigkeitsbericht (23. TB, III 17.3) dargestellt, wurden wir am 15. Juni 2011 durch die behördliche Datenschutzbeauftrage der Bezirke (N/DSB) und die Presse über eine unzulässige Entsorgung von standesamtlichen Unterlagen informiert. Mitteilungen verschiedener Standesämter an die Standesamtliche Registerstelle waren dort unbearbeitet in einem Müllcontainer entsorgt worden, wo sie von einem Bürger gefunden und einer Hamburger Tageszeitung zugespielt wurden. Aus Anlass dieser unzulässigen Entsorgung hatten wir am 16. Juni 2011 unter Einbeziehung von N/DSB ein Ad-hoc-Prüfungsverfahren bei der Standesamtlichen Registerstelle mit dem Generalregister der Hamburgischen Standesämter eingeleitet. Gegenstand der Prüfung waren bzw. sind Aufgaben und Arbeitsabläufe, einschließlich eingerichteter elektronischer Verfahren und die Feststellung des Umfangs und Ausmaßes des durch die unzulässige Entsorgung eingetretenen Schadens. Das Prüfverfahren war im Berichtszeitraum des 23. TB noch nicht abgeschlossen, daher hatten wir angekündigt und gehofft, die Ergebnisse der Prüfung im 24. TB abschließend darstellen zu können. Leider gestaltete sich bereits die Sachverhaltsaufklärung aber auch das weitere Prüfverfahren sehr schwierig und langwierig. Während einige Prüfungspunkte inzwischen abgeschlossen werden konnten, sind andere nach wie vor offen und klärungsbedürftig. Im Einzelnen:

▶ unzulässige Entsorgung von standesamtlichen Unterlagen:

Bei den unzulässig entsorgten Unterlagen handelte es sich um unbearbeitete Mitteilungen von Standesämtern zur Fortschreibung der Zweitbücher. Die im Müll aufgefundenen Dokumente wurden an die Registerstelle zurückgegeben. Ob es sich um einen Einzelfall gehandelt hat oder ob und in welchem Umfang darüber hinaus ein Schaden (Datenverlust) eingetreten ist, konnte nicht aufgeklärt werden. Nach fachlicher Einschätzung des Leiters der Registerstelle (N/STL) und der Behörde für Inneres und Sport (BIS) als Aufsichtsbehörde wäre hierfür ein Abgleich sämtlicher Erst- und Zweitbücher erforderlich, welcher nicht als verhältnismäßig erachtet werde und personaltechnisch nicht zu leisten sei. Wir haben darauf hingewiesen, dass wegen der zentralen Bedeutung der Personenstandsregister und des ihnen zuerkannten Beweiswertes die Tatsache, dass es für einen gewissen Zeitraum keine Gewähr für die Richtigkeit und Vollständigkeit der Zweitbücher gibt, zumindest dauerhaft und nachvollziehbar dokumentiert werden muss.

▶ Eingestellte Aktualisierung der Zweitbücher / Digitalisierungsverfahren:
Aufgrund von Personaleinsparungen wurden die standesamtlichen Mitteilungen (Fortführungen und Berichtigungen) ab 1997 durch die Registerstelle nicht mehr unverzüglich in die Zweitbücher umgesetzt, sondern zum Teil nur noch geordnet in Aktenordnern abgelegt. Eine Fortführung des jeweiligen Zweitbuches soll erst im Bedarfsfall (Untergang von Eintragungen im Erstregister) erfolgen. Seit 2009 wurden die Mitteilungen zu den Heirats-Zweitbüchern unpaginiert, nach Standesämtern, Jahrgängen und Registernummern sortiert, in der Registerstelle aufbewahrt und stehen für eine Aktualisierung der Zweitbücher jederzeit zur Verfügung. Da für die standesamtlichen Mitteilungen eine mindere Papierqualität verwendet wurde, wurden diese in regelmäßigen Abständen auf ihre Lesbarkeit hin überprüft und zu deren Erhalt fotokopiert. Die Mitteilungen der Standesämter zu den Geburten-Zweitbüchern wurden aufgrund des für eine Papierlagerung zu hohen Aufkommens in der Registerstelle digitalisiert. Die Mitteilungen wurden mittels eines netzwerkfähigen Kopierers eingescannt und sortiert auf dem normalen Gruppenlaufwerk abgelegt. Das Original wurde anschließend vernichtet. Die Verzeichnisse auf dem Gruppenlaufwerk wurden in unregelmäßigen Abständen auf CD gesichert. Lediglich die Sterbe-Zweitbücher werden aufgrund des geringen Aufkommens laufend aktualisiert.
Hier haben wir problematisiert, dass der Verzicht auf eine laufende Aktualisierung der Zweitbücher keine getreue Umsetzung der personenstandsrechtlichen Vorgaben darstellt, wonach die Zweitbücher unmittelbar nach erfolgten Eintragungen in die Erstbücher zu aktualisieren und jahrgangsweise abzuschließen sind. Die Reduzierung auf eine nur bedarfsweise Umsetzung der Einträge in den Zweitbüchern bzw. Sicherungsregistern ist nicht vorgesehen. Auch den Verlust der Urkundenqualität durch das Fotokopieren und Digitalisieren der Mitteilungen haben wir problematisiert. Für das Digitalisierungsverfahren konnten zudem weder eine Verfahrensbeschreibung und eine Risikoanalyse nach §§ 8,9 HmbDSG noch geregelte Handlungsanweisungen vorgelegt werden. Da somit keine ausreichenden technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten nachgewiesen werden konnten, wurde die Digitalisierung noch am Tag der Ad-hoc-Prüfung eingestellt. Die Mitteilungen für die Geburten-Zweitbücher werden seitdem ebenfalls sortiert aufbewahrt. Zu den von uns aufgezeigten Problemstellungen hat die BIS als zuständige Aufsichtsbehörde erklärt, dass auch sie die aufgrund von Sparzwängen eingeführte Vorgehensweise bei den Heirats- und Geburten-Zweitbüchern aus heutiger Sicht zwar als datenschutzrechtlich nicht optimal und gemessen an personenstandsrechtlichen Vorgaben auch als Qualitätseinbuße ansieht, aber aus fachlicher Sicht weiterhin für vertretbar hält, weil der Zweck der Zweitbuchführung, nämlich die Wiederherstellung eines in Verlust geratenen Erstbuches nicht gefährdet sei. Die notwendigen inhaltlichen Informationen seien in den abgehefteten und zum Erhalt der Lesbarkeit kopierten Mitteilungen bzw. in den Digitalisierungen vollständig vorhanden. Aus diesem Grund könne auf eine Nachholung der Aktualisierung (ggf. durch Nachbeurkundung) der Zweitbücher verzichtet werden, zumal diese unter Ressourcenaspekten nicht zu leisten sei. Wir haben die BIS darauf hingewiesen, dass diese Bewertung aus fachlicher Sicht bezüglich des

Verfahrens bei den Heirats-Zweitbüchern zwar vertretbar erscheinen mag, dass dies jedoch nicht für das Verfahren bei den Geburten-Zweitbüchern gilt, weil es sich beim Digitalisierungsverfahren nicht um ein geordnetes oder geregeltes Verfahren handelt, sondern um ein technisch unbegleitetes Verfahren ohne festgelegte und dokumentierte Zuständigkeiten, Abläufe und Sicherheitsmaßnahmen. Es existiert bislang keine Verfahrensbeschreibung oder Risikoanalyse, auf deren Grundlage festgestellt werden könnte, ob und durch welche technischen und organisatorischen Maßnahmen gewährleistet ist, dass die digitalisierten Informationen aus den Mitteilungen vollständig und richtig gescannt wurden und dauerhaft gesichert und verfügbar gehalten werden können. Eine abschließende Bewertung ist u.E. daher erst nach Vorlage der noch zu erstellenden Verfahrensbeschreibung und Risikoanalyse durch die Registerstelle möglich.

▶ Mikroverfilmte Zweitbücher: gesetzliche Aufbewahrungsfrist und vorzeitige Abgabe an das Staatsarchiv:

Im Zweiten Weltkrieg waren viele Erstbücher zerstört worden. Daher wurden 1943 die Zweit- zu Erstbüchern erklärt und die Mikroverfilmung als schnellste Form zur Wiedererstellung der Zweitbücher gewählt. Diese mikroverfilmten Zweitbücher wurden an das Staatsarchiv abgegeben, obwohl noch nicht für sämtliche Daten das Ende der gesetzlichen Aufbewahrungszeit nach dem Personenstandsgesetz abgelaufen ist. Dies ist nach § 3 Abs. 6 HmbArchG zulässig, jedoch bleibt die abgebende Stelle bis zum Ablauf der Aufbewahrungsfrist Daten verarbeitende Stelle i.S.d. HmbDSG, und die Daten dürfen ausschließlich nach Maßgabe des Personenstandsgesetzes verarbeitet werden. Hier wurde uns seitens der Registerstelle und des Staatsarchives dargestellt, dass dies sichergestellt ist.

▶ Generalregister

Das Generalregister ist eine spezifisch hamburgische Einrichtung, die mit Einführung der staatlichen Personenstandsführung 1876 geschaffen wurde. Aufgrund der damaligen Vielzahl von Hamburgischen Standesämtern wurde die Einrichtung eines zentralen Suchverzeichnisses für zweckmäßig erachtet. Nach § 39 Abs. 1 der außer Kraft getretenen Allgemeinen Verwaltungsvorschrift zum Personenstandsgesetz (DA für Standesbeamte und ihre Aufsichtsbehörden) mussten für jedes Personenstandsbuch Namensverzeichnisse in doppelter Ausfertigung geführt werden. Eine Ausfertigung hatte der Standesbeamte jährlich mit dem Zweitbuch an die für die Verwahrung und Fortschreibung der Zweitbücher zuständige Behörde abzugeben. Hieraus wurde das Generalregister zusammengestellt, an welches sich Standesämter und private Dritte wenden konnten, um zu erfahren, bei welchem hamburgischen Standesamt ein Personenstandsfall beurkundet ist. Das Generalregister wurde bis 1978 in Papierform und danach elektronisch geführt, wobei die Verfahren und Datenbestände im Laufe der Zeit mehrmals der Technik angepasst wurden. Heute werden die Daten über die Standesamtssoftware Autista verwaltet. Während der Ad-hoc-Prüfung wurde festgestellt, dass für das Verfahren Generalregister die von einer Daten verarbeitenden Stelle nach §§ 8 und 9 HmbDSG verpflichtend zu erstellende und fortzuführende Verfahrensbe-

schreibung und Risikoanalyse nicht existierten. Da die rechtlichen Grundlagen für das Generalregister als zentrales Suchverzeichnis nicht dargelegt werden konnten, wurde festgestellt, dass hier Klärungsbedarf besteht. Insbesondere für die praktizierte Auskunftserteilung an private Dritte konnte überhaupt keine rechtliche Grundlage benannt werden, daher wurde diese bereits am 20.06.2011 eingestellt.

Die Standesamtliche Registerstelle wurde von uns aufgefordert, die Risikoanalyse vorzunehmen sowie die nach §§ 8,9 HmbDSG erforderlichen Unterlagen zu erstellen und im Rahmen dessen die rechtlichen Grundlagen für das Verfahren auch mit Blick auf die geänderte Rechtslage nach Inkrafttreten des neuen PStG 2009 und der Einführung des elektronischen Personenstandsregisters im Januar 2012 zu klären und zu benennen und die ggf. zu ziehenden Konsequenzen für die Zukunft des Verfahrens Generalregister darzulegen. Obwohl seitens N/DSB und N/ITB frühzeitig Unterstützung angeboten worden war, sah sich die Standesamtliche Registerstelle dazu lange Zeit nicht in der Lage. Erst Anfang 2013 lagen die ersten Entwürfe der geforderten Unterlagen vor und wurden unter unserer Beteiligung besprochen. Hierzu wurde von uns als auch von N/DSB u.a. darauf hingewiesen, dass die von der Registerstelle als einzige Rechtsgrundlage angegebene bereits außer Kraft getretene Dienstanweisung für Standesbeamte und ihre Aufsichtsbehörden (DA) als rechtliche Grundlage für das Verfahren unzureichend ist und zudem weder durch die DA oder eine sonstige Rechtsvorschrift des alten PStG legitimiert war, dass

- die Namensverzeichnisse für die Zweitbücher nicht von den Standesämtern selbst, sondern zentral durch das Generalregister und zudem elektronisch geführt wurden,
- das Generalregister als Zweitnamensverzeichnis nicht nur Sicherungszwecken diente, sondern aktiv zur Suche und Beauskunftung eingesetzt wurde.

Auch die unzureichende Absicherung der bisherigen Datenübertragungswege von den Standesämtern zur Registerstelle haben wir bemängelt.

Die nur sehr zögerliche Befassung und Auseinandersetzung mit der rechtlichen Situation und der Zukunft des Verfahrens Generalregister wurde seitens der Registerstelle damit begründet, dass aufgrund des Inkrafttretens des neuen PStG und der Einführung des elektronischen Personenstandsregisters 2012 sowie der lange Zeit offenen Frage, ob Hamburg ein zentrales Personenstandsregister einführen wird, breite Verunsicherung bestanden habe. Der Leiter der Registerstelle machte zudem deutlich, dass die Beantwortung der aufgetretenen Fragen und die Lösung der vorhandenen Probleme sowie die hierfür zu treffenden Entscheidungen nicht allein durch ihn erfolgen können, sondern die Beteiligung und Mitarbeit der Standesämter und der BIS als aufsichtsführende Fachbehörde erfordern.

Wir haben daher den Kreis der Verantwortlichen unter Hinweis auf die nach Inkrafttreten des neuen PStG 2009 veränderte Rechtslage und den danach möglichen Lösungs-

ansätzen aufgefordert, sich gemeinsam des Problems anzunehmen, die offenen Fragen zu klären und eine rechtskonforme Lösung für das Verfahren Generalregister zu finden.

Eine hierzu zugesagte gemeinsame Stellungnahme der Verantwortlichen erreichte uns kurz vor Redaktionsschluss im Dezember 2013. Leider beinhaltet diese aber noch keinen konkreten Lösungsansatz. Nach der Stellungnahme ist jedoch beabsichtigt, Lösungsvorschläge vorzubereiten und diese im neuen Jahr vorzulegen. Wir erwarten daher, dass die verantwortlichen Stellen nunmehr einen Lösungsansatz, der unsere bekannten Anforderungen aufnimmt, im 1. Quartal des kommenden Jahres vorlegen.

19. Meldewesen

19.1 Was bringt das neue Bundesmeldegesetz?

Das neue Bundesmeldegesetz tritt am 1. Mai 2015 in Kraft. Der Gesetzgeber ist vielen Hinweisen und Forderungen der Datenschutzbeauftragten nicht nachgekommen, so dass das Gesetz aus datenschutzrechtlicher Sicht erhebliche Defizite aufweist.

Im Zuge der Föderalismusreform im Jahre 2006 wurde das Meldewesen in die ausschließliche Gesetzgebungskompetenz des Bundes überführt. Das Gesetzgebungsverfahren für ein neues Bundesmeldegesetz (BMG) wurde von den Datenschutzbeauftragten des Bundes und der Länder intensiv begleitet (vgl. dazu 22.TB, III 17; 23 TB, III 17.1).Wie bereits im 23. TB dargestellt, enthielt der von der Bundesregierung vorgelegte Entwurf eines Gesetzes zur Fortentwicklung des Meldewesens vom 16. November 2011 (Bundestagsdrucksache 17/7746) aus datenschutzrechtlicher Sicht zwar einige Verbesserungen gegenüber früheren Referentenentwürfen, wie etwa den Verzicht auf ein zentrales Bundesmelderegister oder eine Einwilligungslösung bei einfachen Melderegisterauskünften für Zwecke der Werbung und des Adresshandels. Jedoch bestanden noch wesentliche datenschutzrechtliche Forderungen und Bedenken, welche nicht berücksichtigt wurden. So hatten die Datenschutzbeauftragten u.a gefordert:

- die Rechte der Betroffenen bei Melderegisterauskünften zu stärken.
- die Hotelmeldepflicht als unverhältnismäßige Vorratsdatenspeicherung abzuschaffen.
- auf die Wiedereinführung der Mitwirkungspflicht des Vermieters und die damit verbundene zusätzliche Erhebung und Speicherung von Daten sowohl des Meldepflichtigen als auch des Wohnungsgebers zu verzichten.
- einen umfassenden Auskunftsanspruch des Betroffenen hinsichtlich der gespeicherten Daten und der erfolgten Datenübermittlungen zu schaffen, ohne diesen auf bestimmte Arten und Formen von Datenübermittlungen zu beschränken.

Der Deutsche Bundestag hatte in seinem Gesetzesbeschluss am 28. Juni 2012 nicht

nur diese Forderungen nicht berücksichtigt, sondern auf Vorschlag des Innenausschusses Änderungen beschlossen, die die im Regierungsentwurf enthaltenen Datenschutzbestimmungen deutlich verschlechtern. So war insbesondere bei Melderegisterauskünften für Zwecke der Werbung und des Adresshandels statt der Einwilligungslösung nur noch eine Widerspruchslösung vorgesehen, welche zudem ins Leere lief, weil die Unternehmen selbst bei einem Widerspruch des Meldepflichtigen Auskunft erhalten sollten, wenn die Daten ausschließlich zur Berichtigung oder Bestätigung bereits vorhandener Daten verwendet werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) hatte daraufhin in der Entschließung vom 22. August 2012 und einer gemeinsamen fachlichen Stellungnahme auf die erheblichen datenschutzrechtlichen Defizite hingewiesen und den Bundesrat aufgefordert, dem Gesetz nicht zuzustimmen, damit im Vermittlungsverfahren die angemahnten datenschutzrechtlichen Verbesserungen erfolgen können. Die DSK-Entschließung „Melderecht datenschutzkonform gestalten!" und die dazu gehörige fachliche Stellungnahme können unter
http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/83_84DSK_Melderecht.html?nn=409240
http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/83_84DSK_StellungnahmeMelderechtsreform.html?nn=409240 abgerufen werden.

Zwar hat der Bundesrat die Einberufung des Vermittlungsausschusses verlangt, allerdings wurden durch diesen nicht alle datenschutzrechtlichen Bedenken aufgegriffen. Lediglich die auch in der Öffentlichkeit heftig kritisierte Widerspruchslösung bei Melderegisterauskünften zu Zwecken der Werbung und des Adresshandels wurde gekippt. Künftig dürfen Meldedaten für Zwecke der Werbung und des Adresshandels nur mit Einwilligung des Betroffenen herausgegeben werden. Auch die Zweckbindung wurde gestärkt, und die Adressdaten müssen nach Erfüllung des Übermittlungszweckes gelöscht werden. Allerdings enthält die neue Regelung insofern ein Defizit, als dass die Einwilligung auch von dem anfragenden Unternehmen eingeholt werden kann und die Meldebehörden nur zur stichprobenhaften Überprüfung des tatsächlichen Vorliegens einer Einwilligung verpflichtet werden.

Für Melderegisterauskünfte in besonderen Fällen enthält das neue BMG nur eine Widerspruchsmöglichkeit statt der geforderten Einwilligung der Betroffenen. Dies führt für Hamburger Bürger zu einer erheblichen Einschränkung ihres informationellen Selbstbestimmungsrechts, da die bisher im HmbMG bestehende Einwilligungslösung in den Fällen der Auskunftserteilung bei Wahlen zur Bürgerschaft und den Bezirksversammlungen und bei Alters- und Ehejubiläen entfällt. Eine weitere Verschlechterung stellt die nach dem HmbMG bisher nicht bestehende Möglichkeit der Auskunftserteilung an Adressbuchverlage dar, für die im neuen BMG nur eine Widerspruchsmöglichkeit vorgesehen ist.

Das neue Bundesmeldegesetz wurde im März 2013 vom Deutschen Bundestag und Bundesrat verabschiedet und wird am 1. Mai 2015 in Kraft treten.

20. Personalausweis- und Passwesen

20.1 Antragsverfahren für ePass und neuen Personalausweis endlich datenschutzgerecht

Die von uns bereits 2008 festgestellten Mängel sollen jetzt Anfang 2014 endlich behoben werden.

Anlässlich der Prüfung des Antragsverfahrens für den elektronischen Reisepass (ePass) hatten wir bereits 2008 festgestellt, dass dieses IT-Verfahren zwei gravierende Mängel aufweist (vgl. 22. TB, III 18.1). Eine Nachprüfung des Antragsverfahrens zum neuen Personalausweis und ePass im Juni 2011 hatte ergeben, dass die in der Stellungnahme des Senats zum 22. Tätigkeitsbericht zugesagte Mängelbeseitigung nicht erfolgt war (vgl. 23. TB, III 18.2).

Im aktuellen Berichtszeitraum ist es der zuständigen Fachlichen Leitstelle der Bezirksämter N/ITB nun gelungen, in enger Abstimmung mit uns die Mängelbeseitigung so weit voranzutreiben, dass voraussichtlich ab Anfang 2014 eine datenschutzgerechte Lösung produktiv genutzt werden kann:

- Die Prüfung hatte aufgezeigt, dass die zu einem ePass erhobenen Passantragsdaten nach der Erfassung verändert werden könnten. So könnten z.B. die Fingerabdruckdaten ausgetauscht werden, ohne dass dies auffallen würde. Da bei vergleichbaren Prüfungen in anderen Bundesländern ebenfalls diese Mängel an den dort genutzten IT-Verfahren festgestellt wurden, für deren Beseitigung Veränderungen an der Melde- bzw. Passamtssoftware erforderlich sind, haben sich die Datenschutzbeauftragten des Bundes und der Länder im Berichtszeitraum erneut an die Hersteller dieser Softwareprodukte gewandt und eine datenschutzgerechte Lösung angemahnt. Der Software-Hersteller für das Programm OK.EWO, das in der FHH für die Antragsbearbeitung genutzt wird, hat dennoch im Standard keine Lösung für die Beseitigung dieses Mangels angeboten. Aus diesem Grund hat die FHH eine Lösung beauftragt, bei welcher der gesamte Datensatz unmittelbar nach der Erfassung so durch ein Zertifikat miteinander verbunden wird, dass Veränderungen im weiteren Prozess deutlich erkennbar werden würden. Die Bestellung eines Passes bzw. Personalausweises bei der Bundesdruckerei mit manipulierten Daten wird dadurch verhindert. Die veränderten Software-Module wurden mit der Version 7.80 ausgeliefert. Diese für die FHH programmierte Erweiterung in OK.EWO kann nunmehr auch von anderen Kunden des Software-Herstellers genutzt werden.

- Des Weiteren war bereits 2006 von uns festgestellt worden, dass die gesetzlich vorgegebenen Löschungsfristen für die Fingerabdruckdaten beim ePass nicht eingehalten wurden.

Bei der Lösung galt es drei Ziele zu berücksichtigen.

1. Die bei der Personalausweisbehörde gespeicherten Fingerabdrücke sind spätestens nach Aushändigung des ePasses bzw. des Personalausweises an die antragstellende Person zu löschen. Die Löschung bezieht sich auf alle Daten in der Anwendungs- und Sicherungsebene. Gerade die Beachtung der gesetzlichen Löschungsverpflichtung auch für die Backup-Dateien bereitete Schwierigkeiten, da regelhaft deutlich längere Aufbewahrungsfristen für Sicherungsdateien bestehen.

2. Um die erforderliche Sicherheit des IT-Verfahrens gewährleisten zu können, soll die Datenbank mindestens zum Beginn des Vortages vollständig wiederhergestellt werden können. Dazu sind entsprechende Vollsicherungen und Log-Files zu erstellen.

3. Das Modell soll eine wiederholte Übermittlung von Antragsdaten mit Fingerprint an die Bundesdruckerei am Folgetag ermöglichen. Dies ist erforderlich, da seitens der Bundesdruckerei keine unmittelbar automatisiert auswertbare Rückmeldung erfolgt, ob die weitere Verarbeitung der übermittelten Antragsdaten technisch möglich ist. Mit dieser Option, die Antragsdaten im Fehlerfalle am Folgetag erneut übermitteln zu können, wird das erneute Vorsprechen von Bürgerinnen und Bürgern für die Fälle vermieden, dass die Bundesdruckerei die übermittelten Daten nicht verarbeiten konnte, die Antragsdaten aber technisch korrekt sind.

Um diesen Anforderungen auch bei der Beantragung von Express-Pässen gerecht werden zu können, wurde eine datenschutzrechtlich akzeptable Lösung festgeschrieben, bei der die Vollsicherung und die Logdateien, in denen die Fingerabdruckdaten eines Antragstellers enthalten sind, 3 Tage nach Antragstellung gelöscht werden. Die Anpassung der entsprechenden Betriebsprozesse war Ende 2013 jedoch noch nicht abgeschlossen.

20.2 Dauerbrenner: Anforderung von Personalausweiskopien und Hinterlegungsverbot

Das Fotokopieren von Personalausweisen ist außerhalb der gesetzlich geregelten Fälle nur in wenigen Ausnahmefällen zulässig. In der Regel ist lediglich ein Vermerk, dass ein gültiger Personalausweis zur Feststellung der Identität vorgelegen hat, erforderlich und auch ausreichend.

Im vergangenen Berichtszeitraum haben uns wieder zahlreiche Eingaben erreicht, in denen sich die Betroffenen darüber beschwert haben, dass von ihnen – sei es bei der Beantragung einer Leistung, einer Auskunftserteilung oder in sonstigen Fällen, die Vorlage einer Ausweiskopie oder die Hinterlegung des Ausweises verlangt wurde. Aber auch öffentliche und nicht-öffentliche Stellen haben sich mit Anfragen zu dieser Thematik an uns gewandt.

Das Personalausweisgesetz (PAuswG) normiert in § 1 Abs. 1 S. 3 ausdrücklich, dass vom Ausweisinhaber nicht verlangt werden darf, den Personalausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben. Lediglich für gesetzlich zur Identitätsfeststellung berechtigte Behörden, wie die Polizei, gilt dies nicht. Die in vielen öffentlichen und privaten Stellen früher durchaus übliche Praxis der Hinterlegung des Ausweises beim Betreten von gesicherten Gebäuden oder Grundstücken oder die Hinterlegung als Pfand sind daher unzulässig.

Zur Frage der Rechtmäßigkeit der Anforderung und Erstellung von Ausweiskopien enthält das Personalausweisgesetz zwar keine so ausdrückliche Regelung. Jedoch ergibt sich aus der Gesamtschau der anzuwendenden Vorschriften des PAuswG und der Gesetzesbegründung, dass der Personalausweis grundsätzlich ein Identifizierungsmittel ist, was der Inhaber vorlegt und vorzeigt, um sich auszuweisen. Auch im Hinblick auf die neuen Funktionalitäten des neuen Personalausweises sollte nach dem Willen des Gesetzgebers das unbeschränkte Erfassen der Ausweisdaten – insbesondere durch Kopieren und Scannen – untersagt werden, um so die Datensicherheit zu erhöhen, weil einmal erfasste und gespeicherte Daten leicht missbräuchlich verwendet werden könnten.

Zudem gibt es in Spezialgesetzen, wie etwa dem Geldwäschegesetz, dem Telekommunikationsgesetz oder der Fahrerlaubnisverordnung, Vorschriften, welche die Vorlage einer Ausweiskopie, z.B. aufgrund bestehender gesetzlicher Dokumentationspflichten explizit verlangen oder zulassen.

Für Bereiche außerhalb dieser spezialgesetzlichen Regelungen hat das Bundesministerium des Inneren für die Erstellung von Kopien von Personalausweisen folgende

Voraussetzungen formuliert, mit denen den sicherheits- und datenschutzrechtlichen Bedenken gegen die Anfertigung von Ausweiskopien Rechnung getragen wird:

- Die Erstellung einer Kopie muss erforderlich sein. Dabei ist insbesondere zu prüfen, ob nicht die Vorlage des Personalausweises und ggf. die Anfertigung eines entsprechenden Vermerks (z.B. „Personalausweis hat vorgelegen") ausreichend ist.
- Die Kopie darf ausschließlich zu Identifizierungszwecken verwendet werden.
- Die Kopie muss als solche erkennbar sein.
- Daten, die nicht zur Identifizierung benötigt werden, können und sollen von den Betroffenen auf der Kopie geschwärzt werden. Dies gilt insbesondere für die auf dem Ausweis aufgedruckte Zugangs- und Seriennummer. Die Betroffenen sind auf die Möglichkeit und Notwendigkeit der Schwärzung hinzuweisen.
- Die Kopie ist vom Empfänger unverzüglich zu vernichten, sobald der mit der Kopie verfolgte Zweck erreicht ist.
- Eine automatisierte Speicherung der Ausweisdaten ist nach dem Personalausweisgesetz unzulässig.

Bei der Prüfung des Vorliegens dieser Voraussetzungen sind aus sicherheits- und datenschutzrechtlichen Gründen strenge Maßstäbe anzulegen. Dies führt dazu, dass die notwendige Erforderlichkeit der Erstellung einer Ausweiskopie bei der Identifizierung unter Anwesenden im Regelfall nicht vorliegen und daher in diesen Fällen die Kopieerstellung unzulässig sein wird.

Bereits im 23. TB (IV 6.1) hatten wir dargestellt unter welchen Bedingungen Auskunfteien eine Personalausweiskopie anfordern dürfen, wenn Betroffene von ihrem Auskunftsanspruch nach § 34 BDSG Gebrauch machen.

III.

BESCHÄFTIGTENDATENSCHUTZ IV.

1. Das ausgefallene Gesetzgebungsverfahren 172
2. Arbeitskreis Beschäftigtendatenschutz 173
3. Prüfung der Beschäftigtendatenverarbeitung mit SAP beim UKE 173
4. KoPers/ePers - Sachstand 174

1. Das ausgefallene Gesetzgebungsverfahren

Kein Beschäftigtendatenschutzgesetz in Sicht.

In unserem 23. Tätigkeitsbericht 2010/2011 (IV 10.1) waren wir optimistisch, dass das angestoßene Gesetzgebungsverfahren zum Beschäftigtendatenschutz noch vor der Bundestagswahl im September 2013 abgeschlossen werden könnte. Der Gesetzentwurf wurde in den Ausschüssen des Bundestages behandelt. Eine Sachverständigenanhörung fand statt. Auch in der Öffentlichkeit wurden die beabsichtigten Regelungen sehr kontrovers diskutiert. Zu Beginn des Jahres 2013 sollte der Gesetzentwurf nach Änderungsvorschlägen der Regierung wieder auf die Tagesordnung kommen. Die Datenschutzbeauftragten des Bundes und der Länder hatten dazu noch am 25. Januar 2013 die Entschließung „Beschäftigtendatenschutz nicht abbauen, sondern stärken" verabschiedet.

Leider ist der Gesetzentwurf zweimal von der Tagesordnung des Bundestages genommen worden. Der Entwurf unterlag mittlerweile durch das Ende der 17. Legislaturperiode der Diskontinuität.

Der Koalitionsvertrag für die 18. Legislaturperiode enthält nun folgende Passage: „Die Verhandlungen zur Europäischen Datenschutzgrundverordnung verfolgen wir mit dem Ziel, unser nationales Datenschutzniveau - auch bei der grenzüberschreitenden Datenverarbeitung - zu erhalten und über das Europäische Niveau hinausgehende Standards zu ermöglichen. Sollte mit einem Abschluss der Verhandlungen über die Europäische Datenschutzgrundverordnung nicht in angemessener Zeit gerechnet werden können, wollen wir hiernach eine nationale Regelung zum Beschäftigtendatenschutz schaffen."

Die bisherigen Entwürfe zur EU-Datenschutz-Grundverordnung hatten den Beschäftigtendatenschutz bisher nicht im Fokus. Die Vorschläge des LIBE-Ausschusses (Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des europäischen Parlaments) vom 21. Oktober 2013 gestatten den Mitgliedstaaten nun in Art. 82, nur in gewissem Rahmen gesetzliche Ausgestaltungen zur Beschäftigtendatenverarbeitung vornehmen zu können (http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf). Sollten die vorgeschlagenen Regelungen in Kraft treten, würden sie allerdings noch hinter den durch das Bundesdatenschutzgesetz und die Rechtsprechung geprägten deutschen Standards zurückbleiben.

2. Arbeitskreis Beschäftigtendatenschutz

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit übernimmt den Vorsitz des Arbeitskreises Beschäftigtendatenschutz.

Nach jahrelangem Vorsitz des AK Personalwesen in Niedersachsen, der schwerpunktmäßig die datenschutzrechtlichen Themen der Beschäftigten der öffentlichen Stellen behandelte, haben wir nun den Vorsitz des Arbeitskreises Beschäftigtendatenschutz übernommen. Er bündelt zukünftig sowohl die datenschutzrechtlichen Fragen der öffentlichen als auch der nicht-öffentlichen Stellen und koordiniert die Abstimmung bei entsprechenden Gesetzesvorhaben. Die erste Sitzung wird im Januar 2014 stattfinden. Über die Ergebnisse werden wir berichten.

3. Prüfung der Beschäftigtendatenverarbeitung mit SAP beim UKE

Personalaktendaten werden beim UKE unzulässig durch eine nicht-öffentliche Stelle im Wege der Auftragsdatenverarbeitung verarbeitet.

Im April 2013 hatten wir begonnen, die Beschäftigtendatenverarbeitung beim UKE zu prüfen. Neben einer technischen Kontrolle des eingesetzten Systems SAP ERP HCM stand im Vordergrund die Zulässigkeit der Auftragsdatenverarbeitung an eine nicht-öffentliche Stelle. Mit SAP werden auch Personalaktendaten verarbeitet.

Für Personalaktendaten gilt vorrangig das Hamburgische Beamtengesetz (HmbBG). Dies ergibt sich aus § 2 Abs. 7 HmbDSG. Das HmbBG enthält für die in § 89 Abs. 2 beschriebenen Aufgaben klare Regelungen. Die Anwendung des HmbDSG kommt im Hinblick auf die Auftragsdatenverarbeitung nur einschränkend in Betracht. Die Formulierung in § 89 Abs. 2 HmbBG „. . . an eine andere Behörde oder öffentliche Stelle . . ." lässt keine andere Auslegung zu. Aus der Gesetzesbegründung zu § 89 Abs. 2 HmbBG ist nicht erkennbar, dass die „Auslagerung" entgegen der gesetzlichen Formulierung an eine nicht-öffentliche Stelle erlaubt sein soll.

Weiterhin spricht das HmbBG von „weitergeben". Dieser Begriff findet keinen Niederschlag im Datenschutzrecht und ist nicht identisch mit dem datenschutzrechtlichen Begriff „Übermitteln". Vielmehr impliziert der Begriff „weitergeben" eben auch solche Weitergaben im Rahmen der Auftragsdatenverarbeitung, die datenschutzrechtlich nicht als Übermitteln zu qualifizieren sind. Der Gesetzgeber hat damit zum Ausdruck

gebracht, dass auch solche Weitergaben nur an öffentliche Stellen oder Behörden erfolgen sollen.

Im Übrigen ist zu bedenken, dass der Zugang zu Personalaktendaten auf die in § 85 Abs. 4 HmbBG genannten Beschäftigten begrenzt ist. Dazu gehören nicht die Beschäftigten einer nicht-öffentlichen Stelle, auch nicht im Rahmen einer Auftragsdatenverarbeitung. Diese Auffassung hat das Personalamt als oberste Dienstbehörde in anderen Fällen bereits mehrmals vertreten.

Das UKE teilt unsere und die Auffassung der behördlichen Datenschutzbeauftragten nicht. Vielmehr wird davon ausgegangen, dass auch nach der Novellierung des Hamburgischen Beamtengesetzes im Jahr 2009 eine Auftragsdatenverarbeitung von Personalaktendaten an eine nicht-öffentliche Stelle erlaubt sei.

Gegenwärtig ist aufgrund der letzten Äußerung des UKE davon auszugehen, dass eine Änderung des Verfahrens nicht angestrebt wird, die bisherigen nicht–öffentlichen Auftragnehmer weiterhin unzulässigerweise Personalaktendaten des UKE verarbeiten.
Dies ist bedauerlich, zumal in einem Gespräch mit den Verantwortlichen im Dezember 2013 uns gegenüber noch die Bereitschaft signalisiert wurde, eine rechtmäßige Lösung zur Verarbeitung der Beschäftigtendaten umzusetzen. Wir werden weiterhin auf eine tragfähige, den gesetzlichen Regelungen entsprechende Lösung hinwirken.

4. KoPers/ePers - Sachstand

Eine datenschutzrechtliche Beurteilung der beabsichtigten Einführung eines neuen Personalmanagementsystems ist nach wie vor nicht möglich.

In unserem 23. Tätigkeitsbericht 2010/2011 (III, 2.1) berichteten wir über das Projekt zur Einführung eines neuen Personalmanagementsystems. Der ursprüngliche Zeitplan konnte nicht eingehalten werden. Der Produktivstart in Hamburg ist derzeit für 01.04.2014 (Versorgungsempfänger) und 01.01.2015 (aktiv Beschäftigte) vorgesehen. Eine umfassende datenschutzrechtliche Beurteilung ist gegenwärtig noch nicht möglich, da weder eine Verfahrensbeschreibung noch Risikoanalysen bis zum Redaktionsschluss vorgelegt wurden.
Das unabhängig davon entwickelte Bewerbermanagementverfahren wurde im Frühjahr 2012 eingeführt. Die damit verbundenen datenschutzrechtlichen Fragestellungen wurden mit uns auf Basis der Verfahrensbeschreibung sowie Risikoanalyse abgestimmt.

Wir werden weiter berichten.

IV.

TELEMEDIEN V.

1. Orientierungshilfe Soziale Netzwerke 178
2. Umsetzung der Cookie-Richtlinie 179
3. Do Not Track 182
4. Nutzung sozialer Netzwerke durch öffentliche Stellen 183
5. Nutzung Sozialer Netzwerke insbesondere Facebook durch die Polizei Hamburg 185
6. Google 187
7. Facebook 194
8. Xing – Auftragsdatenverarbeitung und CDN 199
9. Datenschutz und Online-Dating 200
10. Abgeordnetenwatch.de 201
11. Private Fahndung in Sozialen Netzwerken 203
12. Das Ausspähprogramm PRISM und die US-Diensteanbieter 205

V. TELEMEDIEN

1. Orientierungshilfe Soziale Netzwerke

Soziale Netzwerke sind die Wahrzeichen der Sozialen Medien und des Web 2.0. Die Wahrung des Datenschutzes bei der Nutzung Sozialer Netzwerke wird durch die Orientierungshilfe „Soziale Netzwerke" adressiert (http://www.datenschutz-hamburg.de/news/detail/article/orientierungshilfe-soziale-netzwerke.html).

Die Nutzung sozialer Medien insbesondere sozialer Netzwerke wie Facebook, Google+, Xing, Twitter, WhatsApp oder LinkedIn ergreift alle gesellschaftlichen Bereiche. Sie werden nicht nur zur privaten Individualkommunikation eingesetzt. Auch private Unternehmen, Vereine und politische Interessengruppen nutzen sie, um ihre Produkte, Dienste oder Informationen zu bewerben bzw. zu verbreiten. Auch der Staat kann sich diesem Trend nicht entziehen. Abseits der großen Netzwerkbetreiber wie der Facebook Inc. oder Google Inc. entstehen viele kleinere Themennetzwerke und soziale Medien, die nicht so sehr im Fokus der Öffentlichkeit stehen. Jedoch stellen sich bei allen diesen Telemediendiensten vergleichbare datenschutzrechtliche Fragen.

Bei der Um- und Durchsetzung datenschutzrechtlicher Forderungen durch die Aufsichtsbehörden wurden wir häufig mit der Forderung nach klaren und vor allem einheitlichen Vorgaben im Hinblick auf das Betreiben derartiger Netzwerke konfrontiert. Gemeinsam mit den anderen Aufsichtsbehörden haben wir daher im Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Orientierungshilfe „Soziale Netzwerke" verabschiedet. Sie reflektiert das gemeinsame Verständnis der Datenschutzbeauftragten und Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich zur Beachtung der datenschutzrechtlichen Vorgaben beim Einsatz sozialer Netzwerke zur Erfüllung eigener Aufgaben oder Geschäftszwecke. Wie die anderen Aufsichtsbehörden auch waren wir der Auffassung, dass ein effektiver Datenschutz nicht allein dadurch gewährleistet werden kann, den privaten Nutzerinnen und Nutzern im Wege des Selbstdatenschutzes die Verantwortung für die Wahrung ihrer Rechte zuzuschreiben. Alle Beteiligten haben ihren Teil dazu beizutragen. Die Orientierungshilfe richtet sich daher sowohl an die professionellen Verwender als auch an die Betreiber der Dienste.

Ziel der Orientierungshilfe ist die Konkretisierung der gesetzlichen Mindeststandards und das Aufzeigen von Best-Practice-Ansätzen. Letzteres gilt vor allem in den Bereichen, in denen der gesetzliche Normierungsrahmen Lücken hinsichtlich eines ausreichenden Schutzes des Rechts auf informationelle Selbstbestimmung und des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aufweist.

Die Darstellung basiert auf der datenschutzrechtlichen Bewertung verschiedener

„Schichten" sozialer Netzwerke. Die jeweilige „Schicht" wird durch die Art der auf ihr verwendeten Daten wie Inhaltsdaten, Bestandsdaten und Nutzungsdaten charakterisiert. Grundlage der Orientierungshilfe sind die bestehenden gesetzlichen Grundlagen und die einschlägigen Beschlüsse und Entschließungen der nationalen und internationalen Gremien, insbesondere der Artikel-29-Datenschutzgruppe.

Zusammen mit den anderen Aufsichtsbehörden haben wir angestrebt, einen praxisorientierten Ansatz bei der Darstellung der datenschutzrechtlichen Anforderungen an soziale Netzwerke zu wählen. Das bedeutet, dass sich die Gliederung der Orientierungshilfe an den Schutzzielen des Datenschutzes und der Datensicherheit orientiert. Nach einer Auseinandersetzung mit den Anforderungen an die technische Sicherheit, der datenschutzrechtlichen Verantwortlichkeit und den rechtlichen Grundlagen werden Hinweise zur Beachtung der Schutzziele der Vertraulichkeit, Verfügbarkeit, Transparenz und Kontrolle sowie der Wahrung der Betroffenenrechte gegeben. Die Lösung von Einzelproblemen, die auch aus unserer aufsichtsbehördlichen Praxis entspringen, haben ebenfalls Eingang in die Orientierungshilfe gefunden.

Mit dem Scheitern des Versuches der Betreiber sozialer Netzwerke, sich im Wege der Selbstregulierung auf Regeln zur Beachtung des Datenschutzes und der Datensicherheit zu einigen, wird dieses Dokument sicherlich einen weiteren Bedeutungszuwachs erhalten.

2. Umsetzung der Cookie-Richtlinie

Die Umsetzung des Art. 5 Absatz 3 der Richtlinie 2002/58/EG des Europäischen Parlaments und Rates mit Stand vom 18.12.2009 (E-Privacy Richtlinie) ist in Deutschland gescheitert. Er sieht vor, dass Nutzerinnen und Nutzer u.a in das Setzen von Cookies, die zur Erbringung des Dienstes technisch nicht erforderlich sind, einwilligen müssen. Wir werden uns jedoch dafür einsetzen, dass die Grundgedanken der Richtlinie Eingang in die Gestaltung von Internetdiensten finden.

Ziel der Richtlinie ist ein verbesserter Schutz der Nutzerinnen und Nutzer bei der Verwendung von elektronischen Kommunikationsdiensten. Dienstanbieter setzen mittlerweile die unterschiedlichsten Techniken ein, um die Nutzung von Internetdiensten individueller auf die Nutzerinnen und Nutzer zuzuschneiden oder die Nutzung zu vereinfachen. Neben der rein technischen Verbesserung der Dienstangebote erfassen Anbieter mit denselben Techniken auch das individuelle Nutzungsverhalten und damit die Interessen und Vorlieben der Nutzerinnen und Nutzer. Mit diesen Erkenntnissen kann auf deren Willensbildung zum Zweck der Werbung, des Marketings oder anderweitiger Zielsetzungen eingewirkt werden. Eine der zu diesem Zweck genutzten Techniken ist das Setzen von Cookies.

Cookies sind kleine Textdateien, die auf den Rechnern der Nutzerinnen und Nutzer abgespeichert werden. Sie können von rein technischen, nicht personenbezogenen Informationen über eindeutige Identifikationsmerkmale bis hin zu unmittelbar personenbezogene Informationen enthalten. Mit Blick auf die Persönlichkeitsrechte der Betroffenen stellt der Einsatz von Cookies zwar nur eine, jedoch die derzeit wohl üblichste Form der Individualisierung der Nutzerinnen und Nutzer im Internet dar. Sie ist Voraussetzung für die Auswertung des Nutzerverhaltens zum Beispiel zur Erstellung verhaltensbasierter Werbung im Internet.

Durch die E-Privacy Richtlinie wird explizit anerkannt, dass es sich bei dem Einsatz derartiger Technologien einerseits um legitime und nützliche Hilfsmittel bei der Prüfung der Wirksamkeit einer Webseite oder deren Gestaltung sowie der Werbung handeln kann. Auch zur Ermöglichung bestimmter Funktionalitäten und der Vereinfachung der Bedienung von Webangeboten kann es erforderlich sein, Cookies oder vergleichbare Technologien einzusetzen. Andererseits kann deren Einsatz eine Gefährdung für die Wahrung der Vertraulichkeit der Kommunikation und der Beachtung der Persönlichkeitsrechte der Nutzerinnen und Nutzer darstellen.

Daher sollen Nutzerinnen und Nutzer über den Einsatz und die potentielle Gefährdung ihrer Privatsphäre und Persönlichkeitsrechte informiert werden. Außerdem soll ihnen das Recht eingeräumt werden, über die Privatsphäre verletzende Nutzungen dieser Technologien selbst zu entscheiden. In diesen Fällen müssen sich Dienstanbieter vor dem Einsatz dieser Technologien eine Einwilligung einholen (25. Erwägungsgrund E-Privacy Richtlinie). Soweit jedoch der Einsatz der Cookies zur Übertragung der Informationen erforderlich oder zur Erbringung der Dienste, so wie ihn Nutzerinnen und Nutzer angefordert haben, notwendig ist, bedarf es keiner Einwilligung durch die Betroffenen.

Die Art-29-Datenschutzgruppe, ein Zusammenschluss der Datenschutzaufsichtsbehörden der EU-Mitgliedsstaaten und des Europäischen Datenschutzbeauftragten, hat zur Umsetzung und Anwendung der Richtlinie in nationales Recht zwei Stellungnahmen veröffentlicht. Bereits 2012 konkretisierte sie die Vorgaben der Richtlinie im Hinblick auf das Einwilligungserfordernis bezüglich des Setzens von Cookies (Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht vom 07. Juni 2012). Danach erfüllen Tracking-Cookies sozialer Plugins, Third-Party-Cookies zu Werbezwecken und First-Party-Analysecookies nicht die Ausnahmevoraussetzungen der E-Privacy Richtlinie. Deren Einsatz ist danach nur mit einer Einwilligung i.S.d der Datenschutzrichtlinie zulässig.

Bei der Umsetzung der Anforderungen an die geforderte Einwilligung bestand im Laufe des Berichtszeitraums eine erhebliche Unsicherheit und uneinheitliche Praxis auf europäischer Ebene. Daher verabschiedete die Art-29-Datenschutzgruppe eine weitere Stellungnahme zu den Anforderungen an eine rechtswirksame Einwilligung bei der Umsetzung der Vorgaben des Art. 5 Abs. 3 E-Privacy Richtlinie. Wir haben uns an

der Formulierung der Anforderungen an eine rechtlich wirksame Einwilligung beteiligt. Denn die teilweise als Einwilligungslösungen bezeichnete Mitwirkung der Nutzerinnen und Nutzer stellte unserer Auffassung nach eine Widerspruchslösung dar, oder die Aktivitäten der Nutzerinnen und Nutzer hatten keinen Erklärungswert im Hinblick auf das Setzen des Cookies. Die Anforderungen an eine wirksame Einwilligung in das Setzen der Cookies sind im Einklang mit der Auffassung der Art-29-Datenschutzgruppe dann erfüllt, wenn die Betroffenen spezifisch und ausführlich informiert werden, die Einwilligung zeitlich vor dem Setzen des Cookies eingeholt wird, das Verhalten der Nutzerinnen und Nutzer unzweifelhaft als Willensäußerung im Hinblick auf das Setzen des Cookies gedeutet werden kann und eine echte Wahlfreiheit besteht.

Eines der größten Hindernisse bei der Gewährung dieses verbesserten Schutzes der Nutzerinnen und Nutzer z.B. vor der exzessiven Profilbildung zu Werbezwecken ist jedoch die fehlende Umsetzung der Vorgaben des Art. 5 Abs. 3 E-Privacy Richtlinie in nationales Recht. Der deutsche Gesetzgeber hat bisher versäumt, entsprechende Regeln in das nationale Recht einfließen zu lassen. Die auch von der Bundesregierung geäußerte Meinung, die bestehenden Regelungen des Telemediengesetzes seien ausreichend und würden die Vorgaben des Art. 5 Abs. 3 E-Privacy Richtlinie erfassen, trifft unserer Auffassung nach nicht zu. Ebenso gilt dies für die teilweise geäußerte Rechtsmeinung, die E-Privacy Richtlinie fände wegen der abgelaufenen Umsetzungsfrist unmittelbar Anwendung im nationalen Rechtsraum. Wir vertreten die Auffassung, dass der durch das Europarecht erweiterte Schutz der Persönlichkeitsrechte den deutschen Nutzerinnen und Nutzern durch den deutschen Gesetzgeber vorenthalten wird. Der derzeitige Rechtsstand des Telemediengesetzes sieht keine Einwirkungsmöglichkeiten der Betroffenen auf den Einsatz von Cookies oder vergleichbaren Techniken, die Eingriffe in die Persönlichkeitsrechte vorbereiten, vor. Im Telemediengesetz findet sich lediglich die Pflicht von Dienstanbietern, die Nutzerinnen und Nutzer über den Einsatz von Techniken zu informieren, die eine spätere Identifizierung der Nutzer ermöglichen oder die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vorbereiten, § 13 Abs. 1 Satz 2 TMG. Eine echte Einwirkungsmöglichkeit bleibt den Nutzerinnen und Nutzern in der Regel zeitlich nachträglich durch das in § 15 Abs. 3 TMG vorgesehene Widerspruchsrecht gegen die Erstellung von pseudonymen Nutzungsprofilen. Hierbei handelt es sich aber um ein Widerspruchsrecht, welches zeitlich dem Setzen der Cookies nachgelagert und daher streng von der Regelung des Art. 5 Abs. 3 E-Privacy-Richtlinie zu trennen ist. Art. 5 Abs. 3 E-Privacy Richtlinie verlangt zur Eröffnung des Anwendungsbereiches keine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten.

Die fehlende Reaktion des Gesetzgebers führt letztlich dazu, dass in Deutschland Nutzerinnen und Nutzer in deutlich geringerem Umfang über den Einsatz von Cookies informiert werden und im Verhältnis zu anderen europäischen Staaten weniger Rechte im Hinblick auf die Kontrolle über die eingesetzten, potentiell persönlichkeitsrechtsgefährdenden Techniken haben. Wir werden uns daher vor allem auch im Rahmen des

Arbeitskreises Medien dafür einsetzen, im Rahmen der bereits bestehenden gesetzlichen Regelungen mehr Transparenz und Kontrolle den Nutzerinnen und Nutzer von Telemediendienstleistungen zu schaffen.

3. Do Not Track

Mit dem Standard Do Not Track kann der Nutzer von Telemedien sein Widerspruchsrecht gegen die Erstellung von Nutzungsprofilen geltend machen. Es ist Aufgabe der Anbieter, dies geeignet umzusetzen.

Seit einiger Zeit wird ein Standard entwickelt, der es Nutzern von Telemedien auf leichte Weise möglich machen soll, den Inhaltsanbietern ihre Präferenz hinsichtlich der Erstellung eines Nutzerprofils (z.B. für Werbezwecke) mitzuteilen. Diese unter dem Namen Do Not Track (bzw. kurz DNT) bekannte Technik sieht vor, dass bei jedem Kontakt des Browsers mit einem Webserver ein Datenfeld übermittelt werden kann, das bei einem Wert von „1" bedeutet, dass der Nutzer nicht verfolgt werden möchte, also kein Nutzerprofil angelegt werden darf. Bei einem Wert von „0" stimmt der Nutzer einem solchen Profil hingegen zu. Hat der Nutzer keine Festlegung seiner Präferenz getroffen, wird kein entsprechendes Datenfeld übermittelt.

Die meisten Browser unterstützen den DNT-Standard mittlerweile, so dass man von einer nahezu flächendeckenden Abdeckung ausgehen kann. In der Regel sind die entsprechenden Auswahlmöglichkeiten Bestandteil der jeweiligen Einstellungsoptionen der Browser und sollten sich leicht finden lassen.

Durch DNT wird die Verarbeitung im Browser nicht direkt beeinflusst. Es unterscheidet sich daher prinzipiell von anderen Techniken wie z.B. dem Löschen von Cookies oder verfügbaren Browser-Erweiterungen, mit denen die Anzeige von Werbung verhindert oder gesteuert werden soll. DNT sendet nur ein Präferenzsignal des Nutzers an den Webseitenbetreiber aus in der Erwartung, dass dieser Präferenz Rechnung getragen wird. Gerade aus diesem Grund eignet sich DNT in besonderem Maße zur Umsetzung eines Widerspruchsrechts.

Wir sind uns mit den anderen deutschen Datenschutzaufsichtsbehörden daher darüber einig, dass die Aktivierung der Do-Not-Track-Option im Browser für den Webseitenbetreiber als Signal zu verstehen ist, dass der Nutzer sein Widerspruchsrecht nach § 15 Abs. 3 Telemediengesetz ausübt. Empfängt ein Webserver das Signal „DNT: 1", muss auf die Erstellung eines Nutzerprofils unter Pseudonym verzichtet werden. Die für diesen Zweck erzeugten Cookies sind zu verwerfen.

Namhafte Anbieter (z.B. Twitter, Pinterest) haben sich erfreulicherweise bereits in der

Weise geäußert, dass sie die DNT-Information auswerten und sich entsprechend verhalten. Unsere Erwartungshaltung ist, dass auch diejenigen, die sich nicht so explizit positionieren wollen, ihre Angebote DNT-konform ausgestalten.

4. Nutzung sozialer Netzwerke durch öffentliche Stellen

Die Frage nach dem Einsatz sozialer Netzwerke zur Erfüllung dienstlicher und geschäftlicher Aufgaben stellt sich auch öffentlichen Stellen. Wir unterstützen die Forderungen nach einem Engagement der öffentlichen Verwaltung bei dem Einsatz neuer Formen der Kommunikation und Interaktion insbesondere im Bereich der sozialen Medien. Wie jedes andere staatliche Handeln auch muss dies jedoch unter Beachtung der Grundrechte, im Besonderen dem Recht auf informationelle Selbstbestimmung und den dazu erlassenen datenschutzrechtlichen Vorgaben, speziell dem Telemedienrecht, erfolgen.

Die Informations- und Kommunikationstechnologie und der Wunsch, die neuen Formen dieser Art der Kommunikation zu nutzen, haben sich im Berichtszeitraum rasant entwickelt. Vor allem die sozialen Medien und davon speziell die „Sozialen Netzwerke" nehmen einen immer größeren Raum in der gesellschaftlichen und privaten Kommunikation ein. Diese Evolution der Kommunikation wird maßgeblich durch privatwirtschaftliche, nicht selten global agierende Unternehmen geprägt. Sie geben nicht nur den Takt der technologischen Entwicklung vor. Häufig bestimmen sie auch die rechtlichen Rahmenbedingungen für Zweck, Art und Umfang der Verarbeitung personenbezogener Daten. Der unbestrittene Erfolg der sozialen Netzwerke in wirtschaftlicher wie auch technologischer Hinsicht zeigt auch in der öffentlichen Verwaltung und der Politik der FHH Wirkung. Das naturgemäß geringere Innovationspotential des Staates bei der technischen Entwicklung seiner eigenen Kommunikationsmittel soll durch die verstärkte Nutzung dieser privatwirtschaftlichen, oft auf den ersten Blick scheinbar kostenlosen Angebote wettgemacht werden. Die FHH hatte zur Aktivierung dieser Potentiale einen entsprechenden Social Media Guide veröffentlicht, in dem wir jedoch unsere datenschutzrechtliche Sicht des Einsatzes der sozialen Medien zur Erfüllung staatlicher Aufgaben nicht einbringen konnten. Wir stehen mittlerweile mit den für die Erstellung dieses Leitfadens zuständigen Stellen in Kontakt und hoffen, das Thema des Datenschutzes in diese Handreichung maßgeblich einfließen lassen zu können (siehe dazu auch V. 1.).

Dass ein großes Interesse an der Nutzung sozialer Medien besteht, verstehen und akzeptieren wir. Jedoch kann der Staat beim Einsatz dieser Dienste nicht die bestehenden datenschutzrechtlichen Regeln ignorieren. In unserer täglichen Praxis haben wir auf drei Ebenen Defizite bei der Umsetzung des europarechtlich und verfassungsrechtlich gewährleisteten Rechts auf informationelle Selbstbestimmung identifiziert.

Zum einen fehlt es an modernen, technologieneutralen gesetzlichen Regeln, die das Risiko im Hinblick auf die Persönlichkeitsrechte der Betroffenen adäquat auffangen und ein hinreichendes Schutzniveau normieren. Wir haben außerdem feststellen müssen, dass Anbieter sozialer Medien nicht selten ihre bestehende Marktmacht einsetzen, um die eigenen Regeln des Umgangs mit personenbezogenen Daten durchzusetzen, und europäische und nationale Vorgaben eher unwillig umsetzen. Und letztlich mangelt es an einem effektiven Vollzug der bestehenden Regeln, weil den zuständigen Aufsichtsbehörden häufig nicht die erforderlichen personellen Ressourcen zur Verfügung stehen. Letzteres gilt nicht nur für den klassischen aufsichtsbehördlichen Vollzug, sondern auch für die Beratung von Dienstanbietern.

Wir vertreten gemeinsam mit den Aufsichtsbehörden der anderen Länder die Auffassung, dass bei der Nutzung sozialer Netzwerke zu wirtschaftlichen Zwecken oder der Erfüllung staatlicher Aufgaben die Vorgaben des nationalen Datenschutzrechts einzuhalten sind (Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich - Düsseldorfer Kreis am 08. Dezember 2011 und Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011). Es darf keine Möglichkeit der Flucht von Betreibern und professionellen Verwendern sozialer Medien in „Häfen" geben, in denen das Datenschutzrecht ineffektiv ist oder kaum wirksam umgesetzt wird und somit dem auch europarechtlich anerkannten Recht auf Datenschutz (Art. 8 Charta der Grundrechte der Europäischen Union) nicht hinreichend genug Geltung verschafft wird. Dies gilt insbesondere für Dienste, die staatliche Stellen bei der Verwendung sozialer Netzwerke zur Erfüllung hoheitlicher Aufgaben oder Vollzugstätigkeit einsetzen.

Wir fordern, dass bei der Nutzung sozialer Medien staatliche Stellen grundsätzlich in der Lage sind, die zur Aufgabenerfüllung verwendeten Verfahren und Prozesse gerade auch bei dem Rückgriff auf privatwirtschaftliche Angebote zu beherrschen bzw. entsprechende Vereinbarungen mit den Betreibern zu treffen.

Dazu zählt neben der Kontrolle der veröffentlichten personenbezogenen Daten auch in den Kommentarfunktionen

- die Wahrung der Vertraulichkeit und Integrität der nichtöffentlich geführten Kommunikation
- die Bindung der Verarbeitung personenbezogener Daten an die gesetzlich vorgesehenen Zwecke
- die Vermeidung unnötiger und exzessiver Profilbildung bei der Analyse der Nutzerdaten und der Reichweitenanalyse
- die Beachtung des Rechts der Möglichkeit auf anonyme und pseudonyme Nutzung der eingesetzten Dienste und
- die Gewährleistung einer effektiven Wahrnehmung von Betroffenenrechten, insbesondere des Widerspruchsrechts gegen die Bildung von Interessens- und Nutzungsprofilen unter Verwendung von Nutzungsdaten.

Wir erwarten von öffentlichen Stellen bei der Entscheidung über die Nutzung sozialer Medien die Erstellung einer umfassenden Risikoanalyse.

Außerdem müssen staatliche Stellen beim Einsatz der Angebote privater Dienstanbieter die Gewähr bieten, dass keine exklusiven Zugänge zu den veröffentlichten Informationen geschaffen werden. D.h. Betroffene müssen weiterhin die Möglichkeit haben, anbieterneutral und ohne Registrierung bei privaten Dienstanbietern die staatlicherseits zur Verfügung gestellten Dienste oder Informationen nutzen zu können. In der Regel kann dies durch die parallele Veröffentlichung der Angebote und Informationen auf den offiziellen Internetseiten der staatlichen Stellen realisiert werden.

Wir werden auch zukünftig gemeinsam mit sämtlichen Beteiligten und Interessensvertretern einen konstruktiven Dialog pflegen, um eine datenschutzkonforme Nutzung von sozialen Medien auch durch staatliche Stellen zu ermöglichen. Dabei werden wir uns weiterhin für Best-Practice-Ansätze stark machen, jedoch bei Verstößen auch die uns zustehenden rechtlichen Instrumente einsetzen.

5. Nutzung Sozialer Netzwerke insbesondere Facebook durch die Polizei Hamburg

Das Social Media Konzept für die Öffentlichkeitsarbeit des 200 jährigen Geburtstages der Polizei Hamburg wird durch uns nicht beanstandet. Unsere ernsthaften Zweifel an Datenschutzkonformität der Nutzung des Dienstes Facebook zu Fahndungszwecken sind bisher noch nicht ausgeräumt.

Die Polizei Hamburg stellte uns ihr für 2014 geplantes „Social Media Konzept" vor, welches unter anderem die Nutzung einer Fanpage auf der Plattform des Sozialen Netzwerkanbieters Facebook Inc. vorsieht. Dazu erstellte die Polizei Hamburg einen umfassenden Projektplan und eine entsprechende datenschutzrechtliche Risikoanalyse. In dieser wird auf die möglichen Gefährdungen des Rechts auf informationelle Selbstbestimmung der Nutzerinnen und Nutzer umfassend eingegangen. Die Polizei Hamburg sagte außerdem zu, an sieben Tagen in der Woche eine jeweils 24-stündige Betreuung der Fanpage und des Dienstangebotes zu gewährleisten und darüber sicherzustellen, dass keine rechtwidrigen Inhalte über die Kommentarfunktionen auf den Angeboten der Polizei erscheinen. Außerdem wird ein 4-Augen-Prinzip beim Veröffentlichen von Inhalten gewährleistet. Dadurch soll die effektive Kontrolle der Einhaltung der datenschutzrechtlichen Grenzen der Veröffentlichung von personenbezogenen Daten gesichert werden. Außerdem haben wir gefordert, dass Bürgerinnen und Bürger, die nicht Mitglied der von der Polizei genutzten privaten Dienstanbieter sind, dennoch auf das gesamte Informationsangebot der Polizei zugreifen können. Eine bevorzugte „Bedienung" einzelner Dienstanbieter soll dadurch verhindert werden. Wir

wollen außerdem vermeiden, dass sich Nutzerinnen und Nutzer auf Plattformen privater Dienstanbieter anmelden müssen, die durch die FHH nicht effektiv kontrolliert werden können.

Zu guter Letzt haben wir mit der Polizei vereinbart, am Ende des Jubiläums Anfang 2015 eine Bewertung des zeitlich begrenzten Projektes vorzunehmen. Erst danach soll über die weitere Nutzung u.a. des Dienstes Facebook zur Erfüllung polizeilicher Aufgaben entschieden werden.

Unter der zum Zeitpunkt der Erstellung dieses Berichtes geltenden Rechtslage bzw. Rechtsprechung besteht für die Nutzungsdatenverarbeitung der Nutzerinnen und Nutzer des Dienstes Facebook keine datenschutzrechtliche Verantwortlichkeit der Fanpagebetreiber. Eine entsprechende Entscheidung hatte das Verwaltungsgericht Schleswig zu insgesamt drei gegen das Unabhängige Landeszentrum für Datenschutz geführten Klage getroffenen (VG Schleswig Urteil vom 09. Oktober 2013, Az. 8 A 37/12, 8 A 14/12, 8 A 218/11). Danach seien Fanpagebetreiber für die Nutzungsdatenverarbeitung und die daraus resultierende Analyse des Nutzungsverhaltens auf der Plattform des Anbieters Facebook Inc. datenschutzrechtlich nicht verantwortlich. Auch wenn gegen das Urteil Berufung durch das ULD eingelegt wurde, konnten wir diese grundlegende Entscheidung bei der Bewertung der Nutzung einer Fanpage durch die Polizei nicht außer Acht lassen. Wir haben daher die Nutzung der Fanpage zu Zwecken der Öffentlichkeitsarbeit nicht beanstandet, auch wenn gegen die Entscheidung des VG Schleswig rechtliche Bedenken bestehen.

Restriktiver bewerten wir jedoch die Nutzung sozialer Netzwerke, insbesondere das Netzwerk des Dienstanbieters Facebook Inc., zur gesetzlichen Vollzugstätigkeit der Polizei wie der Öffentlichkeitsfahndung. Daran kann auch der Beschluss der Innenministerkonferenz vom 04. – 06. 12. 2013 zur Zulässigkeit der Nutzung sozialer Netzwerke zur Öffentlichkeitsfahndung nichts ändern. Die pauschale Feststellung, dass eine Öffentlichkeitsfahndung auf sozialen Netzwerken bereits nach den derzeit bestehenden gesetzlichen Vorgaben zulässig sei, können wir in der Pauschalität nicht nachvollziehen.
Nach unserer derzeitigen Auffassung setzt neben den bereits für die Öffentlichkeitsarbeit formulierten Anforderungen der Einsatz sozialer Netzwerke zu Fahndungszecken mindestens voraus, dass

- die Veröffentlichung personenbezogener Fahndungsdaten über technische Infrastrukturen erfolgt, die sich in und unter der vollständigen Kontrolle der Sicherheitsbehörden befinden und dadurch z.B. sichergestellt werden kann, dass Änderungen oder Löschungen der Daten effektiv durchgeführt werden,
- über die verwendeten Dienste privater Anbieter keine die Fahndung betreffende Kommunikation erfolgt, d.h. z.B. Hinweise oder Angaben zur Sache nur über die außerhalb der Drittanbieter liegenden Kommunikationskanäle erfolgt, z.B. Telefon,

- durch eine 7/24-Kontrolle der verwendeten Medien, z.B. der Kommentarfunktionen, eine unverzügliche Reaktion möglich ist, um Aufrufe zur Selbstjustiz, Hetzkampagnen oder Verunglimpfungen zu vermeiden, und
- die Verwendung der bei der Kenntnisnahme der Inhalte durch die Nutzerinnen und Nutzer anfallenden Nutzungs- und Verkehrsdaten z.B. zum Zweck der Reichweitenanalyse gemäß § 15 Abs. 3 TMG, nur im gesetzlich zugelassenen Rahmen erfolgt.

Weitere Beratungen in der Konferenz der Datenschutzbeauftragten sollen nähere Einzelheiten für die Öffentlichkeitsfahndung festlegen. Vor allem bezüglich der letzten Anforderung beobachten wir die Entwicklung der Rechtsprechung zur Frage der datenschutzrechtlichen Verantwortung bei Betreibern von Fanpages des Dienstanbieters Facebook genau. Wir werden die bereits begonnenen Gespräche mit dem Arbeitskreis I der Innenministerkonferenz führen sowie die Diskussion mit der Justizministerkonferenz, die eine Änderung der RistBV zur Einführung der Öffentlichkeitsfahndung im strafrechtlichen Ermittlungsverfahren plant, suchen. Es gilt, darauf zu achten, dass bei der Fahndung in sozialen Medien die richtige Balance zwischen den Interessen an einer effektiven Strafverfolgung und den Interessen an der Wahrung der betroffenen Grundrechte, z.B. dem Grundrechte auf informationelle Selbstbestimmung und der verfassungsrechtlich vorgesehenen Unschuldsvermutung, gefunden wird und die spezifischen Risiken des Einsatzes derartiger Technologien beachtet werden. Letztlich gilt es sicherzustellen, dass Aufrufe zu Selbstjustiz und Hetzjagden unterbleiben.

6. Google

Die Durchführung der Datenschutzaufsicht und die Bearbeitung von Nutzerbeschwerden im Hinblick auf die Verarbeitung personenbezogener Daten durch die Google Inc. ist eines unserer Dauerthemen. Wir koordinieren für die anderen Aufsichtsbehörden der Länder die Aktivitäten und Kommunikation mit Google.

Abgesehen von den folgenden Themen (V. 6.1 – V 6.4) konnten wir in Gesprächen mit Google erreichen, dass auf Eingaben von Betroffenen direkter reagiert und die Nutzerführung bei der Einreichung von Beschwerden transparenter wird. Unser Ziel ist, dass die Betroffenen in die Lage versetzt werden, ihre Rechte wirksam und effektiv eigenständig geltend machen zu können. Google hat dazu unter anderem eine Seite veröffentlicht, auf der sich Nutzerinnen und Nutzer über ihre Rechte informieren und im Wege des Selbstdatenschutzes diese teilweise auch wahrnehmen können (https://support.google.com/). Durch die Verlagerung des Erstkontaktes der Petenten auf Google konnten wir eine Reduktion der Eingabezahlen in unserer Dienststelle erreichen. Die dadurch frei werdenden Ressourcen wurden jedoch durch die steten Veränderungen der Produkte und Nutzungsbedingungen von Google aufgebraucht.

Dennoch bleiben wir weiterhin Ansprechpartner für die Betroffenen, andere Aufsichtsbehörden, Politik und Verbände, soweit Fragen des Datenschutzes bei der Nutzung der Dienste des Unternehmens Google im Raum stehen.

6.1 Verfahren gegen die Google Datenschutzbestimmungen

Gemeinsam mit der Britischen (ICO), Französischen (CNIL), Italienischen (Garante), Niederländischen (CBL) und Spanischen (AGPD) Datenschutzaufsichtsbehörde nehmen wir an einem durch die CNIL auf der Ebene der Art-29-Datenschutzgruppe europaweit koordinierten Verfahren gegen die Google Inc. wegen der seit März 2012 geltenden Datenschutzbestimmungen sowie der Erstellung umfassender Nutzerprofile durch das Unternehmen teil.

Im März 2012 änderte die Google Inc. die bis dahin verwendeten Datenschutzbestimmungen. Das Unternehmen hatte uns vorab allgemein über die anstehenden Änderungen informiert. Bereits damals äußerten wir Bedenken bezüglich der datenschutzrechtlichen Zulässigkeit der in der Erklärung dargestellten Verfahren. Die bis dahin geltenden zahlreichen Regelungen zu einzelnen Google-Diensten sollten nach Angaben des Unternehmens in einer einheitlichen Regelung aufgehen und nunmehr global für sämtliche Dienste gelten. Bereits kurz nach dem Inkrafttreten der neuen Erklärung begann auch die Art-29-Datenschutzgruppe der EU, die sich aus den nationalen Aufsichtsbehörden und dem europäischen Datenschutzbeauftragten zusammensetzt, unter Führung der CNIL mit einer Untersuchung der Datenschutzbestimmungen. Die Bitte der Art-29-Datenschutzgruppe, vor der endgültigen Klärung der rechtlichen Zweifel an den neuen Datenschutzbestimmungen deren Anwendung vorläufig auszusetzen, lehnte Google ab. Trotz verschiedener Aktivitäten auf der Ebene der Art-29-Datenschutzgruppe war eine Klärung der im Raum stehenden Fragen nicht zu erreichen, so dass auf EU-Ebene vereinbart wurde, dass sechs Aufsichtsbehörden parallel nationale aufsichtsbehördliche Verfahren durchführen. Auch wir haben stellvertretend für die deutschen Aufsichtsbehörden gegen die Google Inc. ein Verwaltungsverfahren wegen der Verletzung von datenschutzrechtlichen Vorgaben, vorrangig denen aus dem Telemediengesetz, eingeleitet. Das Verfahren kann in dem Erlass einer Änderungs- bzw. Untersagungsanordnung nach § 38 BDSG münden.

Nach unserer Auffassung sehen wir drei wesentliche datenschutzrechtliche Vorgaben als verletzt an. Der zentrale Verstoß gegen die datenschutzrechtlichen Vorgaben und Kern unseres Verfahrens ist die fehlende Einwilligung bzw. gesetzliche Grundlage für das dienstübergreifende Zusammenführen sämtlicher Nutzungs- und Bestandsdaten und die damit einhergehende Erstellung von umfassenden und inhaltlich äußerst aussagekräftigen Nutzungs- und Interessensprofilen über Nutzerinnen und Nutzer. Google räumt sich in der Datenschutzerklärung das Recht ein, die gesetzlich vorgeschriebene

Trennung der bei der Nutzung von verschiedenen Diensten entstehenden personenbezogenen Informationen zu überwinden und sämtliche Daten miteinander zu verschneiden. Die Erhebung und Verknüpfung der Daten ist nach der Formulierung der Erklärung auch nicht auf bestimmte Datenkategorien beschränkt. Es besteht die Gefahr, dass Google individualisierte Profile erstellt, die detaillierte Auskünfte über die Interessen, Vorlieben, Kommunikationsbeziehungen und das Nutzungsverhalten enthalten. Aufgrund der Vielfältigkeit der angebotenen Dienste des Unternehmens berührt diese Form der Datenverarbeitung das Recht auf informationelle Selbstbestimmung. Wir fordern daher von Google, soweit gesetzliche Regeln diese Form der Datenverarbeitung nicht rechtfertigen, von den Nutzerinnen und Nutzern eine den Vorgaben des Telemediengesetzes bzw. Bundesdatenschutzgesetzes entsprechende Einwilligung einzuholen. Anderenfalls müsste die Profilerstellung untersagt werden.

Außerdem stellt die neue Datenschutzerklärung nicht hinreichend deutlich, transparent und bestimmt genug dar, zu welchem Zweck und in welchem Umfang Google personenbezogene Daten, vor allem die Nutzungsdaten, verarbeitet und nutzt. Wir haben daher von Google gefordert, ergänzend zu der bestehenden Erklärung den jeweiligen Diensten bzw. Dienstgruppen angepasste Informationen über Zweck sowie Art, Umfang und Dauer der Datenverarbeitung zu erstellen.

Schließlich sind wir der Auffassung, dass die Regelungen zu den Speicherfristen unzureichend sind und fordern entsprechend den gesetzlichen Vorgaben, Aufbewahrungszeiträume für die Nutzungsdaten festzulegen. Nach den Vorgaben des Telemedienrechts müssen die bei der Nutzung der Dienste anfallenden, personenbezogenen Daten unmittelbar nach der Beendigung gelöscht bzw. - soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen - gesperrt und die Länge der Speicherfristen für Inhaltsdaten auf das erforderliche Maß reduziert werden.

Auch wenn es sich um ein Verwaltungsverfahren auf den Grundlagen des nationalen Datenschutz- und Verfahrensrechts handelt, stehen wir in einem sehr engen inhaltlichen Austausch mit den beteiligten nationalen Aufsichtsbehörden, um eine größtmögliche Kohärenz zwischen den Forderungen der jeweils durchgeführten Verfahren mit den Verfahren in den anderen Mitgliedsstaaten zu erzielen.

6.2 Google WLAN Bußgeldverfahren

Die wegen einer fehlenden effektiven Datenschutzorganisation und -kontrolle erfolgte Erhebung und Speicherung von in unverschlüsselten WLAN übertragenen Daten wurde mit einem Bußgeld gegen die Google Inc. geahndet.

In den Jahren 2008 bis 2010 führte Google im gesamten Bundesgebiet, so auch in Hamburg, Fahrten mit speziell ausgerüsteten Fahrzeugen durch, um Daten für den Panoramadienst Google Street View zu erfassen (23. TB IV 3.5). Die dafür eingesetzten Fahrzeuge waren außer mit Kameras auch mit einem GPS-Ortungssystem, Einrichtungen zur Erfassung und Speicherung von Daten aus Funk-Netzwerken und der entsprechenden Software ausgestattet. Diese war durch Google entwickelt und auf dem System installiert worden. Nach Angaben des Unternehmens existierte bei der Entwicklung von Software ein Validierungsprozess, der u.a. auch die Beachtung datenschutzrechtlicher Vorgaben sicherstellen sollte. Jedoch soll dieser Prozess durch den Entwickler in diesem konkreten Fall nicht eingehalten worden sein. Daher kam es zu der Erhebung sämtlicher der in der Reichweite der Messeinrichtungen befindlichen WLAN ausgesendeten Informationen. Diese Informationen wurden georeferenziert erhoben und gespeichert. Zu den betroffenen Angaben bzw. Informationen gehörten GPS-Positionsdaten, MAC-Adressen, Service Set Identifier (SSID), Verschlüsselungsstatus des jeweiligen WLAN, Signalstärke, Funkkanal und Inhaltsdaten (sog. Payload Daten) unverschlüsselter WLAN. Zwar wurden auch verschlüsselte Daten erhoben, jedoch wurden diese unmittelbar aus dem System entfernt und nicht auf den Festplatten der Fahrzeuge gespeichert. Die unverschlüsselt erhobenen und gespeicherten Payload-Daten enthielten u.a. Namen und Anschriften, E-Mail-Adressen, Kommunikationsinhalte z.B. von E-Mails, Passwörter, URL-Adressen, Bilddateien, IP-Adressen, Suchanfragen in Suchmaschinen und nutzerbezogene Gerätenamen. Wir konnten die eingesetzten Festplatten einer technischen Prüfung unterziehen und eigene Erkenntnisse über die Art und den Umfang der Datenerhebung gewinnen.

Aufgrund dieser Erkenntnisse leiteten wir einerseits ein eigenes Bußgeldverfahren ein und stellten andererseits eine Strafanzeige bei der Staatsanwaltschaft Hamburg. Letztere mündete in ein Ermittlungsverfahren, welches jedoch Ende 2012 eingestellt wurde. In dem weiter anhängigen Bußgeldverfahren legten wir dem Unternehmen eine fahrlässige Missachtung der Vorgaben an eine datenschutzkonforme Aufbau- und Ablauforganisation zur Last. Nicht erweislich war, dass die Google Inc. bei der Erhebung dieser nicht allgemein zugänglichen personenbezogenen Daten vorsätzlich gehandelt hat. Deutlich wurde, dass zwar ein theoretisches Konzept der Überprüfung des Einsatzes neuentwickelter Technologien durch das Unternehmen existierte. Jedoch wurden diese Regeln nicht eingehalten und führten in dem konkreten Fall zu einer unbefugte Erhebung und Speicherung nicht allgemein zugänglicher Daten. Diese Ordnungswidrigkeit ahndeten wir mit einem Bußgeld in Höhe von 145.000 Euro. Dies

entspricht fast der in derartigen Fällen gesetzlich vorgesehenen Höchststrafe für die fahrlässige Begehung. Die Tatsache, dass Google im Verlauf des Verfahrens mit uns bezüglich der Aufarbeitung des Verstoßes kooperierte, hat zu einer leichten Reduzierung der Bußgeldhöhe geführt.

Rechtlich vertreten wir die durch Google bestrittene und von der Staatsanwaltschaft ebenfalls nicht geteilte Auffassung, dass personenbezogene Daten, die über ungesicherte WLAN transportiert werden, keine Daten aus einer allgemein zugänglichen Quelle im Sinne des BDSG sind. Allgemein zugänglich ist eine Quelle, wenn sie technisch geeignet und dazu bestimmt ist, einer unbestimmten Anzahl von Personen Zugang zu den entsprechenden Daten zu verschaffen. Die Allgemeinzugänglichkeit der betroffenen Netze wird nicht dadurch begründet, dass aus technischer Sicht keine besonderen Hürden zu überwinden sind, um die übertragenen Daten aus den ungesicherten WLAN auszulesen. Erforderlich ist vielmehr, dass die Betroffenen den Willen hatten, die Daten über das entsprechende Netzwerk der Allgemeinheit zur Verfügung zu stellen. Dies war erkennbar nicht der Fall, zumal der Betrieb privater unverschlüsselter WLAN in einer Vielzahl der Fälle zum damaligen Zeitpunkt auf das Unwissen über die Risiken der Betreiber zurückgeführt werden muss. Dennoch verbinden wir mit diesem Fall auch die Warnung an die Nutzerinnen und Nutzer, unverschlüsselte WLAN zu nutzen bzw. zu betreiben. Derartige Netze bieten keinen ausreichenden technischen Schutz gegen das unbefugte Auslesen der darüber transportierten Daten. Vertrauliche Informationen oder die Verwendung von Passwörtern sollten nicht ohne Schutzmaßnahmen, z.B. verschlüsselte Internetverbindungen (https://), versandt werden.

Rechtspolitisch zeigt dieses Verfahren, dass die geringen Sanktionshöhen keine abschreckende und disziplinierende Wirkung entfalten. Der derzeit diskutierte Entwurf der EU Datenschutzgrundverordnung sieht deutlich höhere Sanktionen vor und ist damit zu begrüßen.

6.3 Google Analytics

Die Firma Google hat weitere technische Möglichkeiten geschaffen, die es Webseitenbetreibern erleichtern, die gesetzlichen Anforderungen einzuhalten, wenn sie Google Analytics in ihre Angebote integrieren. Die konkrete Umsetzung bleibt in der Verantwortung der Webseitenbetreiber.

Im aktuellen Berichtszeitraum haben wir die Verhandlungen mit der Firma Google über Datenschutzverbesserungen für Google Analytics weitergeführt. Wie berichtet (23. TB, IV 4.1), hatten wir entscheidende Änderungen durchgesetzt, die deutschen Webseitenbetreibern in vielen Fällen einen beanstandungsfreien Einsatz von Google Analytics ermöglichen. Hierzu gehört das Schließen eines Auftragsvertrags nach § 11 BDSG sowie

eine entsprechende Konfiguration auf Produktebene durch den Webseitenbetreiber. Allerdings waren damit noch nicht alle Probleme gelöst. Die bei einer Reichweitenmessung und einem Nutzertracking relevanten Bestimmungen des Telemediengesetzes (TMG), insbesondere § 15 Abs. 3, sehen vor, dass der Nutzer widersprechen können muss, wenn er eine solche (pseudonyme) Erfassung nicht wünscht. Dies hatte Google zwar für die Browser ermöglicht, mit denen die Mehrheit der Nutzer von ihrem Standard-PC auf das World Wide Web zugreifen. Dabei kommt ein sog. Browser-Add-on zum Einsatz. Die entsprechende Technik wird allerdings nicht von allen Browsern unterstützt. Insbesondere Smartphone-Browser sind hier in aller Regel ausgenommen. Daher konnte bei Zugriffen von Smartphones dieses Widerspruchsrecht nicht oder nur mit erheblichem Aufwand für den Webseitenbetreiber umgesetzt werden.

Seitdem wurden weitere Ergänzungen durch Google vorgenommen, die mit allen Browsern, auch denjenigen von Smartphones, kompatibel sind. Es existiert nun ein Schalter im Programmcode von Google Analytics, durch den die Erfassung der Trackingdaten fallweise deaktiviert werden kann. Diesen Schalter kann ein Webseitenbetreiber verwenden, um den Widerspruch des Nutzers auch in den Fällen umzusetzen, in denen kein Browser-Add-on zur Verfügung steht. Dies ist unter https://developers.google.com/analytics/devguides/collection/gajs/?hl=de#disable beschrieben, einschließlich eines Programmier-Beispiels, das die entsprechende Interaktion mit dem Nutzer zeigt.

Alle Webseitenbetreiber, die Google Analytics einsetzen und auch Zugriffe von Smartphone-Browsern verzeichnen (insbesondere natürlich solche, deren Inhalte sich explizit an solche Nutzer richten), müssen sich um entsprechende Lösungen kümmern. Andernfalls ist ein gesetzeskonformer Betrieb nicht möglich.

Google Analytics kann auch für das Tracking von mobilen Apps auf Android- oder Apple-Geräten eingesetzt werden. Diese Analysen erfolgen auf Ebene einzelner Anwendungen für mobile Geräte und sind damit nicht an Browser bzw. den klassischen Internetzugriff gebunden. Auch für diese Erfassung sind Möglichkeiten vorhanden, das Tracking fallweise zu deaktivieren (siehe https://developers.google.com/analytics/devguides/collection/android/v3/advanced?hl=de#opt-out und https://developers.google.com/analytics/devguides/collection/ios/v3/advanced?hl=de#opt-out). App-Entwickler bzw. -Anbieter sollten diese Möglichkeiten nutzen, um den Widersprüchen der Nutzer zu entsprechen. Auch hier gilt: Ohne solche Opt-Out-Möglichkeiten ist ein gesetzeskonformer Betrieb einer App mit Einbindung von Google Analytics nicht möglich.

Unser Engagement für mehr Datenschutz bei Google Analytics hat sich nun offenbar auch auf europäischer Ebene ausgezahlt. Unter http://www.google.com/analytics/terms/dpa/dataprocessingamendment_20130906.html stellt das Unternehmen seit kurzem eine Fassung der Auftragsbedingungen für alle Länder zur Verfügung, die unter die EU-Datenschutzrichtlinie fallen.

6.4 Löschung von Suchergebnissen aus der Google Suchmaschine

Einen Großteil der Eingaben zum Unternehmen Google betreffen die Suchergebnisse der Suchmaschine des Unternehmens. Es gelang, mit Google ein Vorgehen zu vereinbaren, mit dem die Betroffenen ihre Rechte gegenüber Google primär selbst wahrnehmen können und nur in besonderen Situationen, z.B. wenn die Wahrnehmung der Rechte nicht erfolgreich ist, die Bearbeitung der Eingaben die Aufsichtsbehörde übernimmt.

Die Suchmaschine des Unternehmens Google verweist in der Regel auf Quellen, die außerhalb des Einflussbereiches des Unternehmens Google liegen. Lediglich für die im Cache gespeicherten Daten der Suchmaschine besteht eine datenschutzrechtliche Verantwortung des Betreibers. Die Löschung von Suchergebnissen mit Bezug zu personenbezogenen Daten setzt daher voraus, dass zuerst die entsprechenden Veröffentlichungen der Informationen in den Originalquellen gelöscht werden. Anderenfalls verweist die Suchmaschine erneut auf die betreffenden Informationen, und eine Bereinigung der Suchergebnisse ist erfolglos.

Sobald jedoch die Löschung der Informationen erfolgte, können Betroffene die Entfernung der Suchergebnisse aus dem Speicher der Suchmaschine selbst vornehmen. Dazu muss das auf der Seite der Google Inc. (https://support.google.com/websearch/troubleshooter/3111061) vorgesehene Verfahren durchlaufen werden.

In der Regel wird innerhalb einer Woche das Suchergebnis bereinigt sein. In den Fällen, in denen dies nicht erfolgt, bitten wir die Betroffenen, sich an den Kundensupport der Google Inc. zu wenden und die Probleme dort direkt zu schildern. Die entsprechenden Kontaktmöglichkeiten finden sich auf der genannten Seite. Denn wir sind nicht in der Lage, die Löschung von Einträgen selbst vorzunehmen. Unsere Kommunikation mit der Google Inc. erfolgt über die in Hamburg ansässige Deutschlandvertretung.

Nur in den Fällen, in denen auch nach einem direkten Kontakt die Google Inc. die Suchergebnisse nicht bereinigt, übernehmen wir die Bearbeitung von Eingaben. Dafür benötigen wir neben der Schilderung des konkreten Problems, ggf. auch unter Nennung des jeweiligen Links, die Bearbeitungsnummer (Ticketnummer), die durch den Kundensupport von Google vergeben wird. Dies ist für uns und Google unbedingt erforderlich, damit die Eingaben ordnungsgemäß bearbeitet werden können.
In seltenen Ausnahmefällen kann diese Vorgehensweise umgangen werden, und wir übernehmen die Eingaben direkt, z.B. in Fällen, in denen die Veröffentlichung einen Straftatbestand erfüllt oder besondere personenbezogene Daten betroffen sind und eine effektive Einwirkung der Betroffenen auf die Verantwortlichen der veröffentlichenden Stellen nicht möglich ist, z.B. weil diese sich im Ausland befinden oder sich bewusst einer Inanspruchnahme entziehen.

7. Facebook

Die Datenverarbeitung durch den sozialen Netzwerkbetreiber Facebook mit seinem derzeit weltweit größten und im Berichtszeitraum deutlich gewachsenen Sozialen Netzwerk, war immer wieder Gegenstand von aufsichtsbehördlichen Prüfungen.

Vergleichbar mit dem Unternehmen Google band der Dienst in hohem Maße unsere personellen Ressourcen in dem zuständigen Referat, aber auch in anderen Referaten (vgl. V. 4. und 5.). Während wir die Bearbeitung der individuellen Eingaben von Nutzerinnen und Nutzern dadurch senken konnten, dass die Facebook Inc. bzw. die Facebook Irland Ltd. unsere Forderungen nach einem besseren Kundensupport umsetzte, stand vor allem die Kontrolle der immer wieder vorgenommenen Änderungen der Datenschutzeinstellungen und –bestimmungen im Fokus unserer Tätigkeit. Auch wenn wir mit den Vertretern Facebooks eine aktive Kommunikation pflegen, wird seitens der Betreiber des Netzwerkes immer deutlich gemacht, dass diese eine Anwendung deutschen Datenschutzrechts ablehnen und die Auffassung vertreten, allein unter das Datenschutzrecht Irlands zu fallen. Wie wir bereits im 23. Tätigkeitsbericht darstellten (23. TB VI 3.3), vertreten wir die Auffassung, dass nur für einen kleinen Teil der Datenverarbeitung, nämlich die unmittelbar für die Umsetzung von Nutzersupportanfragen erforderliche Datenverarbeitung, die Facebook Irland Ltd. datenschutzrechtlich verantwortlich zeichnet und somit irisches Recht zur Anwendung kommt. Für grundlegende Entscheidungen über die Datenverarbeitung wie z.B. Art und Umfang der Nutzung personenbezogener Daten der Nutzerinnen und Nutzer zur Werbung oder biometrischen Auswertung ist die Facebook Inc. verantwortliche Stelle und hat damit auch die Vorgaben des nationalen Datenschutzrechts einzuhalten.

Wir vertreten die Auffassung, dass auch innerhalb des Europäischen Rechtsraumes sichergestellt sein muss, dass die Bestimmung der Anwendbarkeit datenschutzrechtlicher Vorschriften sich nach den tatsächlichen Gegebenheiten und den realen Entscheidungsstrukturen über die Datenverarbeitung in einem Unternehmen richten muss. Durch die bloße Behauptung einer datenschutzrechtlichen Verantwortlichkeit sollte nicht die Möglichkeit für Unternehmen eröffnet werden, sich das günstigste Recht oder die genehmste Aufsichtsbehörde aussuchen zu können. Ein „Forum-Shopping" der Unternehmen darf es im Hinblick auf einen möglichst effektiven Schutz der Persönlichkeitsrechte und des Datenschutzes als europäisches Grundrecht nicht geben. Das gilt es insbesondere für eine künftige einheitliche europäische Datenschutzordnung zu beachten.

7.1 Facebook Gesichtserkennung

Im 23. Tätigkeitsbericht (23. TB IV. 3.3) kündigten wir rechtliche Schritte gegen die Facebook Inc. wegen der unzulässigen Erstellung biometrischer Profile der Nutzerinnen und Nutzer des sozialen Netzwerkes an und erließen daraufhin in diesem Berichtszeitraum die entsprechende rechtliche Anordnung.

Wie bereits im 23. Tätigkeitsbericht ausführlich dargelegt, vertreten wir die Auffassung, dass die Verwendung digitaler Bilder zur Erstellung biometrischer Gesichtsprofile nicht ohne ausdrückliche Einwilligung der Betroffenen erfolgen darf. Facebook war nicht ohne weiteres bereit, diese Vorgaben umzusetzen. Es verwies auf die irische Rechtslage, da nach der Behauptung der Facebook Inc. für europäische Nutzerinnen und Nutzer die Facebook Irland Ltd. die verantwortliche Stelle sei. Es sei nach irischem Recht datenschutzrechtlich zulässig, auch ohne Einwilligung digitale Bilder zur Gesichtserkennung zu verarbeiten. Auch die irische Aufsichtsbehörde vertrat die Ansicht, dass durch das bloße Nutzen des Dienstes Nutzerinnen und Nutzer ihre Zustimmung in die biometrische Auswertung ihrer Bilder erteilen.

Wir haben zum einen die Konformität dieser Auslegung des irischen Datenschutzrechts mit den Vorgaben der europäischen Datenschutzrichtlinie bezweifelt und die Auffassung vertreten, dass für die Zulässigkeit einer derartigen Verarbeitung von Bilddaten eine Einwilligung erforderlich ist. Außerdem kommt nach unserer Auffassung zur Bewertung der Zulässigkeit der Gesichtserkennung bei deutschen Nutzerinnen und Nutzern deutsches Datenschutzrecht zur Anwendung.

Wir sehen uns in unserer Rechtsauffassung im Hinblick auf die Anforderungen an die Zulässigkeit der Gesichtserkennung durch die Stellungnahme der Art-29-Gruppe bestätigt. Danach ist die Erstellung dauerhafter biometrischer Gesichtsprofile z.B. durch Anbieter sozialer Netzwerke nur mit der ausdrücklichen Einwilligung der Betroffenen zulässig (Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten vom 22. März 2012). Ohne gesetzliche Grundlage ist die Erstellung derartiger Profile wegen der hohen Sensibilität der Informationen nur mit einer informierten und freiwillig erteilten Zustimmung der Betroffenen rechtlich zulässig.

Da diese Vorgaben durch die Facebook Inc. nicht beachtet wurden, erließen wir im September 2012 eine Verwaltungsanordnung. Mit dieser wurde das Unternehmen verpflichtet, deren Gesichtserkennungsverfahren auch rückwirkend datenschutzkonform zu gestalten. Neben der Verpflichtung zur umfassenden Information über das Verfahren war auch die Implementierung einer aktiven Einwilligung vor allem für die bereits registrierten Nutzerinnen und Nutzer Gegenstand der Anordnung. Parallel dazu hatten

weitere deutsche Aufsichtsbehörden angekündigt, eigene Verfahren einzuleiten und ggfs. entsprechende Anordnungen zu erlassen.

Nach Eingang des Widerspruchs und kurz vor unserer Entscheidung über diesen teilte der Netzwerkbetreiber mit, das Verfahren der Gesichtserkennung für europäische Nutzerinnen und Nutzer vorläufig einzustellen und bisher erstellte biometrische Profile zu löschen. Diese Ankündigung wurde zum Anlass genommen, die Anordnung zu widerrufen. Denn die Forderung nach der Implementierung eines Einwilligungsprozesses für ein nicht betriebenes Verfahren wäre zwecklos gewesen.

Entsprechend der Zusicherung durch Facebook und nach unserem Kenntnisstand soll für deutsche Nutzerinnen und Nutzer derzeit keine biometrische Auswertung von Bildern erfolgen. Jedoch wurde bei der letzten Änderung der globalen Datenverwendungsrichtlinie von Facebook die Gesichtserkennung in den Text mit aufgenommen und der Umfang der Auswertung sogar erweitert. Wir werden daher die Entwicklung weiterhin genau beobachten und, wie bereits bei dem Widerruf der Anordnung angekündigt, nicht zögern, erneut ein Verfahren einzuleiten, sollten die nationalen und europäischen Vorgaben bei der erneuten Einführung der Gesichtserkennung bei deutschen Nutzerinnen und Nutzern durch das Unternehmen nicht eingehalten werden.

7.2 Fanpages und Social Plugins

Bei der Nutzung der technischen Plattform des Dienstanbieters Facebook z.B. mittels Fanpages und Social Plugins zur Verfolgung eigener wirtschaftlicher Zwecke oder Erfüllung von staatlichen Aufgaben müssen private und öffentliche Stellen grundsätzlich die Vorgaben des nationalen Datenschutzrechts beachten (siehe auch V 4 und 5).

Der Soziale Netzwerkdienst des Unternehmens Facebook richtet sich nicht allein an private Nutzerinnen und Nutzer. Auch Wirtschaftsunternehmen und staatliche Einrichtungen werden durch Facebook umworben, ihre Inhalte und Angebote in das Netzwerk einzustellen und so die Attraktivität des Dienstes zu steigern. Die aktive Werbekampagne des Unternehmens zeigt Wirkung, und immer mehr staatliche und nichtstaatliche Stellen greifen auf das Dienstangebot zurück, um hauptsächlich Werbung, Marketing und Öffentlichkeitsarbeit zu betreiben.

Die Konferenz der Beauftragten für den Datenschutz des Bundes und der Länder und der Düsseldorfer Kreis hatten bereits 2011 festgestellt, dass der Einsatz von Social Plugins allgemein und im Besonderen der von Facebook, nur mittels Einwilligung der Betroffenen zulässig sei (sog. Zwei-Klick-Lösung). Im Berichtszeitraum haben wir diese Forderungen z.B. bei dem Dienstangebot www.hamburg.de durchgesetzt. Nach

den bisherigen Erkenntnissen werden durch die Einbindung von Social Plugins des Dienstanbieters Facebook umfangreiche Nutzungsdaten an Facebook übermittelt, ohne dass die Nutzerinnen und Nutzer darauf Einfluss nehmen konnten. Die von uns akzeptierte Zwei-Klick-Lösung, die rechtlich gesehen eine Einwilligung darstellt, kann die datenschutzrechtlichen Bedenken gegen den Einsatz dieser Funktionalität ausräumen. Dies setzt voraus, dass der Webseitenbetreiber hinreichende Informationen über die Art und den Umfang der durch die Nutzung des Social Plugins ausgelösten Verarbeitung zur Verfügung stellt und die Betroffenen selbst aktiv werden müssen, um in die Verarbeitung einzuwilligen. Dieses Vorgehen gilt im Übrigen auch für Social Plugins anderer Anbieter, bei denen vergleichbare Verfahren der Verwendung von Nutzungs- und Verkehrsdaten zur Anwendung kommen.

Da in der Regel die Webseitenbetreiber den Funktionsumfang und die entsprechenden Datenverarbeitungsprozesse nicht kennen, ist Facebook aufgefordert, über den Umfang der mit der Nutzung des Social Plugins ausgelösten Datenverarbeitung Klarheit herzustellen.
Vergleichbares gilt für den Einsatz von Fanpages, wobei hier jedoch die technische Realisierung datenschutzrechtlicher Vorgaben durch Facebook unterbunden wird. Fanpages sind Webseiten eines Unternehmens oder einer öffentlichen Stelle auf der technischen Plattform von Facebook. Die Gestaltungsmöglichkeiten der Fanpagebetreiber sind zwar gering. Dennoch tragen Fanpagebetreiber für die Inhaltsdatenverarbeitung personenbezogener Daten die datenschutzrechtliche Verantwortung und nicht Facebook. Die Beachtung und Einhaltung der datenschutzrechtlichen Grenzen der Erhebung, Verarbeitung, insbesondere Veröffentlichung und Nutzung personenbezogener Informationen und die Wahrung der Vertraulichkeit der über Facebook geführten nichtöffentlichen Kommunikation obliegt den Fanpagebetreibern. Inwieweit die datenschutzrechtliche Verantwortung der Fanpagebetreiber sich auf die Erhebung und Verarbeitung von Nutzungs- und Verkehrsdaten der Betroffenen, insbesondere die Reichweitenanalyse erstreckt, lässt sich derzeit rechtlich nicht mit hinreichender Sicherheit beantworten. Das VG Schleswig (Urteil vom 09. Oktober 2013, Az. 8 A 37/12, 8 A 14/12, 8 A 218/11) lehnte eine datenschutzrechtliche Verantwortung in einem Urteil gegen eine Verfügung des Unabhängigen Landeszentrums Schleswig-Holstein (ULD) ab. Die Entscheidung ist zwar nicht rechtskräftig und wird nach entsprechenden Ankündigungen des ULD durch das zuständige OVG überprüft werden. Wir beobachten die Entwicklung der Rechtsprechung genau und werden unsere Maßnahmen und Aktivitäten danach ausrichten.

7.3 Graph Search

Die flexible Suche von Facebook-Mitgliedern anhand ihrer Daten und Aktivitäten eröffnet den Nutzern eine Vielzahl neuer, teilweise weit reichender Recherchemöglichkeiten. Die Bedeutung der Privatsphäreeinstellungen wird dadurch weiter erhöht.

Im Frühjahr 2013 kündigte die Firma Facebook eine neue Funktion innerhalb des sozialen Netzwerks an. Über eine flexible, nahezu in natürlicher Sprache formulierbare Suchanfrage können mit Graph Search Nutzer des Netzwerks gefunden werden, die bestimmte Kriterien erfüllen. Gesucht bzw. gefunden werden können so z.B. „Personen, die gerne Fahrrad fahren und aus meiner Heimatstadt stammen" oder „Restaurants in London, die meine Freunde besucht haben".

Während der Sinn solcher eher harmlosen Beispiele einleuchten mag, sind auch (nicht nur) aus Datenschutzsicht deutlich problematischere Anfragen möglich. Um ein häufig zitiertes Beispiel zu nennen: „Single-Frauen, die in der Nähe wohnen, an Männern interessiert sind und sich gerne betrinken". Derartige Anfragen fördern Nutzer(innen) zu Tage, die die Tragweite ihrer persönlichen Angaben in dem sozialen Netzwerk möglicherweise nicht vollständig übersehen oder jedenfalls nicht mit der Transparenz rechnen, die Graph Search dem sozialen Netzwerk verleiht.

Seit Sommer 2013 ist diese Suchfunktion auch in Deutschland verfügbar, bislang allerdings nur in englischer Sprache. Die oben genannten Beispiele können so also nicht verwendet werden; es muss zunächst die Sprache auf Englisch umgestellt werden. Dies mag die Nutzungsfrequenz hierzulande einschränken – die damit verbundenen Risiken reduziert es nicht. Denn auch wenn man Graph Search selbst nicht nutzt, kann das eigene Profil von einer entsprechenden Graph-Search-Anfrage erfasst werden. Die Grundmenge, auf die sich jede Suchanfrage bezieht, ist das gesamte Facebook-Universum.

Allerdings berücksichtigt Graph Search jeweils nur diejenigen Daten, auf die der Nutzer, der eine Anfrage stellt, sowieso zugreifen kann. Dementsprechend können Details des eigenen Profils, die nur einem eingeschränkten Personenkreis (z.B. den Facebook-Freunden) zugänglich sind, auch nur von diesem Personenkreis bei einer Suche ausgewertet werden. Gibt man seinen Beziehungsstatus oder seine Vorliebe fürs Fahrradfahren nicht für alle Nutzer sichtbar bekannt, kann man von Fremden bei entsprechenden Suchen auch nicht gefunden werden.

Die Herausforderung liegt daher auf Seiten der Nutzer. Sie müssen sich stärker als je zuvor um den für sie passenden Zugriffschutz für ihre Facebookdaten kümmern. Das Vertrauen darauf, in der großen Menge der Facebook-Nutzer zu verschwinden oder nur für diejenigen erkennbar zu sein, mit denen man sowieso in einem engeren Austausch steht, ist nicht mehr ausreichend.

Facebook bietet die nötigen Instrumente zum Schutz des eigenen Profils. Zwar sind die Standardeinstellungen weit gewählt, was von Seiten der Datenschutzbeauftragten wiederholt kritisiert wurde. Doch jeder Nutzer ist in der Lage, die Vorgaben auf das gewünschte Maß zu reduzieren und z.B. nur Freunde oder bestimmte Personen an seinen Veröffentlichungen und Informationen teilhaben zu lassen.

Hilfreich ist dabei die Anzeigemöglichkeit des eigenen Profils aus der Sicht eines anderen („Anzeigen aus der Sicht von ..."). Alle Daten, die unter der Ansicht „Öffentlich" sichtbar sind, können bei einer Graph-Search-Suche durch jedes andere Facebook-Mitglied ausgewertet werden. Jeder sollte sich kritisch fragen, ob dies wirklich der gewünschte Zustand ist.

Da seit kurzem auch Minderjährige ihre Beiträge für die Öffentlichkeit sichtbar machen können, gilt die entsprechende Vorsicht in besonderem Maße für Jugendliche bzw. deren Eltern. Gerade in diesem Alterssegment dürfte eine weltweite Auffindbarkeit des eigenen Profils auf Grundlage der veröffentlichten Inhalte in aller Regel unerwünscht sein.

8. Xing – Auftragsdatenverarbeitung und CDN

Die Xing AG überprüfte ihre Auftragsdatenverarbeitungsverträge und zieht technische Maßnahmen zur Verbesserung des Schutzes der personenbezogenen Daten der Nutzerinnen und Nutzer in Erwägung.

Im Berichtszeitraum führten wir regelmäßig mit der Xing AG Prüfungs- und Beratungstermine durch. Als vorteilhaft erwies sich dabei die grundsätzliche Aufgeschlossenheit des Unternehmens, datenschutzrechtliche Probleme gemeinsam mit der Aufsichtsbehörde zu lösen und ggfs. nach Best-Practice-Ansätzen zu suchen. Neben Einzeleingaben zur Verarbeitung und Nutzung personenbezogener Daten und der datenschutzkonformen Ausgestaltung einzelner Features des Netzwerkes oder besonderer Dienste z.B. der Xing-App, stand vor allem die Ausgestaltung der Auftragsdatenverarbeitungsverhältnisse des Betreibers mit seinem Content-Delivery-Network (CDN) im Fokus der aufsichtsbehördlichen Prüftätigkeit.

CDNs unterstützen Anbieter von Webdiensten, die für den Betrieb des Dienstes erforderlichen Daten möglichst ohne hohe Verzögerung an Nutzerinnen und Nutzer auszuliefern. Da CDNs in dieser Funktion keine eigenen Inhalte anbieten und kein eigenes wirtschaftliches Interesse an den übertragenen personenbezogenen Daten haben, sondern diese lediglich unter technischen Gesichtspunkten ausliefern, werden die CDNs als Auftragsdatenverarbeiter i.S.d. § 11 BDSG tätig.

Auch die Xing AG bedient sich eines derartigen CDN. Aufgrund einer Eingabe und entsprechender Medienberichte prüften wir die Konformität der geschlossenen Auftragsdatenverarbeitungsverträge mit den datenschutzrechtlichen Vorgaben. Dazu zählten z.B. die Begrenzung und rechtlich verbindliche Festlegung der Zwischenspeicherzeiten personenbezogener Daten durch die XING AG gegenüber dem CDN-Betreiber.

Außerdem diskutieren wir derzeit – nunmehr auch unter dem Eindruck der Enthüllungen der NSA-Spähaffäre – mit der Xing AG technische Möglichkeiten, den unberechtigten Zugriff Dritter durch die Gestaltung der Übertragungstechnik zu erschweren, indem die Auslieferung von Daten möglichst über in der EU belegene Infrastrukturen realisiert wird, und wie entsprechende Verschlüsselungsverfahren zum Einsatz kommen können.
Die Arbeit mit diesem Unternehmen zeigt deutlich, dass seitens der deutschen Internetwirtschaft durchaus Bedarf an einer fundierten datenschutzrechtlichen Beratung vor allem im Hinblick auf Best-Practice-Ansätze besteht. Wir tun alles, um im Rahmen unserer begrenzten personellen Ressourcen diesen Bedarf zu erfüllen.

9. Datenschutz und Online-Dating

Bei der Prüfung der Verfahren eines Online-Dating Portal Betreibers wurden durch uns schwere Mängel festgestellt.

Aufgrund von Eingaben Betroffener und Medienberichten leiteten wir gegen den Betreiber einer Online Partner-Börse ein Prüfverfahren ein. Der Hauptvorwurf bezog sich auf das umfassende Erheben von E-Mail-Adressen aus den Adressbüchern von Nutzerinnen und Nutzern und die Verwendung dieser Angaben zur Bewerbung des eigenen Angebotes.
Nach ersten Schwierigkeiten in der Kommunikation mit uns und einer kurzfristigen „Verlegung" des Firmensitzes von Hamburg in die USA, die jedoch kurze Zeit später wieder zurückgenommen wurde, kooperierte das Unternehmen unter einer neuen Geschäftsführung mit uns.

Bei einer erfolgten Prüfung der Verfahren und Systeme vor Ort stellten wir fest, dass das Unternehmen in großem Umfang E-Mail-Adressen gespeichert hatte, ohne eine entsprechende Rechtsgrundlage für die Speicherung nachweisen zu können. Außerdem setzte das Unternehmen einen Auftragsdatenverarbeiter mit Sitz in der Ukraine ein, ohne die für ein derartiges Verhältnis erforderlichen Vertragsunterlagen und damit einhergehenden rechtlichen Bindungen geschaffen zu haben.

Die Erhebung erfolgte durch das Auslesen von Adressbüchern bzw. die Eingabe der

Mailadressen durch Nutzerinnen und Nutzer, die sich einen Überblick verschaffen wollten, wer bereits von den eigenen Kontakten in dem Netzwerk registriert war. Das Vorgehen glich dem bereits im 23. TB beschrieben Friend-Finding des Netzwerkbetreibers Facebook (vgl. 23. TB IV 3.2). Nach unseren Erkenntnissen erhob und speicherte das Unternehmen E-Mail-Adressen im siebenstelligen Bereich, ohne dafür die Einwilligung der Betroffenen oder eine sonstige Rechtsgrundlage vorlegen zu können. Aufgrund dieser Feststellungen forderten wir in einem ersten Schritt das Unternehmen auf, die unzulässig erhobenen Daten zu löschen. Dieses wurde zwischenzeitlich umgesetzt.

Außerdem thematisierten wir die Einbindung des ukrainischen Unternehmens in die Wartung der Datenbanken. Die Mitarbeiter dieses Unternehmens haben vollen Zugriff auf die personenbezogenen Daten der Mitglieder des Portals. Aufgrund der Tatsache, dass es sich bei dem Auftragsdatenverarbeiter um ein Unternehmen mit Sitz außerhalb der EU handelt, stellten wir sicher, dass zwischen dem Betreiber neben dem Abschluss eines den Vorgaben des § 11 BDSG entsprechenden Vertrages auch ein den europäischen Standardvertragsklauseln entsprechender Vertrag geschlossen wurde, um ein angemessenes Datenschutzniveau im Sinn des § 4 b BDSG seitens des Auftragsdatenverarbeiters sicherzustellen.

Zu guter Letzt prüften wir die datenschutzrechtlichen Auswirkungen der Verlegung des Hauptsitzes des Unternehmens in die USA. Nach Angaben des Betreibers wurde ein administrativer Zugriff von den USA auf die Datenbanken des Portals nicht festgestellt.
Nach unserer Prüfung wurden die festgestellten Mängel durch die verantwortliche Stelle beseitigt. Eine abschließende Entscheidung über die Sanktionierung der Verstöße war wegen der geringen personellen Ressourcen in dem zuständigen Referat im Berichtszeitraum bedauerlicherweise nicht möglich.

10. Abgeordnetenwatch.de

Die Veröffentlichung von bereits im Internet veröffentlichten Angaben über Mandatsträgerinnen und -träger kommunaler Volksvertretungen auf dem Internetportal ist nach einer Prüfung nunmehr datenschutzrechtlich nicht zu beanstanden.

Aufgrund einer Eingabe überprüften wir die datenschutzrechtliche Zulässigkeit der Veröffentlichung von personenbezogenen Daten von kommunalen Mandatsträgerinnen und –trägern sowie die Zulässigkeit des Aufbaus eines digitalen Wählergedächtnisses durch den Betreiberverein Parlamentwatch e.V. (http://www.abgeordnetenwatch.de). Auf dessen Plattform wurden bisher Angaben von Parlamentariern des Bundestages und der Landtage veröffentlicht und Nutzerinnen und Nutzern die Gelegenheit gege-

ben, sich über die Personen, deren Abstimmungsverhalten oder Tätigkeiten zu informieren und direkt mit diesen über den Dienst in Kontakt zu treten. Nutzerinnen und Nutzer sind in der Lage, öffentlich an die Parlamentarier Fragen zu stellen. Eingehende Antworten werden ebenfalls veröffentlicht bzw. mitgeteilt, dass die Frage nicht beantwortet wurde. Fragen und Antworten unterliegen einer Inhaltskontrolle entsprechend dem auf der Seite veröffentlichten Moderationskodex.

Die Betreiber erweiterten während des Berichtszeitraumes ihr Angebot auch auf Mandatsträgerinnen und Mandatsträger kommunaler Volksvertretungen. Aufgrund der Eingabe eines kommunalen Spitzenverbandes zur Zulässigkeit der Veröffentlichung der Daten auf dieser Plattform und der Veröffentlichung der Kommunikation setzten wir uns mit der datenschutzrechtlichen Zulässigkeit des Dienstes auseinander. Die Hauptbesorgnis des Petenten lag in der befürchteten stigmatisierenden Wirkung der Veröffentlichung der Informationen und der Kommunikation vor allem dann, wenn die Mandatsträgerinnen nicht in der Lage oder willens sind, über diese Plattform zu kommunizieren. Denn in der Regel handelt es sich anders als bei den Landes- und dem Bundesparlament nicht um Berufsparlamente. Auch wurde die öffentliche Bedeutung der Funktion kommunaler Vertretungen nicht derart hoch eingeschätzt, dass deren Vertreter eine Veröffentlichung ihrer personenbezogenen Daten dulden müssten.

Wir haben nach einer umfassenden Prüfung und schriftlichen Stellungnahme erreicht, dass die Veröffentlichung der personenbezogenen Daten der Mandatsträgerinnen und –träger nur unter bestimmten Voraussetzungen entlang der Rechtsprechung des BGH zu Spick-mich.de zulässig ist. Zu betonen ist, dass wir nur die datenschutzrechtliche Zulässigkeit der Veröffentlichung der Angaben auf dem Internetangebot des Betreibers Parlamentwatch e.V. geprüft haben. Die Zulässigkeit der originären Einstellung personenbezogener Daten auf den Internetangeboten der jeweiligen Kommunen und Gemeinden unterliegt den entsprechenden landesrechtlichen Datenschutzgesetzen oder kommunalen Satzungen, auf die sich unsere Prüfkompetenz nicht erstreckt. Wir haben auf der Grundlage der Vorgaben des BDSG und TMG die Zulässigkeit des Angebotes geprüft. Danach dürfen Angaben wie Name, Geschlecht, E-Mail-Adresse, Parteizugehörigkeit und Zeitraum der Mandatsausübung von Mitgliedern kommunaler Volksvertretungen für die Zwecke des Aufbaus einer Datenbank auf der Internetseite abgeordnetenwatch.de ohne Einwilligung gemäß § 29 Abs. 1 Nr. 2 BDSG veröffentlicht werden. Dies setzt jedoch voraus, dass die betreffenden Informationen bereits aus dem Internet entnommen wurden, also allgemein zugänglich sind. Die Aufgabe und Bedeutung der mandatsbezogenen Tätigkeit der Betroffenen bedingt, dass diese einen Eingriff in ihre Persönlichkeitsrechte in diesem Umfang dulden müssen. Die Veröffentlichung darüber hinausgehender Angaben ist hingegen nur mit der vorherigen Einwilligung der Betroffenen zulässig. Widersprüche der Betroffenen gegen die Veröffentlichung dieser Angaben ohne Einwilligung sind beachtlich, wenn durch die Veröffentlichung weitergehende Individualinteressen der Betroffenen beeinträchtigt werden.

Im Hinblick auf die veröffentlichte Kommunikation zwischen den Nutzerinnen und Nutzern und den Mitgliedern der kommunalen Volksvertretungen wurde der Betreiber durch uns verpflichtet sicherzustellen, dass keine stigmatisierenden Wirkungen entstehen können. Dies gilt z.B. dann, wenn Betroffene aufgrund begrenzter eigener Ressourcen nicht in der Lage sind, auf massenhaft eingehende Fragen zu antworten. Der Betreiber muss gewährleisten, dass in derartigen und vergleichbaren Fällen dem Umstand ausreichend Rechnung getragen wird, dass es sich bei diesen Mandatsträgerinnen und -trägern größtenteils um ehrenamtliche und in ihrer Freizeit tätige Personen handelt.

Außerdem haben wir die zeitlich unbegrenzte Speicherung von Profilen der Betroffenen untersagt und den Betreiber aufgefordert, ein an den Zwecken des Dienstes ausgerichtetes Speicherkonzept vorzulegen.

Bei der Gesamtbewertung dieses Dienstes strebten wir eine ausgewogene Balance zwischen den berechtigten Interessen der Betroffenen an der Wahrung ihrer Persönlichkeitsrechte und der Förderung der öffentlichen Teilhabe an und Transparenz von kommunalen Entscheidungen an. Diese herzustellen fällt jedoch nicht immer leicht. Die Tatsache, dass am Ende sämtliche Beteiligte sich mit der von uns getroffenen Einschätzung arrangiert haben, erscheint uns als Zeichen, dass wir in diesem konkreten Fall einen guten Ausgleich der Interessen gefunden haben.

11. Private Fahndung in Sozialen Netzwerken

Die Verwendung Sozialer Netzwerke zur privaten „Fahndung" nach mutmaßlichen Tätern unter Ausnutzung der sogenannten viralen Effekte mag in Einzelfällen menschlich nachvollziehbar sein, verstößt jedoch gegen das Datenschutzrecht.

Immer wieder erhalten wir Hinweise auf die Veröffentlichung personenbezogener Daten in Profilen und auf Seiten in Sozialen Netzwerken und vergleichbaren Diensten durch private Personen mit dem Zweck der „Fahndung". Gesucht werden oft Personen, die von der Nutzerin oder dem Nutzer verdächtigt werden, Straftaten begangen zu haben oder die mit Verhaltensweisen aufgefallen sind, die als sozial inadäquat angesehen werden. Das Ziel ist häufig, die hohe Geschwindigkeit der Verbreitung von Informationen und die erzielbare große Reichweite der Sozialen Medien zu nutzen.

Die Veröffentlichung von personenbezogenen Daten an einen unbestimmten Empfängerkreis mit dem Ziel, größtmögliche Aufmerksamkeit zu erzeugen, ist nur dann zulässig, wenn die Person, die diese Daten veröffentlicht, sich auf eine entsprechende Rechtsgrundlage berufen kann. Zwar existiert eine Rechtgrundlage in § 28 BDSG, wonach zur

Verfolgung berechtigter Interessen die Verarbeitung personenbezogener Daten zulässig ist. Jedoch setzt dies voraus, dass die Veröffentlichung zum einen für die Verfolgung der berechtigten Interessen erforderlich ist und außerdem keine schutzwürdigen Interessen der Betroffenen der Veröffentlichung entgegenstehen.

Bereits die Frage nach der Erforderlichkeit der privaten Veröffentlichung von Bildern oder vergleichbaren personenbezogenen Informationen muss in der Regel verneint werden. Nach dem rechtsstaatlichen Verständnis des Grundgesetzes liegt die Verantwortung für die Ahndung von Straftaten und Ordnungswidrigkeiten auf Seiten des Staates. Fahnden Private auf sozialen Netzwerken, übernehmen sie Aufgaben, die ausschließlich den staatlichen Stellen, insbesondere Strafverfolgungsbehörden zugewiesen sind. Das Gewaltmonopol liegt beim Staat. Allein der Umstand, dass die Erstattung einer Strafanzeige bei der Polizei oder Staatsanwaltschaft umständlicher und zeitaufwändiger ist, rechtfertigt nicht, dieses Grundprinzip zu missachten. Betroffene, selbst wenn sie Anlass für eine Nachforschung gegeben haben sollten, haben einen Anspruch auf ein rechtsstaatlich geordnetes Verfahren bezüglich der Feststellung ihrer Identität und der Ahndung etwaiger Verstöße.
Außerdem muss auch die Frage nach der Verhältnismäßigkeit einer derartigen Fahndung als Abwägung zwischen den verfolgten Interessen durch die fahndende Person und den schutzwürdigen Interessen der Betroffenen bewertet werden. In Betracht zu ziehen ist dabei einerseits die Unschuldsvermutung und andererseits die mit der Veröffentlichung in Sozialen Netzwerken zusammenhängenden Risiken.

So kann sich der sogenannte virale Effekt der Verbreitung von Informationen zu einem öffentlichen Pranger entwickeln oder in eine virtuelle Hetzjagd umschlagen und zu einer Vorverurteilung des Betroffenen führen. Die ursprünglich veröffentlichende Person verliert in der Regel die Kontrolle über die einmal veröffentlichten Informationen und kann die Entwicklungen nicht mehr beeinflussen. Die stigmatisierende Wirkung virtueller Pranger oder die kampagnenartige Mobilisierung der öffentlichen Meinung gegen einzelne Personen sind keine rechtsstaatlichen Formen der Ahndung von Verstößen. Abgesehen davon, dass der bloße Verdacht allein für die Feststellung eines Verstoßes nicht ausreicht, obliegt es neutralen staatlichen Stellen, die vorgesehenen Strafen festzulegen und diese zu vollziehen.
Die zweifellos in Einzelfällen verständlichen Emotionen der Geschädigten und die Empfindung, staatlicherseits vorgesehenen Sanktionsverfahren seien unzureichend und behäbig, dürfen nicht dazu verleiten, einem digitalen Faustrecht das Wort zu reden. Die digitale Jagd nach dem Täter verstößt nicht allein gegen die verfassungsrechtlichen Rechte des Einzelnen, sondern berührt auch die rechtsstaatlichen Prinzipien unserer Gesellschaft.

12. Das Ausspähprogramm PRISM und die US-Diensteanbieter

Das Internet und andere Kommunikationsinfrastrukturen unterliegen offenbar einer umfassenden, flächendeckenden und anlasslosen Überwachung durch verschiedene Geheimdienste. Neben dem Umstand der Überwachung an sich sind vor allem fehlende Transparenz über das Ausmaß der Ausspähung und der Beteiligung maßgeblicher Internetunternehmen an diesen Aktivitäten und die fehlenden Kontrollmöglichkeiten Grund für Sorgen um die Rechtsstaatlichkeit dieses Vorgehens.

Mitte 2013 legte der ehemalige Geheimdienstmitarbeiter Edward Snowden umfangreiche Materialen offen, die belegen, dass die NSA (National Security Agency), der größte Auslandsgeheimdienst der USA, gemeinsam mit dem GCHQ (Government Communications Headquarters), einem britischen Nachrichtendienst, umfassend und ohne erkennbare Begrenzung die über das Internet getätigte Kommunikation ausspähen. Die Unterlagen geben Hinweise darauf, dass diese Aktivitäten unter Beteiligung einiger Internetunternehmen erfolgten. Im Zusammenhang mit dem Programm „PRISM" wurden Unternehmen wie Google, Facebook und AOL genannt, die der datenschutzrechtlichen Aufsicht durch uns unterliegen. Wir haben daraufhin diese Unternehmen zu einer Stellungnahme aufgefordert.
Alle Unternehmen reagierten auf unsere Anfrage mit einer im Kern gleichlautenden Antwort. Sie bestritten sowohl eine Beteiligung an den Aktivitäten als auch jede weitergehende Kenntnis darüber. Die Antworten enthielten keine Informationen, die nicht bereits in den durch die Unternehmen offiziell herausgegebenen Statements enthalten waren.

Nachdem nachträglich Informationen auftauchten, in denen der Verdacht geäußert wurde, dass die NSA sogar eigene technische Infrastrukturen in den Unternehmen untergebracht hatte und Entschädigungszahlungen an diese geleistet worden seien, hakten wir nochmals nach. Offenbar waren die Unternehmen selbst Opfer von gezielten Aktivitäten der Geheimdienste, indem deren technische Sicherungen wie etwa dedizierte Kommunikationsleitungen überwunden wurden.

Aus dem letztlich erfolglosen Versuch, Klarheit über das konkrete Ausmaß der Überwachung und die Beteiligung von Unternehmen an dieser zu gewinnen, muss der Schluss gezogen werden, dass ein effektiver Schutz der Nutzerinnen und Nutzer vor der unverhältnismäßigen Ausspähung durch staatliche Geheimdienste nur durch staatliche Maßnahmen bewerkstelligt werden kann. Transparenz über Geheimdienst-tätigkeiten herzustellen, kann nicht den Unternehmen überlassen sein. Vor allem dann nicht, wenn gesetzliche Regeln die Herstellung von Transparenz unter Strafe stellen. Vertraulichkeit und Integrität der Kommunikation im Internet muss und kann nur nach-

haltig durch den Staat und die demokratische Begrenzung seines Informationsinteresses hergestellt werden.

Die Initiativen von Google und Facebook, mehr Transparenz über staatliche Auskunftsbegehren über Nutzerdaten zu schaffen, begrüßen wir ausdrücklich.
Zusätzlich und flankierend sind solche technischen Maßnahmen erforderlich, die die Vertraulichkeit gespeicherter und übermittelter Daten weitgehend sicherstellen. Diese Kernanforderung des Datenschutzes muss anlässlich der Enthüllungen Edward Snowdens übergreifend in den Fokus rücken.

V.

DATENSCHUTZ IM NICHT-ÖFFENTLICHEN BEREICH VI.

1. Die Europäische Datenschutz-Grundverordnung 210
2. Internationaler Datenverkehr 214
3. Justiz 218
4. Versicherungswirtschaft 220
5. Handel 225
6. Auskunfteien 229
7. Transport und Verkehr 233
8. Videoüberwachung 238
9. Wohnungswirtschaft 242
10. Werbung 247
11. Bußgeldfälle und Anordnungen 249
12. Meldepflicht und Prüftätigkeit 250

1. Die Europäische Datenschutz-Grundverordnung

1.1 Überblick

Sowohl die immer dringender werdende Notwendigkeit der Vereinheitlichung des Datenschutzes in Europa als auch die sich zügig entwickelnde Technologie über alle Grenzen hinweg macht ein einheitliches Datenschutzrecht für Europa unerlässlich.

Seit dem ersten Bundesdatenschutzgesetz in Deutschland von 1977 hat es im Hinblick auf die Gefährdungen der informationellen Selbstbestimmung des Einzelnen eine derart rasante Entwicklung gegeben, dass zwischenzeitlich immer wieder Anpassungen an die Lebenswirklichkeit notwendig wurden. Dabei hat sich schon früh gezeigt, dass ein auf Deutschland begrenzter Datenschutz weder ausreicht, die personenbezogenen Daten unter Berücksichtigung der zunehmenden Europäisierung und Globalisierung zu schützen, noch den Herausforderungen des Internetzeitalters gerecht zu werden.

Zuletzt wurde auf europäischer Ebene im Jahre 1995 eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr verabschiedet. Diese Richtlinie hatte schon zum damaligen Zeitpunkt eine Vereinheitlichung des Datenschutzrechts in ganz Europa zum Ziel. Allerdings ist es das Wesen einer Richtlinie, dass sie nicht direkt, sondern erst nach Umsetzung durch die Mitgliedstaaten der Europäischen Union (EU) im jeweiligen Land gilt. Trotz der darin enthaltenen Umsetzungsfrist von drei Jahren hat es bis zur Novellierung des Bundesdatenschutzgesetzes (BDSG) mit der erforderlichen Anpassung an diese Richtlinie sechs Jahre gedauert. Besonders hervorzuheben ist in diesem Zusammenhang die Vorgabe der EU-Richtlinie, dass die Kontrollstellen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrzunehmen haben.

Seit der Anpassung des BDSG an die Richtlinie von 1995 im Jahre 2001 gab es mehrere Novellierungen, zuletzt 2009. Wichtige Änderungen des BDSG hat es dabei im Bereich der Auskunfteien, des Scoring, der Werbung, des Beschäftigtendatenschutzes, des Auskunftsrechts Betroffener, der Informationspflichten von Unternehmen und der Bußgeldvorschriften gegeben. All dies reicht aber nicht aus, auch nur annähernd verlässlich sicherzustellen, dass persönliche Daten im Umfeld des Internet geschützt werden. Darüber hinaus gab es selbst in den europäischen Ländern durchaus unterschiedliche Umsetzungen der Richtlinie von 1995, so dass von einer vollständigen Vereinheitlichung des Datenschutzrechts in Europa bisher nicht die Rede sein kann.

Diesem Umstand versucht der am 25. Januar 2012 veröffentlichte Entwurf der EU-Kommission Rechnung zu tragen, der aus folgenden drei Teilen besteht:

- Mitteilung über die politischen Ziele der Kommission.

- Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung).
- Richtlinie zum Schutz personenbezogener Daten, die zum Zweck der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten und für damit verbundene justizielle Tätigkeiten verarbeitet werden.

Insbesondere über die Datenschutz-Grundverordnung hat es bisher endlose Diskussionen gegeben, so dass wir uns an dieser Stelle auf einige Aspekte dieses Regelwerkes beschränken.

Erklärtes Ziel der EU-Kommission ist es, mit der technikneutralen Datenschutz-Grundverordnung zu einer Harmonisierung des Datenschutzes in Europa zu gelangen. Erreicht werden soll, dass gerade durch die Wahl einer unmittelbar geltenden Verordnung eine Einheitlichkeit des Datenschutzes in Europa durchgesetzt wird. Die in der Verordnung enthaltenen Regelungen sollen sowohl für die Behörden, als auch für die Unternehmen gleichermaßen gelten. In Deutschland gilt das BDSG ebenfalls für die (Bundes-) Behörden und die privaten verantwortlichen Stellen, allerdings gelten viele Vorschriften innerhalb des BDSG entweder nur für Behörden oder nur für Private. Daneben gibt es noch in jedem Bundesland ein Landesdatenschutzgesetz, das ausschließlich für die öffentlichen Stellen des jeweiligen Landes gilt.

Der Entwurf der Datenschutz-Grundverordnung enthält viele Komponenten, die eine deutliche Verbesserung, insbesondere hinsichtlich des einheitlichen Datenschutzes in Europa und der Anwendbarkeit auch für außereuropäische Unternehmen erwarten lassen. Daneben gibt es jedoch auch aus unserer Sicht Punkte, die zu kritisieren sind. Insgesamt hat es Tausende von Änderungsvorschlägen zu diesem Entwurf gegeben, so dass zum jetzigen Zeitpunkt nicht deutlich ist, ob die guten Ansätze des Entwurfs sich überhaupt noch durchsetzen können oder die Kritikpunkte der Datenschutzaufsichtsbehörden sich in entsprechenden Verbesserungen niederschlagen.

Nach Veröffentlichung des Entwurfs hat es Änderungsvorschläge der Regierungen aus jedem Land der europäischen Union, von Unternehmensverbänden, Organisationen, der Wissenschaft und den jeweiligen Datenschutzaufsichtsbehörden gegeben. Daneben versuchen aber auch außereuropäische Unternehmen, Regierungen und viele andere, ihren Einfluss geltend zu machen. Daher ist zum jetzigen Zeitpunkt noch nicht vollständig absehbar, welchen konkreten Text die Verordnung haben wird und ob das Ziel eines besseren Datenschutzes für ganz Europa erreicht werden kann.

Nachdem sich der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des europäischen Parlaments intensiv mit dem Entwurf der Kommission auseinandergesetzt hatte, legte der Berichterstatter im Januar 2013 den Entwurf eines Berichts des Europäischen Parlaments vor, der zahlreiche Änderungsvorschläge enthielt. Dieser Bericht ist abrufbar unter: http://www.europarl.europa.eu.

Derzeit beschäftigen sich Rat, Parlament und Kommission intensiv mit mehr als 3000 Änderungsvorschlägen, die aus allen Bereichen eingegangen sind.

Es wurde zwar zunächst davon ausgegangen, dass die Regelung bereits im Jahr 2014 in Kraft treten würde, ob dies jedoch in die Realität umgesetzt werden kann, ist nicht absehbar. Mitte Oktober 2013 einigten sich die Fraktionen im Europäischen Parlament auf ein Maßnahmenpaket, in das bereits etliche Änderungsvorschläge zu dem ursprünglichen Entwurf eingearbeitet waren. Kurz darauf nahm der Innenausschuss des EU-Parlaments diesen Entwurf mit großer Mehrheit an. Außerdem erteilte der Ausschuss das Mandat für die unmittelbare Aufnahme von Verhandlungen zwischen dem Parlament, dem Rat und der Kommission im sogenannten Trilog-Verfahren ohne erste Lesung im Parlament. Dies sollte der Beschleunigung des Verfahrens dienen, um eine Verabschiedung der Verordnung vor den Neuwahlen des Parlaments im Mai 2014 erreichen zu können. Ab Ende November 2013 wurden jedoch die Anzeichen dafür, dass die Grundverordnung nicht zu diesem Zeitpunkt verabschiedet werden kann, deutlicher. Das Trilog-Verfahren hat auch bis Ende Dezember 2013 noch nicht begonnen, so dass mit einer Einigung bis zu den Parlamentswahlen der EU 2014 nicht mehr zu rechnen ist.

Angesichts der Vielzahl der Neuerungen in den bis jetzt als Entwurf vorliegenden Bestimmungen beschränken wir uns an dieser Stelle auf eine kurze Beschreibung zweier Punkte, ohne dass es sich auch nur annähernd um eine Aufzählung der wichtigsten Punkte handeln könnte:

- Sehr zu begrüßen ist es, dass die Datenschutz-Grundverordnung sich – anders als die EU-Richtlinie von 1995 und in der Folge das BDSG - nicht auf die Datenverarbeitung der Unternehmen beschränkt, die ihren Sitz in Europa haben. Vielmehr weitet sie den räumlichen Anwendungsbereich auf die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch nicht in der Union niedergelassene für die Verarbeitung Verantwortliche aus, wenn die Datenverarbeitung dazu dient, diesen Personen in der Union Waren oder Dienstleistungen anzubieten oder ihr Verhalten zu beobachten. Mit dieser Bestimmung können sich weder Unternehmen dadurch aus ihrer datenschutzrechtlichen Verantwortung stehlen, dass sie sich auf einen Status als Drittlandunternehmen berufen, noch können ursprünglich europäische Unternehmen sich durch Verlegung ihres Sitzes aus Europa heraus dem hier geltenden Datenschutzrecht entziehen.
- Außerordentlich umstritten ist die europaweite Einführung von betrieblichen Datenschutzbeauftragten. Hierbei ist zu berücksichtigen, dass in Deutschland – und bisher nur hier – größere Unternehmen ab 10 bzw. 20 Personen, die ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind, verpflichtet sind, betriebliche Datenschutzbeauftragte zu bestellen. Diese Verpflichtung hat in der Vergangenheit dazu geführt, dass insbesondere größere Unternehmen durch entsprechenden Sachverstand im eigenen Unternehmen eher in der Lage sind, datenschutzrechtliche Problemstellungen überhaupt zu erkennen und sachgerecht zu

lösen. Die Datenschutz-Grundverordnung sah im ersten Entwurf von 2012 nun vor, dass zwar behördliche Datenschutzbeauftragte immer zu bestellen sind. Für Unternehmen sollte dies jedoch nur dann gelten, wenn darin mehr als 250 Beschäftigte arbeiten, unabhängig davon, ob diese überhaupt mit personenbezogenen Daten zu tun haben. Hierüber hat eine lebhafte Diskussion auf den unterschiedlichsten Ebenen stattgefunden. Die Länder der EU, in denen für die Unternehmen bisher überhaupt keine Verpflichtung zur Bestellung betrieblicher Datenschutzbeauftragter bestanden hat, fürchten eine massive Wettbewerbsverschlechterung. Für Deutschland wäre eine solche Regelung dagegen ein erheblicher Rückschritt im Hinblick auf den Datenschutz: Einerseits mag es sein, dass in einem Industrieunternehmen mit 250 Beschäftigten überhaupt kein Bedarf für die Bestellung eines betrieblichen Datenschutzbeauftragten besteht, weil nur sehr wenige Personen sich überhaupt mit personenbezogenen Daten beschäftigen. Andererseits kann bei Unternehmen, die viel mit sensiblen Daten arbeiten oder deren Kerngeschäft die Verarbeitung personenbezogener Daten ist, ein großer Bedarf bestehen, schon bei einer deutlich geringeren Anzahl Beschäftigter einen betrieblichen Datenschutzbeauftragten zu bestellen. Zeitweise gab es Anzeichen dafür, dass eine Kompromisslösung dahingehend gefunden werden sollte, den Ländern freizustellen, ob sie betriebliche Datenschutzbeauftragte verbindlich vorschreiben oder nicht. Das allerdings hätte dem erklärten Bestreben nach Harmonisierung des Datenschutzrechts innerhalb der EU entgegengestanden. Nach vielen Diskussionen über dieses Thema gab es im Oktober 2013 Änderungsvorschläge, die an die Verarbeitung von besonderen Kategorien von personenbezogenen Daten (sensible Daten) oder 5000 Betroffenendaten pro Jahr anknüpfen. Eine solche Regelung würde aus unserer Sicht wesentlich mehr Sinn machen als die Bindung an die Anzahl der Beschäftigten eines Unternehmens. Gleichwohl muss abgewartet werden, welche Auslegungen und Auswirkungen eine derartige Regelung erfährt und wie dann in der datenschutzrechtlichen (Aufsichts-) Praxis damit umzugehen ist.

Seit der Veröffentlichung des ersten Entwurfs der Datenschutz-Grundverordnung hat die Konferenz der Datenschutzbeauftragten der Länder insgesamt drei Entschließungen veröffentlicht, die sich auch mit den weiteren problematischen Themen auseinandersetzen. Diese können unter http://www.lda.brandenburg.de und http://www.datenschutz.bremen.de aufgerufen werden. Dabei wird bereits die Befürchtung einer Absenkung des Datenschutzniveaus der EU-Richtlinie von 1995 geäußert. In Deutschland besteht die Sorge, dass nicht nur seit vielen Jahren anerkannte datenschutzrechtliche Regelungen wegfallen oder verwässert werden, sondern insbesondere die mit der Novellierung von 2009 eingeführten Vorschriften zu Auskunfteien, Scoring, Werbung und Beschäftigtendatenschutz wegfallen.

Auch der eingangs erwähnte Entwurf einer EU-Richtlinie zur Verarbeitung personenbezogener Daten zum Zwecke der Strafverfolgung und Strafvollstreckung war 2012 Gegenstand intensiver Erörterungen der Datenschutzbeauftragten. Ein gemeinsam

erarbeitetes Thesenpapier zu den einzelnen Kapiteln des Richtlinienentwurfs fordert neben der Einbeziehung der EU-Organe einerseits ein hohes datenschutzrechtliches Mindestniveau für den Datenaustausch zwischen den Behörden der Mitgliedsstaaten und andererseits die Möglichkeit, im nationalen Recht der Länder über den Standard der Richtlinie hinauszugehen. Es muss verhindert werden, dass das hohe Datenschutzniveau der deutschen Strafprozessordnung und Datenschutzgesetze durch die Richtlinie verbindlich abgesenkt wird. Angesichts der 2014 bevorstehenden Wahlen zum Europaparlament erscheint es zum Ende des Berichtszeitraumes allerdings wenig wahrscheinlich, dass der vorgelegte Entwurf der EU-Richtlinie in überschaubarer Zeit noch verabschiedet wird.

2. Internationaler Datenverkehr

2.1 Auswirkungen von Prism

Angesichts der Enthüllungen über die Spähaktionen der amerikanischen National Security Agency (NSA) stellt sich in Deutschland die Frage, wie unter Berücksichtigung dieser neuen Erkenntnisse die Übermittlungen personenbezogener Daten in die USA rechtlich zu beurteilen sind.

Im Juni 2013 wurde erstmals bekannt, dass der US-Geheimdienst die Rechner von Internetfirmen anzapft, um sich in großem Stil Zugang zu Videos, Fotos, E-Mails und Kontaktdaten zu verschaffen. Auch die Daten von Telefonanbietern sollen millionenfach abgegriffen worden sein. Das geheime Programm Prism soll es bereits seit 2007 geben. Nach den Vorschriften des Bundesdatenschutzgesetzes (BDSG) dürfen personenbezogene Daten in sogenannte Drittländer (außerhalb der EU) nach den §§ 4b, 4c BDSG nur dann übermittelt werden, wenn entweder ein in § 4c BDSG genannter Ausnahmetatbestand (etwa informierte Einwilligung) vorliegt, dort ein angemessenes Datenschutzniveau herrscht oder die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist. Vor dem Hintergrund der Enthüllungen der Vorgehensweise der US-Geheimdienste hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder Pressemitteilungen veröffentlicht, die auf die Folgewirkungen für die datenschutzrechtliche Beurteilung der Datenübermittlung in die USA eingehen und unter http://www.datenschutz-bremen.de aufgerufen werden können.

Darüber hinaus ist auf den Bericht einer EU-US-Arbeitsgruppe hinzuweisen, die Ende November ihren Bericht über die rechtlichen Grundlagen der US-Spähaktionen vorgelegt hat, http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf. Konkrete Folgerungen werden in diesem Bericht nicht gezogen, lassen sich aber einer Presseerklärung und einem Memo vom gleichen Tage entnehmen, http://europa.eu/rapid/press-release_IP-13-

1166_de.htm und http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm. Darüber hinaus hat der Rat der Europäischen Union im Dezember 2013 den Entwurf eines „non-papers" vorgelegt, das Vorschläge enthält, wie die USA die Bedenken der EU und ihrer Mitgliedsstaaten im Hinblick auf die Überwachungsprogramme ausräumen können, http://media.de.indymedia.org/media/2013/12/350846.pdf. Insbesondere geht es dabei um einen stärkeren datenschutzrechtlichen Schutz der in der EU ansässigen Personen, die in dieser Hinsicht noch nicht einmal den US-Bürgern gleichgestellt sind. Darüber hinaus werden Transparenz, Rechtsmittel, Erforderlichkeit und auch Verhältnismäßigkeit angesprochen. Das Papier besteht aus unserer Sicht bisher jedoch lediglich aus Absichtserklärungen, in welche Richtung künftige Gespräche zwischen der EU, den Mitgliedstaaten und den USA führen könnten.

Um ein angemessenes Datenschutzniveau zu erreichen, gibt es in Bezug auf die Datenübermittlungen in die USA – ohne Berücksichtigung der neueren Entwicklung - verschiedene Wege:

2.1.1 Safe Harbor

Zwischen 1998 und 2000 hat die EU ein besonderes Verfahren entwickelt, wonach US-Unternehmen dem Safe Harbor beitreten und sich auf der entsprechenden Liste des US-Handelsministeriums eintragen lassen können, wenn sie sich verpflichten, die sogenannten Safe Harbor Principles zu beachten. Die dem Safe Harbor-Abkommen jeweils beigetretenen Unternehmen können auf einer Liste des US-Handelsministeriums ermittelt werden. Im Jahre 2000 hat die EU anerkannt, dass bei den Unternehmen, die dem Safe-Harbor-System beigetreten sind, ein ausreichender datenschutzrechtlicher Schutz besteht.

Angesichts der Tatsache, dass Hinweise darauf vorlagen, dass die in der Liste aufgeführten Unternehmen nicht immer eine entsprechende aktuelle Zertifizierung hatten oder ihren Verpflichtungen aus dem Abkommen nicht nachkamen, hat der Düsseldorfer Kreis bereits 2010 einen Beschluss gefasst, nach dem übermittelnden Unternehmen in gewissem Umfang Prüfpflichten auferlegt wurden. Dieser Beschluss kann unter www.ldi.nrw.de nachgelesen werden. Mittlerweile führen die neueren Entwicklungen dazu, dass Überlegungen angestellt werden, wie unter Berücksichtigung der Vorwürfe zu Prism die Safe Harbor-Zertifizierung eines Unternehmens überhaupt ausreichen kann, um ein angemessenes – wenigstens in Ansätzen dem deutschen bzw. europäischen Recht vergleichbares – Datenschutzniveau zu gewährleisten. Im Juli 2013 gab die zuständige EU-Kommissarin bekannt, dass das Abkommen vor dem Hintergrund der neueren Erkenntnisse daraufhin überprüft werden wird, ob es in der vereinbarten Form noch Bestand haben kann. Ein entsprechender Bericht sollte bis Ende 2013 vorliegen. Im November 2013 teilte die EU-Kommission mit, dass ein 13-Punkte-Katalog erstellt worden sei, der dafür sorgen solle, dass der Datenschutz im Rahmen von Safe Harbor verbessert wird. Dieser Katalog kann in einer Erklärung der EU-Kommission nachgele-

sen werden, http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm. Die Forderungen aus diesem Katalog müssten von den USA bis zum Sommer 2014 umgesetzt werden, andernfalls könne das Abkommen ausgesetzt werden. Zu den Forderungen gehört etwa eine Verbesserung des Rechtsschutzes für EU-Bürger, die gegen Unternehmen in den USA klagen wollen.

2.1.2 Standardvertragsklauseln

Die EU hat – ebenfalls zur Erleichterung der Übermittlung personenbezogener Daten in Nicht-EU-Länder – Standardvertragsklauseln entwickelt, die es den Unternehmen ermöglichen, bei Abschluss eines solchen Vertrages personenbezogene Daten in sogenannte Drittländer zu übermitteln. Die Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer von 2001, die Alternativen Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer von 2004 und der Beschluss über die Übermittlung personenbezogener Daten an Auftragsdatenverarbeiter in Drittländern von 2010 können auf den Seiten http://eur-lex.europa.eu aufgerufen werden und stellen bei Verwendung durch übermittelnde Unternehmen das erforderliche angemessene Datenschutzniveau her. Dabei wird jedoch grundsätzlich, ebenso wie bei der Entscheidung zu Safe Harbor, davon ausgegangen, dass die dem BDSG unterliegenden personenbezogenen Daten bei Anwendung dieser Verträge im Ausland einen dem europäischen Recht vergleichbaren Schutz erfahren. Mit den Enthüllungen über die Vorgehensweise der NSA in den USA ist dieser Schutz offensichtlich auch mit diesen Sicherungsmaßnahmen nicht mehr zu erreichen. Angesichts der Tatsache, dass weder die EU noch die Bundesregierung bisher konkrete Zusicherungen der US-Regierung zum Schutz der personenbezogenen Daten, die in die USA übermittelt werden, erreichen konnten, bleibt die Datenübermittlung in die USA auch auf der Grundlage von Standardvertragsklauseln mit einem deutlichen Risiko verbunden.

2.1.3 Unternehmensregelungen

Ein weiteres Instrument, ein angemessenes Datenschutzniveau zur Übermittlung personenbezogener Daten in Drittländer zu schaffen, sind verbindliche Unternehmensregelungen (BCR), für deren europaweite Einführung die EU verschiedene Arbeitspapiere veröffentlicht hat. Auch an der Wirksamkeit der BCR, den Schutz der personenbezogenen Daten in Drittländern herzustellen, entstehen zumindest gegenüber Datenübermittlungen in die USA Zweifel.

Zwar gelten im Falle europaweit abgestimmter Unternehmensregelungen diese als Gewähr für ein ausreichendes Datenschutzniveau, bei der Erteilung etwaiger Genehmigungen für konkrete Datenübermittlungen werden sich die Datenschutzaufsichtsbehörden bis zu einer befriedigenden Klärung jedoch zurückhalten (vgl. http://www.datenschutz-bremen.de/sixcms/detail.php?gsid=bremen236.c.9283.de).
Bedauerlicherweise hat die EU-Kommission sich trotz vielfältiger Befassung mit den

Auswirkungen der Spähaktionen seitens der USA noch nicht konkret zu den Folgewirkungen auf die Instrumente zur Herstellung eines angemessenen oder ausreichenden Datenschutzniveaus geäußert.

2.2 Cloud Computing weltweit

Die Verarbeitung personenbezogener Daten in globalen Clouds stößt auf erhebliche datenschutzrechtliche Probleme. Diese sind durch die Enthüllungen über großflächige staatliche Überwachungsmaßnahmen nicht geringer geworden.

Die Verarbeitung personenbezogener Daten in der „Cloud", d.h. in einer ausgelagerten, über Netzwerke angebundenen Infrastruktur hat eine Reihe von rechtlichen und technisch-organisatorischen Implikationen. Eine Orientierungshilfe der Datenschutzbeauftragten des Bundes und der Länder zeigt diese auf und bietet für die verschiedenen Realisierungsformen von Cloud-Diensten Hinweise für Entscheidungsträger sowie betriebliche und behördliche Datenschutzbeauftragte. Das Papier ist von unserem Internetangebot abrufbar (http://www.datenschutz-hamburg.de/news/detail/article/orientierungshilfe-cloud-computing.html).

Besonders komplex wird Cloud Computing aus Datenschutzsicht dann, wenn die Daten grenzüberschreitend übertragen werden. Solange sich dies im innereuropäischen Raum bewegt oder in Staaten erfolgt, in denen ein angemessenes Datenschutzniveau besteht, sind die damit verbundenen Hürden beherrschbar. In den anderen Fällen sind Lösungen wie Standardvertragsklauseln, Processor Binding Corporate Rules (PBCR) oder, im Falle der USA, das Safe-Harbor-Abkommen erforderlich, um eine Rechtsgrundlage für die Übermittlung zu schaffen (zu Details siehe VI 2.1). Diese Instrumente weisen seit den NSA-Enthüllungen ein erhebliches Legitimationsdefizit auf.

Die Datenschutzbeauftragten haben frühzeitig darauf hingewiesen, dass bei Cloud-Dienstleistern, die ihren Hauptsitz in den USA haben, die Auskunftsverpflichtungen gegenüber den dortigen Geheimdiensten u. U. auch dann einer Nutzung von deren Cloud im Weg stehen, wenn sie über Ressourcen (Server etc.) erbracht wird, die vollständig in der EU belegen sind. Denn auch dann würde sich das Unternehmen einem Auskunftsbegehren, das sich auf diese „europäischen Daten" bezieht, wohl nicht entziehen können.

Durch die vielfältigen Enthüllungen rund um die Ausspähungspraxis amerikanischer und britischer Geheimdienste im Jahre 2013 hat sich diese Sorge um die Sicherheit der personenbezogenen Daten nochmals erheblich verstärkt. Die entsprechenden Passagen in der Orientierungshilfe Cloud Computing geben daher nicht den vollständigen, aktuellen Stand der Diskussion unter den Datenschutzbehörden wieder.
Eine Überarbeitung ist daher in Arbeit.

2.3 Fluggastdatenübermittlung

Die Begehrlichkeit nach der Kenntnis der Daten von Flugpassagieren nimmt zu. Immer mehr Länder wollen über die Reisenden informiert sein.

Nach der vorläufigen Unterzeichnung des Abkommens zur Fluggastdatenübermittlung zwischen der EU und den USA im Dezember 2011 (vgl. 23. TB, IV. 2.2) ist das Abkommen im April 2012 endgültig vom EU-Parlament angenommen worden.

Seit März 2013 liegt nun auch der Entwurf zwischen der EU und Kanada zur Übermittlung und Verarbeitung von Passagierdaten vor.
Im Juni 2013 wurde bekannt, dass Russland von den Fluggesellschaften die vorherige Übermittlung etlicher personenbezogener Daten der europäischen Flugpassagiere verlangt. Hierüber hat es keine vorhergehenden Verhandlungen mit der EU gegeben.

Selbst die Mitgliedstaaten der EU sollen nach dem Vorschlag der Richtlinie über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität die Daten sämtlicher Fluggäste – auch bei Flügen innerhalb der EU – fünf Jahre speichern. Deutschland hat sich beim Rat der Justiz- und Innenminister 2012 enthalten, weil innerhalb der Bundesregierung noch gegen mehrere Regelungen des Richtlinien-Vorschlags aus Gründen der Verhältnismäßigkeit erhebliche Bedenken bestanden, vor allem bezüglich der Ausweitung des Entwurfs auf innereuropäische Flüge, der fünfjährigen Gesamtspeicherdauer und der Ausdehnung der Nutzung des unmaskierten Datensatzes auf zwei Jahre. Es ist noch nicht absehbar, wann und mit welchem Inhalt eine derartige Regelung, die weitere Einschränkungen der informationellen Selbstbestimmung bedeutet, verabschiedet wird. In jedem Fall gilt es, einer erneuten Variante der Vorratsdatenspeicherung in Europa entgegenzutreten.

3. Kreditwirtschaft

3.1 Kontaktloses Bezahlen mit Near Field Communikation (NFC)

Wegen der Möglichkeit des unberechtigten und unbemerkten Auslesens von Bankdaten haben die Aufsichtsbehörden Bedenken gegen Bankkarten mit NFC-Funktion.

In der Arbeitsgruppe Kreditwirtschaft, an der wir regelmäßig teilnehmen, wurden die mit der Ausgabe von Geldkarten („girogo-Karte"), die über eine kontaktlose Zahlungsfunktion verfügen, verbundenen datenschutzrechtlichen Probleme erörtert. Einige Sparkassen haben bereits damit begonnen, Geldkarten mit der so genannten NFC-

Technologie herauszugeben. Mittels Near Field Communication (NFC) sollen Beträge bis zu 20 Euro kontaktlos beglichen werden, wenn sich die Geldkarte im Lesebereich des Lesegeräts befindet. Neben Lesegeräten beim Händler ist auch das Auslesen im Smartphone möglich. Die letzten 10 Transaktionen mit der Geldkarte können an Aufladestationen und über das Smartphone, nicht aber beim Händler ausgelesen werden. Das Bezahlen setzt voraus, dass auf der Geldkarte ein Guthaben aufgeladen wurde.

In einem Beschluss des Düsseldorfer Kreises vom 18./19. September 2012 (veröffentlicht unter www.ldi.nrw.de und www.bfdi.bund.de) haben die obersten Aufsichtsbehörden auf die datenschutzrechtlichen Probleme beim Einsatz von NFC bei Geldkarten hingewiesen. Dazu gehört die Möglichkeit des unbemerkten unberechtigten Auslesens einer eindeutigen Kartennummer, von Geldbeträgen und Transaktionshistorien, da diese Daten nicht verschlüsselt werden. Die Geldkartenanbieter wurden aufgefordert, gem. § 9 BDSG im Rahmen der Verhältnismäßigkeit mit angemessenen technisch-organisatorischen Maßnahmen dafür zu sorgen, dass Dritten kein unberechtigtes Auslesen von Daten möglich wird. Außerdem solle das Kartenbetriebssystem schnellstmöglich so geändert werden, dass die Betroffenen die NFC-Funktionalität ein- und ausschalten können. Zudem seien die Betroffenen ausreichend über die Funktionsweise des Mediums, die Risiken und Schutzmöglichkeiten für ihre Daten zu unterrichten.

Zunehmend werden auch Kreditkarten mit NFC-Funktion von Hamburger Kreditinstituten ausgegeben. Dabei sind die Produkte hochgradig standardisiert, so dass die Karten ausgebenden Banken kaum Gestaltungsmöglichkeiten für das Produkt haben. Da bei Kreditkarten mit NFC die Kreditkartennummer kontaktlos ausgelesen werden kann, sind nach Auffassung der Aufsichtsbehörden noch höhere Anforderungen an die Datensicherheit zu stellen. Bei der Kreditkartennummer handelt es sich um eine in § 42 a Bundesdatenschutzgesetz (BDSG) genannten Angabe. Dadurch hat der Gesetzgeber zum Ausdruck gebracht, dass die Kreditkartennummer ein besonders schützenwertes Datum ist. Ein hohes Gefährdungspotential ergibt sich darüber hinaus durch die vielfältigen Nutzungsmöglichkeiten der Kreditkartennummer für Bezahlvorgänge z.B. im Internet und durch den Wegfall einer Beschränkung des möglichen Zahlbetrags, der im Fall der Geldkarte mit NFC-Funktion mit 20 Euro relativ gering ist.

Im Gegensatz zu den nur im Kontaktmodus auslesbaren Magnetstreifen- und Chip-Karten sind bei Einsatz der NFC-Technologie die Kreditkartennummer, das Verfallsdatum und weitere durch die Finanzinstitute festgelegte Informationen kontaktlos auslesbar. Daher besteht aus Sicht der Datenschutzaufsichtsbehörden die Gefahr, dass die Daten unbemerkt durch Dritte, die über entsprechende technische Möglichkeiten verfügen, ausgelesen werden können, z.B. um Kundenprofile anzufertigen. Da die Abrufe der Daten durch die Karten selbst nicht protokolliert werden, besteht für die Betroffenen keine Möglichkeit, die Abrufe zu kontrollieren. Aus Sicht der Datenschutzaufsichtsbehörden ist nicht nur die Möglichkeit des Missbrauchs der so gewonnenen Daten in betrügerischer Absicht problematisch, sondern auch die unbefugte Erhebung und

Nutzung persönlicher Daten durch Dritte zu anderen nicht zulässigen Zwecken.
Da die datenschutzrechtlichen Probleme durch den Einsatz einer speziellen Technik entstehen, wurde die Angelegenheit zunächst im Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder in technisch-organisatorischer Hinsicht geprüft. Insbesondere wurden dort die von den Kartenherausgebern zur Verfügung gestellten Privacy Impact Assessments (PIA) und die datenschutzrechtlichen Folgen der Einführung der NFC-Technik analysiert. Auf Grundlage der im Arbeitskreis Technik erfolgten Einschätzung hat die AG Kreditwirtschaft in Ihrer Sitzung am 11./12. November 2013 mehrheitlich eine abschließende datenschutzrechtliche Bewertung vorgenommen. Um eine datenschutzgerechte Nutzung zu ermöglichen, sind daher technische und organisatorische Sicherheitsmaßnahmen zu treffen, zu denen insbesondere auch die folgenden Punkte gehören:

- Auf Verlangen eines Kunden sollte eine Schutzhülle in der Standardversion für Karten mit NFC-Funktion zur Verfügung gestellt werden, die als Faraday'scher Käfig ein Auslesen der Daten verhindert. Die Aufsichtsbehörden würden es begrüßen, wenn die Hülle kostenfrei zur Verfügung gestellt wird.
- Die Kunden sollten vor der Einführung umfassend über die Nutzungsmöglichkeiten, die Risiken der NFC-Technik und wichtige Schutzmaßnahmen sowie auch den Einsatz der Schutzhülle unterrichtet werden.
- Die Möglichkeit der jederzeitigen Abschaltung der NFC-Funktion auf Wunsch des Karteninhabers sollte schnellstmöglich umgesetzt werden.
- Die Karten ausgebenden Institute werden darauf hingewiesen, dass Drittanwendungen, die geeignet sind, das Pseudonymisierungskonzept der Karte zu unterlaufen, eine neue datenschutzrechtliche Bewertung erforderlich machen.
- Maßnahmen der Kreditwirtschaft, die zu einer weiteren Sicherung des NFC-Konzeptes führen (wie z.B. verhältnismäßige Verschlüsselung der Luftschnittstelle und Randomisierung der Kartennummer) sollten fortgesetzt verfolgt werden.

4. Versicherungswirtschaft

4.1 Bonitätsabfrage bei Krankenversicherungen

Versicherungsunternehmen verzichtet nach unserer Aufforderung auf Schufa-Auskunft bei Krankenversicherung im Basistarif.

In der Arbeitsgruppe Versicherungswirtschaft des Düsseldorfer Kreises, in der wir vertreten sind, ist das Thema Bonitätsabfragen in der Versicherungswirtschaft mit dem Gesamtverband der Versicherungswirtschaft (GDV) mehrfach kontrovers für die verschiedenen Versicherungssparten erörtert worden. Bonitätsauskünfte dürfen gem. § 29 Abs. 2 Nr. 1 Bundesdatenschutzgesetz (BDSG) nur weitergegeben werden, wenn

das Versicherungsunternehmen im konkreten Fall ein berechtigtes Interesse an den Informationen darlegt und gleichzeitig die betroffene Person kein schutzwürdiges Interesse am Unterlassen der Abfrage hat. Nach Auffassung der Aufsichtsbehörden ist für die Zulässigkeit der Abfrage entscheidend, ob für das Versicherungsunternehmen ein kreditorisches Risiko besteht, dem durch die Abfrage begegnet werden soll. Eine Bonitätsabfrage bei der Beantragung einer Krankenvollversicherung im Basistarif wird von den Aufsichtsbehörden nicht akzeptiert, da gem. § 12 Abs. 1b Gesetz über die Beaufsichtigung der Versicherungsunternehmen (VAG) ein Kontrahierungszwang für die Versicherer besteht, so dass ein kreditorisches Risiko für die Vertragsbegründung unerheblich ist.

Durch eine Beschwerde wurden wir darauf aufmerksam, dass ein Hamburger Versicherungsunternehmen vor Abschluss einer Krankenvollversicherung immer eine Bonitätsauskunft bei der Schufa einholte. Zur Begründung wurde mitgeteilt, dass der Gesetzgeber die Unternehmen der Privaten Krankenversicherung verpflichtet habe, Versicherungsschutz (in verringertem Umfang gem. § 193 Abs.6 S.6 Versicherungsvertragsgesetz) auch dann zu gewähren, wenn der Versicherungsnehmer keinerlei Beiträge erbringe. Die insoweit zu gewährenden Leistungen seien dann zu Lasten der Versichertengemeinschaft aufzubringen. Dieses Risiko solle durch die Bonitätsabfragen minimiert werden. Die Antragsformulare enthielten deshalb eine Einwilligungserklärung zur Bonitätsauskunft. Bei der folgenden Antragsbearbeitung durch den Fachbereich würde dann jedoch zwischen einer individuellen privaten Krankenversicherung und der Aufnahme in den Basistarif differenziert. Werde nur der Basistarif beantragt, bleibe das Ergebnis der Schufa-Auskunft ohne Folgen, weil die Versicherung dem Kontrahierungszwang gem. § 12 Abs. 1b VAG unterliege. Da eine Einwilligung der Antragsteller gem. §§ 4, 4a BDSG eingeholt würde, sei die Beantragung der Schufa-Auskunft zulässig.

Das Versicherungsunternehmen wurde von uns darauf hingewiesen, dass angesichts der dargestellten Sachlage erhebliche Zweifel daran bestünden, dass die Einwilligung nach § 4a BDSG wirksam sei. Denn die Betroffenen würden in den Fällen, in denen nur der Abschluss des Basistarifs gewünscht werde, nicht darüber unterrichtet, dass eine Bonitätsauskunft gar nicht erforderlich sei. Sie würden nicht ausreichend über den Zweck der Erhebung sowie über die Folgen der Verweigerung informiert. Ein berechtigtes Interesse des Unternehmens an der Schufa-Auskunft bestünde nicht.

Erfreulicherweise schloss sich das Unternehmen unserer datenschutzrechtlichen Bewertung an. Schufa-Abfragen bei der Beantragung des Basistarifs werden nicht mehr eingeholt. Die Antragsformulare für Krankenvollversicherungen wurden geändert und die Antragsteller werden nun im Text der von Ihnen zu unterschreibenden Einwilligungserklärung darauf hingewiesen, dass eine Bonitätsauskunft nicht bei Beantragung des Basistarifs eingeholt wird.

4.2 Schadenklassedatei

Eine als Auskunftei in Hamburg betriebene Schadenklassedatei soll künftig die ehemalige Malus-Datei für Kfz-Haftpflicht-Versicherer ersetzen.

Im Berichtszeitraum haben wir uns mit dem Vorhaben der GDV Dienstleistungs-GmbH & Co. KG beschäftigt, die vom Hamburgischen Datenschutzbeauftragten im Jahr 1983 erstmals überprüfte Malus-Datei (vgl. 2. TB, 4.3.1.4) durch eine automatisierte Schadenklassedatei zu ersetzen, die als Auskunftei betrieben werden soll. Hintergrund dieser Datei ist das Schadenfreiheits-System in der Kraftfahrtversicherung, das aufgeteilt ist in Schadenfreiheitsklassen (SF ½ - SF 30) und Schadenklassen (S, M, O). Der Beitragssatz bei der Kfz-Haftpflicht-Versicherung richtet sich nach der Dauer von schadenfreien Jahren. Autofahrer, die erstmalig einen Versicherungsvertrag abschließen, haben wenn sie keine Fahranfänger sind, einen Beitragssatz von ca. 100-140 % zu zahlen, der sich nachfolgend abhängig von den schadenfreien Jahren verringert. Kommt es zu einem durch den Fahrer verursachten Schaden, so wird dieser durch seine Versicherung in eine höhere Beitragsklasse eingestuft. In der Regel wird er in eine höhere Schadensfreiheitsklasse gestuft werden, also immer noch unter dem Eingangsbeitragssatz von 100 -140 % liegen. Abhängig von der Anzahl der Schäden in einem bestimmten Zeitraum oder der vorherigen Einstufung, kann es jedoch auch zu einer Einstufung in eine Schadenklasse (S, M, O) mit Beitragssätzen kommen, die über der Eingangsstufe liegen und bis zu jährlich 280 % betragen können.

Bei einem Wechsel des Versicherungsunternehmens wird die Schadenfreiheitsklasse bzw. werden die schadenfreien Jahre übertragen. Wer eine neue Versicherung abschließen will, legt zum Nachweis der Schadenfreiheitsklasse daher in der Regel eine „Versichererwechselbescheinigung" vor, um seine Schadenfreiheitsklasse zu behalten. Jedoch kommt es immer wieder vor, dass Versicherungsnehmer, die nach einem Schaden in eine Schadenklasse mit einer deutlich höheren Versicherungsprämie eingestuft wurden, ihren Versicherer wechseln und behaupten, bisher keine Kfz-Versicherung gehabt zu haben, um in die für sie günstigere Eingangsstufe von 100 -140 % eingestuft zu werden. Um ein solches Vorgehen zu erschweren, wurde bereits in den 80er Jahren die papiergestützte Malus-Datei eingeführt, die künftig als elektronische Warndatei gem. § 29 BDSG mit Sitz in Hamburg betrieben werden soll. In diese Datei sollen wie bisher alle Verträge, die vom Versicherungsnehmer oder vom Versicherer gekündigt wurden und aufgrund des Schadensverlaufs ohne Kündigung in eine Schadenklasse gehören würden, eingemeldet werden. Behauptet ein Antragsteller, bisher keine Kfz-Versicherung gehabt zu haben, kann der Versicherer die Richtigkeit dieser Angabe durch Anfrage bei der Schadenklassedatei überprüfen.

Derzeit werden die Anzahl und der Inhalt der importierten Meldungen und Anfragen protokolliert und ein Jahr gespeichert. Bei Anfragen gleicht das Programm ab, ob dazu

ein passender Datensatz gespeichert ist. Im Falle eines Treffers wird ein Brief mit Name, Adresse und Kfz-Kennzeichen des Betroffenen an das anfragende Unternehmen versendet. Dieses papiergestützte Verfahren soll künftig auf ein automatisiertes vollprotokolliertes Abrufverfahren umgestellt werden, für das eine Stichprobenkontrolle in dem von den Aufsichtsbehörden grundsätzlich bei Auskunfteien geforderten Umfang durchgeführt werden soll.

Nach Angaben der Versicherungswirtschaft ist eine Prüfungsmöglichkeit unverzichtbar, weil in der Kfz-Haftpflichtversicherung ein gesetzlicher Annahmezwang gilt. Die derzeitige Malus-Datei enthielt für das 1. Halbjahr 2012 47.779 Eintragungen. Es wurden 437.115 Anfragen der Versicherer vermerkt, die zu insgesamt 11.506 Treffern führten. Auf das Jahr hochgerechnet konnte durch die Datei nach Angaben der Versicherungswirtschaft jährlich ein Verlust von 4 Mio. Euro verhindert werden.

Die Versicherungswirtschaft sieht keinen Grund zur Annahme eines der Meldung in die Schadenklassedatei entgegenstehenden überwiegenden schutzwürdigen Interesses der Betroffenen. Die Datei werde ausschließlich für Anfragen von Kfz-Versicherungsunternehmen vorgehalten und nur in den Fällen abgefragt, in denen ein Antragsteller angegeben habe, dass er keine Vorversicherung hat. Die Speicherung sorge dann für eine risikogerechte Einstufung des neuen Vertrags. Das System solle gegenüber den Betroffenen transparent betrieben werden. Die Betroffenen sollen sowohl bei Vertragsschluss als auch bei Einmeldung in die Warndatei informiert werden.

Das dargestellte Vorhaben wird von den Aufsichtsbehörden abschließend in der nächsten Sitzung der Arbeitsgruppe Versicherungswirtschaft erörtert und datenschutzrechtlich bewertet werden. Über den Fortgang werden wir berichten.

4.3 Einwilligungs- und Schweigepflichtentbindungserklärung

Versicherungsunternehmen nutzen neue Einwilligungs- und Schweigepflichtentbindungserklärung für die Erhebung, Verarbeitung und Nutzung von Gesundheitsdaten und sonstiger nach § 203 StGB geschützter Daten.

Nach Abstimmung des Mustertextes für eine Einwilligungs- und Schweigepflichtentbindungserklärung (vgl. 23. TB, 5.1) und dessen Billigung im Düsseldorfer Kreis wird die Erklärung bei Neuabschluss von Verträgen von den Versicherungsunternehmen genutzt. Die Formulare sind entsprechend geändert worden. Die Erklärung gilt für die Verarbeitung von Gesundheitsdaten durch Versicherungsunternehmen. Sie berücksichtigt die sich aus dem BDSG ergebenden Anforderungen sowie die Anforderungen aus § 213 Versicherungsvertragsgesetzes (VVG) an die Erhebung und weitere Verarbeitung von Gesundheitsdaten der Antragsteller bzw. Versicherungsnehmer.

Kontrovers erörtert wurde im Kreis der Aufsichtsbehörden jedoch die Frage der Umsetzung der Erklärung gegenüber Bestandskunden (so genannte Altfälle). Dabei ging es um die Frage, ob auch Bestandskunden generell die neue Einwilligung unterschreiben müssen oder ob eine Information der Kunden über die geänderte Erklärung ausreichend ist. Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) hatte angeboten, die Bestandskunden mit nächster Vertragspost über die neue Erklärung zu unterrichten und im Bedarfsfall, z.B. wenn eine Datenerhebung bei einem Arzt aufgrund einer Leistungsfallbearbeitung notwendig wird, eine unterschriebene Einwilligungserklärung einzuholen. Die Aufsichtsbehörden vertreten mehrheitlich die Auffassung, dass ohne einen konkreten Anlass wie eine Leistungsfallprüfung von Bestandskunden nicht verlangt werden muss, die neue Einwilligungserklärung zu unterzeichnen. Sie erwarten allerdings, dass die Bestandskunden verständlich über die wesentlichen Inhalte der geänderten Einwilligungs- und Schweigepflichtentbindungserklärung informiert werden und Ihnen die Erklärung entweder per Post oder im Internet abrufbar zur Kenntnis gegeben wird.

4.4 Verhaltensregeln

Die Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft sind mit dem geltenden Datenschutzrecht vereinbar.

Nach Überarbeitung des Entwurfs der Verhaltensregeln für den Umgang mit personenbezogenen Daten in der Versicherungswirtschaft (vgl. 23 TB, 5.2) hat der Düsseldorfer Kreis in seiner Sitzung im November 2011 die Verhaltensregeln in der bis dahin vorliegenden Form grundsätzlich gebilligt. In der Fassung vom 27. März 2012 wurden sie im schriftlichen Umlaufverfahren von den Aufsichtsbehörden mit einer Anmerkung zu einer Regelung gebilligt, die vom Gesamtverband der Deutschen Versicherungswirtschaft (GDV) nach den Vorgaben der Aufsichtsbehörden umgesetzt wurde. Auf Antrag des GDV hat der für die Verhaltensregeln zuständige Berliner Beauftragte für Datenschutz und Informationsfreiheit gem. § 38 a BDSG die Verhaltensregeln überprüft und im November 2012 festgestellt, dass sie mit dem geltenden Datenschutzrecht vereinbar sind.

Die Verhaltensregeln sind auf der Internetseite des GDV abrufbar. Der Beitritt zu den Verhaltensregeln ist für Versicherungsunternehmen freiwillig. Durch einen Beitritt verpflichten sie sich zur Einhaltung der geregelten Datenschutzstandards, insbesondere zur Vorlage eines umfassendes Datenschutz- und Datensicherheitskonzepts, zur Einhaltung bestimmter Abläufe und zu mehr Transparenz über Datenverarbeitungsvorgänge für die Versicherungsnehmer. Nach Angaben des GDV ist bereits eine Vielzahl von Versicherungsunternehmen den Verhaltensregeln beigetreten.

5. Handel

5.1 Unzulässige Datenverarbeitung durch Versandhändler

Wegen des unzulässigen Abgleichs bei von der Rechnungsadresse abweichenden Lieferadressen wurde gegen ein Versandhandelsunternehmen ein Bußgeld verhängt.

Nachdem wir Beschwerden von Betroffenen erhielten, die sich gegen die Weitergabe von ihren personenbezogenen Daten richteten, haben wir den Verfahrensablauf eines Hamburger Versandhändlers bei Bestelllungen mit abweichender Rechnungs- und Lieferadresse überprüft. In einem Fall hatte eine langjährige Kundin des Versandhauses eine Bestelllung auf Rechnung getätigt, die an ihren Bruder unter einer anderen Anschrift versandt werden sollte. Ihr wurde mitgeteilt, dass aufgrund interner Bestimmungen eine Lieferung an diesen Mitbesteller auf offene Rechnung nicht möglich sei und dass sie Artikel, die in der Zwischenzeit bei ihr einträfen, nur gegen Barzahlung an ihn herausgeben solle. Hintergrund dieses Schreibens war die durch das Versandhaus üblicherweise bei abweichenden Rechnungs- und Lieferadressen vorgenommene Überprüfung der Lieferadresse gegen die konzerneigene interne Warndatei, die einen Missbrauch von Kundenkonten verhindern soll. Da ein den Bruder der Bestellerin betreffender Eintrag in der konzerneigenen Warndatei vorhanden war, wurde das Standardschreiben an sie versandt.

Der Eintrag in der Warndatei beruhte auf einer Kontoeinschränkung durch ein anderes Konzernunternehmen, die sich wegen Zeitablaufs erledigt hatte und eigentlich hätte gelöscht werden müssen. Durch den Abgleich der Lieferadresse mit der konzerneigenen Warndatei durch den Versandhändler wurden unbefugt personenbezogene Daten über den Bruder der Bestellerin an diese weitergegeben. Die Voraussetzungen für eine zulässig Übermittlung von Daten für die Begründung oder Durchführung eines Schuldverhältnisses nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG lagen nicht vor. Das Vertragsverhältnis mit der Kundin hätte abgewickelt werden können, ohne dass ein Abgleich der abweichenden Lieferadresse mit der Warndatei erfolgen musste. Die Kundin war Schuldnerin der Forderung, mit ihr bestand eine langjährige Vertragsbeziehung. Es war nicht Gegenstand des Vertragsverhältnisses und nicht Sache des Versandhauses, seine Kunden rein vorsorglich ohne besondere Anhaltspunkte vor einer theoretisch möglichen Leistungserschleichung durch Dritte zu schützen.

Auch die Voraussetzungen des § 28 Abs. 1 Satz 1 Nr. 2 BDSG lagen in diesem Fall nicht vor. Es ist bereits zweifelhaft, ob das Versandhaus ein berechtigtes Interesse an dem Abgleich hatte. Zwar können auch wirtschaftliche Interessen berechtigte Interessen sein, so grundsätzlich auch die Verhinderung von Forderungsausfällen und Betrug. Allerdings konnte das Unternehmen nicht überzeugend darlegen, dass bei Lieferungen an eine Drittadresse immer ein berechtigtes Interesse an einem Datenabgleich zur

Betrugsprävention und zur Vermeidung von Forderungsausfällen besteht. Berechtigte Interessen an einem Datenabgleich bestehen in der Vielzahl von Fällen, in denen Besteller Waren verschenken und an Dritte liefern lassen wollen, nicht, so dass in der Regel nicht von betrügerischen Absichten ausgegangen werden kann. Durch einen standardmäßigen Datenabgleich kommt es in derartigen Fällen zu einem unzulässigen Ausforschen personenbezogener Daten. Da es Alternativen zu einem Datenabgleich gibt, ist ein solches Ausforschen nicht erforderlich und unverhältnismäßig unter Berücksichtigung der Interessen der Kunden.

Nach unserer Auffassung kann ein berechtigtes Interesse des Versandhauses an einem Datenabgleich bei Bestellungen mit Drittversand nur dann vorliegen, wenn es Anhaltspunkte für einen Betrugsversuch gibt. Diese lagen im Beschwerdefall nicht vor, da die Bestellerin ihre Rechnungen immer bezahlt hatte. Zudem wäre ein Abgleich der Lieferadresse mit der konzerneigenen Warndatei schon deshalb nicht erforderlich gewesen, da andere datensparsamere Möglichkeiten zur Betrugsverhinderung denkbar sind. Auch wenn der Rechnungskauf für den deutschen Internethandel die größte Bedeutung haben sollte, scheint eine Bezahlung per Kreditkarte bei Bestellungen mit abweichender Lieferanschrift, wie sie von anderen großen Versandhändlern angeboten wird, mittlerweile im Versandhandel auf breite Akzeptanz zu stoßen. Als weitere datensparsamere Möglichkeit kommt die Zusendung einer Bestätigungs-E-Mail bei Internetteinkauf bzw. einer schriftlichen Bestätigung bei telefonischen Bestellungen an die hinterlegte E-Mail-Adresse bzw. Anschrift der Besteller in Frage. So würde den Kunden die Möglichkeit gegeben, eventuelle Missbrauchsfälle zu melden.

Im Übrigen stehen der Erhebung und der Weitergabe von personenbezogenen Daten mittels des Datenabgleichs mit der Warndatei in der Regel die überwiegenden schutzwürdigen Interessen der zu beliefernden Dritten entgegen. Wie oben dargestellt, ist nicht ersichtlich, dass es bei Bestellungen mit abweichender Lieferanschrift in der Regel um Betrugsfälle gehen könnte. Nur in diesen Fällen wäre jedoch das Interesse der Betroffenen an einer Datenerhebung nicht schutzwürdig. Bei der weit überwiegenden Anzahl der Fälle hingegen, in denen keine Betrugsabsicht vorliegt, überwiegen nach Auffassung der Aufsichtsbehörde die schutzwürdigen Interessen der rechtschaffenen Besteller und Dritten an dem Ausschluss der Erhebung und Verarbeitung ihrer Daten. Dabei ist zu berücksichtigen, dass negative Daten auch an die Besteller (zumindest mittelbar) weitergegeben werden, was gerade im Verwandten- und Freundeskreis zu äußerst unangenehmen Situationen und zu einer Stigmatisierung der Betroffenen führen kann. Im Beschwerdefall kam noch hinzu, dass es sich um nicht mehr aktuelle Daten des Dritten handelte, die erhoben und weitergegeben wurden.

Der weitere Fall betraf die unzulässige Weitergabe von personenbezogenen Daten eines Vaters an seinen Sohn. Der Vater hatte über das Kundenkonto seines Sohnes bestellt und seine Adresse als Lieferadresse angegeben. Auch in diesem Fall wichen Rechnungs- und Lieferadresse voneinander ab und der Sohn erhielt das Standard-

schreiben, in dem ihm mitgeteilt wurde, dass auf Grund interner Bestimmungen eine Lieferung an seinen Vater als Mitbesteller auf offene Rechnung nicht möglich sei und dass in der Zwischenzeit eingetroffene Artikel nur gegen Barzahlung herausgegeben werden sollen. Er erhielt dadurch negative Daten über seinen Vater. Die Überprüfung der Angelegenheit ergab, dass in der Warndatei keine negativen Daten zum Vater, sondern zu dessen Frau gespeichert waren, die dazu führten, dass die Adresse nicht beliefert wurde. Hintergrund war ein offener Saldo in Höhe von 150 Euro aus einer Bestellung vom Mai 2005. Aufgrund der Beschwerde wurde von dem Versandhaus festgestellt, dass die Adresse der Frau infolge einer Namensverwechslung durch ein Inkasso-Unternehmen ermittelt und dann ohne weitere Prüfung durch das Versandhaus in die Warndatei aufgenommen wurde, es sich mithin um einen falschen Eintrag handelte.

Auch in diesem Fall wurden durch Abgleich der Lieferadresse mit der konzernmeigenen Warndatei unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhoben, gespeichert und an einen Dritten weitergegeben. Erschwerend kam hinzu, dass in der Warndatei falsche Daten vorlagen, die zu einem Warnhinweis hinsichtlich der zu beliefernden Adresse führte. Offensichtlich gab es keine Versuche des Versandhauses, die Forderung geltend zu machen bzw. den Datenbestand in gewissen Zeiträumen zu überprüfen und zu bereinigen. Die durch das Unternehmen getroffenen organisatorischen Regelungen bei dem Betrieb der Warndatei waren nicht ausreichend, um die gesetzlichen Anforderungen zu erfüllen, nach denen zu gewährleisten ist, dass die Daten in der Warndatei aktuell und richtig sind. Die beiden Fälle zeigen, dass negative Eintragungen nicht regelmäßig auf Aktualität überprüft wurden bzw. dass Meldungen übernommen wurden, deren Richtigkeit nicht ausreichend überprüft wurde. Dies hätte bei der nach den datenschutzrechtlichen Vorschriften gebotenen Sorgfalt verhindert werden können.
Darüber hinaus ist äußerst zweifelhaft, ob das Inkasso-Unternehmen die personenbezogenen Daten in zulässiger Weise gem. § 28 a BDSG n. F., § 28 Abs. 1 BDSG a.F. an die Warndatei übermittelt hatte.

Die Verarbeitung der personenbezogenen Fälle durch das Versandhaus wurde in beiden Fällen als Ordnungswidrigkeit nach § 43 Abs. 2 Nr. 1 BDSG in Verbindung mit § 30 Abs. 1 des Gesetzes über Ordnungswidrigkeiten (OWiG) gewertet und ein Bußgeld verhängt.
Das Unternehmen hat den von uns beanstandeten Abgleich bei von der Rechnungsadresse abweichender Lieferadresse mit der konzerninternen Warndatei mittlerweile eingestellt.

5.2 Kundenkarte für Kinder und Jugendliche

Einzelhandelsunternehmen setzt Vermarktung von Kundenkarte für Kinder und Jugendliche wegen datenschutzrechtlicher Mängel aus.

Durch eine Eingabe erhielten wir Hinweise auf die für Kinder und Jugendliche unverständlichen Geschäftsbedingungen des online-Antragsformulars der Kundenkarte eines Hamburger Drogeriemarktes. Der Petent beschwerte sich insbesondere über die Möglichkeiten der Datennutzung für Werbezwecke nach den Allgemeinen Geschäftsbedingungen (AGB). Über die Kundenkarte und die AGB hatten wir bereits in unserem 22. Tätigkeitsbericht aus dem Jahr 2008/2009 (7.1) berichtet. Das Unternehmen hatte seinerzeit große Bereitschaft gezeigt, sich datenschutzgerecht zu verhalten und hatte das Antragsformular für die Kundenkarte für Kinder und Jugendliche umfassend umgestaltet und mit uns abgestimmt. Datenschutzrechtliche Bedenken gegen die Datenverarbeitung im Zusammenhang mit der Kundenkarte hatten wir daher nicht mehr.

Die Überprüfung des Antragsformulars für die Karte auf der Webseite des Unternehmens ergab jedoch nun, dass das Formular und die erhobenen Angaben nicht mit dem Papier-Antragsformular und den AGB zur Kundenkarte für Kinder und Jugendliche übereinstimmte, die im Jahr 2009 zwischen dem Unternehmen und uns abgestimmt worden waren. Wir hatten seinerzeit besonderen Wert darauf gelegt, dass das Unternehmen die Jugendlichen klar und verständlich darüber unterrichtet, welche Angaben erforderlich sind und welche freiwillig erteilt werden können und zu welchen Zwecken diese Angaben genutzt werden. Entgegen der Absprache waren die Erläuterungen sowie die AGB zu dem Online-Antrag, die von den Jugendlichen akzeptiert werden mussten, nicht auf den Empfängerhorizont ausgerichtet und daher für Kinder und Jugendliche völlig unverständlich. Zudem wurden im Online-Antrag mehr Daten als für die Ausstellung der Kundenkarte erforderlich abgefragt. Nicht zulässig war es auch, dass die Kinder und Jugendliche ihr Einverständnis in die Zusendung von Werbung durch Briefpost und per E-Mail erteilen sollten. In diesem Zusammenhang haben wir auf die Entscheidung des OLG Hamm vom 20.09.2012, Az. I-4 U 85/12 hingewiesen, wonach nicht davon ausgegangen werden kann, dass selbst Minderjährige ab dem 15. Lebensjahr grundsätzlich die nötige Reife haben, um die Tragweite der Einwilligungserklärung zur Datenspeicherung und Datenverwendung zu Werbezwecken abzusehen.

Unserer Aufforderung, den Online-Antrag für die Kundenkarte den datenschutzrechtlichen Anforderungen entsprechend umzugestalten oder den Antrag von der Webseite zu entfernen, kam das Unternehmen umgehend nach und blendete den Online-Antrag auf der Unternehmenswebseite aus. Bis auf Weiteres wurde die Neuvermarktung der Kundenkarte sowohl im Online- als auch im Offline-Bereich durch das Unternehmen eingestellt.

Das Konzept für eine Kundenkarte für Kinder und Jugendliche ist mittlerweile grundlegend überarbeitet worden. Wir haben die Umsetzungen der datenschutzrechtlichen Vorgaben kritisch begleitet und sehen derzeit keine Einwände gegen die im Zusammenhang mit der Kundenkarte erfolgende Datenverarbeitung durch das Unternehmen.

6. Auskunfteien

6.1 Stichprobenverfahren

Die Überprüfung verschiedener Auskunfteien auf die Verfahrensweise bei Stichprobenüberprüfungen zum berechtigten Interesse der anfragenden Stellen hat ergeben, dass oft zu oberflächlich kontrolliert wurde. Auch in Hamburg musste eine Auskunftei Änderungen bei der Stichprobenüberprüfung vornehmen.

Nach den Vorschriften des Bundesdatenschutzgesetzes (BDSG) dürfen Auskunfteien Informationen über Personen nur dann an Dritte übermitteln, wenn diese ein berechtigtes Interesse an der Auskunft glaubhaft dargelegt haben und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. In den allermeisten Fällen erfolgen die Übermittlungen in einem automatisierten Abrufverfahren. Den Auskunfteien ist es daher nicht möglich – und es wird gesetzlich auch nicht von ihnen verlangt –, in jedem einzelnen Fall nachzuprüfen, ob das berechtigte Interesse der abfragenden Stelle auch tatsächlich besteht. Vielmehr ist die Stelle, der die Daten übermittelt werden, verpflichtet, die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise der glaubhaften Darlegung gegenüber der Auskunftei aufzuzeichnen. Darauf darf sich die jeweilige Auskunftei jedoch nicht vollständig verlassen, sondern muss im Rahmen eines Stichprobenverfahrens auch das Vorliegen eines berechtigten Interesses einzelfallbezogen feststellen und überprüfen.

Im Rahmen der Erörterung dieser Frage mit verschiedenen Auskunfteien bei einer Sitzung der AG Auskunfteien des Düsseldorfer Kreises stellte sich heraus, dass die Art und Weise der Durchführung des Stichprobenverfahrens von den Auskunfteien nicht nur außerordentlich unterschiedlich gehandhabt wird, sondern in vielen Fällen keineswegs der vorgesehenen einzelfallbezogenen Feststellung und Überprüfung entspricht. Einige Auskunfteien beschränkten sich nämlich darauf, den betrieblichen Datenschutzbeauftragten des anfragenden Unternehmens zu beauftragen, die Stichprobenkontrollen durchzuführen und anschließend das Vorliegen des berechtigten Interesses gegenüber der Auskunftei zu versichern. Eine solche Verfahrensweise entspricht in keiner Weise den gesetzlichen Vorgaben. Vielmehr müssten die Unterlagen, die dem betrieblichen Datenschutzbeauftragten zur Verfügung stehen, der Auskunftei vorgelegt werden. Sofern keine Dokumente vorhanden sind, was etwa bei Onlinebe-

stellungen möglich ist, muss sich das berechtigte Interesse aus dem Kontext ergeben. Selbst bei Internetbestellungen müssten die Unterlagen angesichts des Nachweises von Bestellvorgängen nachvollziehbar generiert werden können.

Die hier aufgeworfene Problematik hat dazu geführt, bei einer Auskunftei in Hamburg zu überprüfen, in welcher Weise dort mit dem Stichprobenverfahren umgegangen wird. Das Unternehmen übersandte uns daraufhin einen Fragebogen, der im Falle von Stichprobenüberprüfungen an die Unternehmen versendet wird. Daraus ergibt sich sehr deutlich, dass nach der Art des abgeschlossenen Geschäfts, der Höhe von Kredit oder Forderung und auch nach den damit in Zusammenhang stehenden Unterlagen gefragt wird. Nähere Überprüfungen sollen stattfinden, wenn sich aus den eingereichten Unterlagen Zweifel hinsichtlich des berechtigten Interesses ergeben oder Betroffene ein solches ausdrücklich bestritten haben. Darüber hinaus werden die übrigen Stichproben einer Plausibilitätskontrolle unterzogen, die allerdings erst nach unserer Intervention jetzt auch dokumentiert wird. Eine solche Dokumentation ist schon deswegen erforderlich, um im Nachhinein feststellen zu können, dass sich tatsächlich eine verantwortliche Person mit den „Rückläufern" befasst hat.

6.2 Umgang mit Schätzdaten

Auskunfteien verwenden im Bereich von Gewerbetreibenden und Freiberuflern häufig „Schätzdaten", die nicht in jedem Fall mit der tatsächlichen Bonität der Betroffenen übereinstimmen. Häufig wurden diese Daten in der Vergangenheit nicht ausreichend als Schätzdaten gekennzeichnet.

Da den Auskunfteien nicht über jeden Gewerbetreibenden oder Freiberufler tatsächliche Werte etwa über Umsätze zur Verfügung stehen, verwenden sie hierfür sogenannte „Branchendurchschnittswerte", die nicht mit den tatsächlichen Werten übereinstimmen, die der Betroffene im Einzelfall erreicht. Bei diesen Daten handelt es sich gesetzlich um Schätzdaten, die im Gesetz ausdrücklich genannt sind und daher von den Auskunfteien auch verwendet werden dürfen. An die Zulässigkeit der Übermittlung dieser Schätzdaten ist jedoch die Voraussetzung geknüpft, dass diese als solche deutlich gekennzeichnet werden. Andernfalls wird bei dem Empfänger der Daten ein falscher Eindruck erweckt. Es könnte zu Fehleinschätzungen in positiver oder auch für den Betroffenen negativer Richtung kommen.

Die Verbände der Handelsauskunfteien vertreten insoweit die Auffassung, dass es bei Übermittlung mehrerer verschiedener Datenarten, von denen nur einzelne geschätzt, andere aber individuell ermittelt wurden, ausreicht, den gesamten Block in einer Weise zu kennzeichnen. Dies könne „Branchendurchschnittswerte" oder „einzelne Daten sind geschätzt" lauten. Dem sind die Datenschutzaufsichtsbehörden

entschieden entgegengetreten.

In Hamburg wurde eine Auskunftei in diesem Punkt geprüft. Dabei hat sich ergeben, dass auch dieses Unternehmen einen ganzen Block von verschiedenen Geschäftszahlen, bei denen es sich teilweise um geschätzte und teilweise um reale Zahlen handelte, mit folgenden Worten untertitelt hatte: „Bei den vorgenannten Unternehmenszahlen kann es sich teilweise um auf Basis von Branchendurchschnittswerten geschätzte Angaben handeln". Eine solche Auskunft ist weder transparent, noch entspricht sie den gesetzlichen Vorgaben, wonach geschätzte Daten deutlich zu kennzeichnen sind. Auf Nachfrage hat das Unternehmen sehr schnell erkennen lassen, dass beabsichtigt ist, eine klare Trennung zwischen geschätzten und tatsächlichen Daten herbeizuführen und dabei die Schätzdaten für den Auskunftsempfänger bzw. den Betroffenen eindeutig (mit einem Sternchen *) zu kennzeichnen.

Bedauerlicherweise zog sich dieses Versprechen auf eine Änderung des Konzepts im Rahmen einer laufenden Projektplanung längere Zeit hin, ohne dass ein konkretes Ergebnis zu verzeichnen gewesen wäre. Im September 2013 hat das Unternehmen die Umstellung jedoch abgeschlossen und verhält sich seitdem datenschutzkonform.

6.3 Hinweis auf Auskunfteimeldung

Werden von einer verantwortlichen Stelle personenbezogene Daten über eine unbestrittene, nicht beglichene Forderung an eine Auskunftei gemeldet, ist dies nur unter Berücksichtigung einer Reihe von Voraussetzungen zulässig. Insbesondere muss der Betroffene rechtzeitig vor der Übermittlung der Angaben über die bevorstehende Übermittlung unterrichtet werden.

Ein hamburgisches Inkassounternehmen, das eng mit einer Auskunftei zusammenarbeitet, hat bereits vor Jahren damit begonnen, die Benachrichtigungspflicht der Auskunftei vorwegzunehmen und die Betroffenen über eine mögliche Speicherung bei der Auskunftei vorsorglich im Vorwege zu unterrichten. Dieses Vorgehen entlastete die Auskunftei in Bezug auf ihre Verpflichtung nach § 33 Abs. 1 Satz 2 BDSG zur Benachrichtigung bei der erstmaligen Übermittlung der personenbezogenen Daten an Dritte.

Zunächst hatte es damals einige Beschwerden über die Information durch das Inkassounternehmen gegeben, weil die Betroffenen sich durch die Ankündigung einer Auskunfteimeldung zur Zahlung genötigt fühlten. In diesem Zusammenhang fanden schon vor Jahren Gespräche mit der Datenschutzaufsichtsbehörde statt, die zum Ergebnis hatten, dass das Inkassounternehmen in der Information die rechtlichen Vorgaben einer Meldung an die Auskunftei, die nur unter eingeschränkten gesetzlich festgelegten Voraussetzungen zulässig sind, genauer darstellte.

Nach der Novellierung des BDSG zur Datenübermittlung an Auskunfteien gibt es sogar eine Verpflichtung der verantwortlichen Stelle nach § 28a Abs. 1 Nr. 4 c) BDSG, den Betroffenen rechtzeitig vor der Übermittlung der Angaben über die Forderung an Auskunfteien über die bevorstehende Übermittlung zu unterrichten. Die Zulässigkeit der Übermittlung selbst ist abhängig von mehreren Voraussetzungen. Daher stellte sich die Frage, mit welchem Text das Inkassounternehmen diese Information in rechtlich zulässiger Weise erteilen kann. Nach Vorlage mehrerer Textentwürfe bei uns und Diskussionen über deren Inhalt hat sich das Unternehmen zuletzt entschlossen, die Betroffenen mit einem Hinweis zu informieren, der die rechtlichen Voraussetzungen, unter denen die Übermittlung nach § 28 a Abs. 1 BDSG erfolgen darf, vollständig wiedergibt. Diese Verfahrensweise, die den Betroffenen Transparenz verschafft, fand auch Zustimmung im Kreis der Arbeitsgruppe Auskunfteien des Düsseldorfer Kreises.

6.4 Benachrichtigung bei Übermittlung von Scorewerten

Auskunfteien sind auch bei ausschließlicher Übermittlung von Scorewerten verpflichtet, die Betroffenen nach § 33 BDSG bei erstmaliger Übermittlung zu benachrichtigen.

Im Rahmen der AG Auskunfteien des Düsseldorfer Kreises wurde die Praxis von Auskunfteien erörtert, bei Übermittlung von Scorewerten über Betroffene an Dritte die Betroffenen entgegen § 33 BDSG über die erstmalige Übermittlung nicht zu benachrichtigen. Die Vertreter der Auskunfteien argumentierten, dass die Scoreberechnung zum Zeitpunkt jeder Anfrage neu berechnet und nicht im Auskunfteidatenbestand gespeichert werde.

Sinn und Zweck der Benachrichtigungspflicht nach § 33 BDSG ist es jedoch, denjenigen Betroffenen, über die Speicherungen oder Übermittlungen personenbezogener Daten vorgenommen werden, darüber Kenntnis und die Möglichkeit zu verschaffen, die Richtigkeit der Daten und auch die Berechtigung der Erhebung der Daten durch einen Dritten zu überprüfen. Andernfalls würde sich der gesamte Vorgang hinter dem Rücken Betroffener abspielen, die davon im Falle unzulässigen Ausspionierens nicht einmal etwas erfahren würden. Der Argumentation der Auskunfteienvertreter musste auch entgegengehalten werden, dass sogar eine gesetzliche Verpflichtung zur Speicherung der Scorewerte für die Auskunftsverpflichtungen nach § 34 BDSG an die Betroffenen besteht und daher auf jeden Fall auch eine Benachrichtigung bei der erstmaligen Übermittlung von Scorewerten zu erfolgen hat.

Die Aufsichtsbehörden stellten klar, dass sie die Möglichkeit haben, nach § 43 Abs.1 Nr. 8 BDSG ein Bußgeld zu erlassen, wenn Auskunfteien gegen die Benachrichtigungspflicht nach § 33 BDSG verstoßen.

7. Transport und Verkehr

7.1 Ortungssysteme in Mietwagen

Die routinemäßige GPS-Ortung von Mietwagen ohne Einwilligung der Mieter ist nicht zulässig.

Durch eine Beschwerde wurde der Aufsichtsbehörde bekannt, dass die Europcar Autovermietung GmbH (Europcar) in 1.300 hochwertigen Fahrzeugen ihrer Flotte Ortungssysteme eingebaut hatte und damit die Mieter ohne deren Wissen ortete. Nach Angaben des Unternehmens diente die Übermittlung der Ortungsdaten dazu, Diebstähle aufzuklären. Außerdem sollte kontrolliert werden, ob sich der Mieter noch im zulässigen Gebiet befindet, da die Benutzung der Fahrzeuge in verschiedenen Ländern vertraglich ausgeschlossen ist. Neben dem Standort wurden Datum, Zeit und auch die Geschwindigkeit der Fahrzeuge erhoben.

Bei Vor-Ort-Ermittlungen stellte die Aufsichtsbehörde fest, dass die Angaben des Unternehmens unvollständig waren. Eine Kontrolle bei einer Firma in Schleswig-Holstein, die im Auftrag des Unternehmens seit 2004 die Fahrzeugortung vornahm, ergab, dass auch ohne Anlass alle 48 Stunden eine Ortung der Fahrzeuge vorgenommen wurde. Außerdem erfolgte eine automatische Übermittlung der Daten, sobald mit dem Fahrzeug in ein Hafengebiet gefahren wurde.

Nach Auffassung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit stellen die heimliche Ortung von Mietfahrzeugen und die heimliche Kontrolle der Mieter einen schweren Eingriff in deren Persönlichkeitsrecht dar. Europcar war es dadurch möglich, Bewegungsprofile seiner Kunden zu erstellen. Mit Hilfe der Ortungstechnik lässt sich nicht nur rekonstruieren, wer sich wann wo aufgehalten hat, sondern auch, wer zu welchem Zeitpunkt mit welcher Geschwindigkeit gefahren ist. Insbesondere durch die anlasslose Ortung wurden die Mieter regelmäßig auch unter einen Generalverdacht gestellt.
Da die Übermittlung der Ortungsdaten ohne Wissen und ohne Einwilligung der Mieter erfolgte, war sie ordnungswidrig. Außerdem gab es zwischen dem Unternehmen und der ausführenden Firma keinen Vertrag zur Auftragsdatenverarbeitung nach dem Bundesdatenschutzgesetz. Europcar hat die heimliche Ortung nach unserem Tätigwerden eingestellt. Gegen das Unternehmen wurde ein Bußgeld festgesetzt.

Der Einsatz von Ortungssystemen bei Mietfahrzeugen setzt zumindest eine vollständige Information über Art und Weise der Ortung sowie die ausdrückliche Einwilligung der Betroffenen in das Tracking voraus. Jeder Mieter muss das Recht haben, selbst darüber zu entscheiden, ob er Fahrzeuge anmieten will, deren Nutzung beim Vermieter oder dessen Vertragspartnern unmittelbar eine individuelle digitale Nutzungsspur hinterlässt. Über die Übermittlung der Ortungsdaten werden Mieter nun im Vorwege

informiert und müssen ihr im Rahmen des Mietvertrags zustimmen. Dadurch wird gewährleistet, dass keine heimlichen Überwachungen mehr stattfinden.

7.2 Datenverarbeitung durch Taxizentralen

Eine Umfrage bei Taxizentralen zur Verarbeitung personenbezogener Daten wurde zum Anlass genommen, Kriterien hierzu zu entwickeln.

Im Berichtszeitraum haben wir uns mit der Verarbeitung von personenbezogenen Daten durch Taxizentralen beschäftigt. Aufgrund der angeforderten Stellungnahmen der Hamburger Taxizentralen wurde eine datenschutzrechtliche Bewertung vorgenommen.

Viele Taxi-Zentralen haben uns mitgeteilt, dass Bestelldaten von Kunden bis zu drei Monaten gespeichert werden. Die Speicherung der Bestelldaten ist im Rahmen der Zweckbestimmung eines Vertragsverhältnisses und zur Durchführung des Vertrages gem. § 28 Abs. 1 Satz 1 Nr. 1 Bundesdatenschutzgesetz (BDSG) zulässig. Eine mehrwöchige Speicherung halten wir je nach Geschäftsverfahren und Abläufen in den einzelnen Zentralen aufgrund von Rechnungsfahrten, Fundstücken, Kundennachfragen und Beschwerden für akzeptabel.

Eine darüber hinausgehende Speicherung von Kundendaten zur schnelleren Bestellabwicklung und kundenfreundlichen Ansprache ist jedoch gem. § 28 Abs. 1 Satz 1 Nr. 2 BDSG nur unter bestimmten Umständen rechtmäßig. Die Taxizentralen haben zwar ein berechtigtes Interesse an einer schnelleren Bestellabwicklung und einer kundenfreundlichen Ansprache. Die Kunden haben jedoch ein schutzwürdiges Interesse daran, dass ihre Daten nicht ohne ihre Kenntnis gespeichert werden. Die Speicherung darf daher – auch aufgrund der Benachrichtigungspflicht des § 33 BDSG - nur erfolgen, wenn die Kunden vor der ersten Speicherung über die Speicherung und deren Zweck informiert wurden und sie dieser Speicherung nicht widersprochen haben.

Einige Taxizentralen haben mitgeteilt, dass die Gesprächsanteile der Mitarbeiter bei Telefongesprächen mit Kunden zur Bearbeitung von Beschwerden aufgezeichnet werden. Dabei ist Folgendes zu beachten:

Das Aufzeichnen von Telefongesprächen ist strafbar, soweit dies unbefugt im Sinne des § 201 Abs. 1 Strafgesetzbuch (StGB) erfolgt. Eine Befugnis zum Aufzeichnen von Telefongesprächen durch eine Taxizentrale besteht nur dann, wenn die Mitarbeiter hierin eingewilligt haben oder eine gesetzliche Erlaubnis vorliegt. Eine Rechtsgrundlage, die die Aufzeichnung der Telefongespräche der Mitarbeiter mit den Kunden ohne deren Einwilligung erlaubt, ist weder in § 32 noch in § 28 Abs. 1 Nr. 2 BDSG zu sehen. Die Interessen der Mitarbeiter überwiegen die Interessen der Taxizentralen an der

Aufzeichnung, weil die Gesprächsinhalte umfangreicher sein können, als für die Erfüllung des Geschäftszweckes erforderlich ist.
Eine arbeitsvertragliche Regelung ist grundsätzlich auch nicht als wirksame Einwilligung eines Mitarbeiters in die Aufzeichnung seiner Gespräche mit Kunden zu werten. Aufgrund des Abhängigkeitsverhältnisses des Mitarbeiters zu seinem Arbeitgeber würde eine Einwilligung in die Aufzeichnung seiner geschäftlichen Gespräche unter faktischem Zwang und demnach nicht wie gesetzlich vorgesehen aufgrund der freien Entscheidung der Betroffenen gegeben werden. Eine Betriebsvereinbarung, in der die Persönlichkeitsrechte der Mitarbeiter Berücksichtigung finden würden, liegt gegenwärtig nicht vor. Eine Auswertung der Daten zu Zwecken der Leistungs- und Verhaltenskontrolle ist im Übrigen unzulässig. Es bestehen daher erhebliche Zweifel, ob eine Befugnis i.S.d. § 201 StGB für die Aufzeichnung vorliegt.

Einige Taxizentralen haben uns mitgeteilt, dass ein GPS-Datenfunksystem genutzt wird. Das System wird zum Zweck der Tourenvermittlung sowie zur Unterstützung der Fahrerinnen und Fahrer bei Notrufauslösung genutzt. Weiterhin wurde angegeben, dass das System zudem für die Fahrtenabrechnung, Bearbeitung von Reklamationen, Nachfragen und Beschwerden sowie zum Auffinden von Fundsachen genutzt wird.

Die Erhebung und Verwendung der GPS-Ortungsdaten zum Zwecke der Tourenvermittlung sowie zur Standortermittlung bei Notfällen halten wir gem. § 28 Abs. 1 Satz 1 Nr. 1 oder Nr. 2 BDSG für rechtlich zulässig. Die Ortung bei der Tourenvermittlung ist darauf gerichtet, u.a. das nächste freie Taxi (das ggf. auch Sonderwünschen des Kunden entspricht) zu vermitteln, dadurch die Wartezeit des Kunden zu verkürzen sowie den Fahrgast bei Bestellung eines Taxis über die Wartezeit zu informieren. Bei Notfällen dient die Ortung der schnellen Vermittlung von Hilfe für die Fahrerinnen und Fahrer sowie dem Wiederauffinden eines (ggf. gestohlenen oder entführten) Wagens.

Eine Erforderlichkeit der GPS-Ortung zum Zwecke der Bearbeitung von Beschwerden sowie zum Auffinden von Fundsachen ist jedoch fraglich, da die Bearbeitung von Reklamationen nicht zu den originären Betriebszwecken einer Taxizentrale zählt. Der Fahrgast geht als Kunde schließlich nur ein Rechtsverhältnis mit dem Taxi-Unternehmer bzw. dem Taxifahrer ein. Zur Rückverfolgung von Taxis kann dem Kunden auch zugemutet werden, sich den Fahrzeughalter, Kennzeichen oder Konzessionsnummer des Taxis zu merken. Bei Rechnungsfahrten ist davon auszugehen, dass es sich um bestellte Taxen handelt und die für die Abrechnung erforderlichen Daten ohnehin als Bestelldaten gespeichert werden. Eine Speicherung der GPS-Daten aufgrund von Kundenbeschwerden über mehrere Wochen ist ebenfalls nicht erforderlich, da davon auszugehen ist, dass die meisten Kunden zeitnah nachfragen oder sich beschweren.

Daher muss die lange Speicherdauer der GPS-Ortungsdaten von teilweise bis zu 55 Tagen als unzulässig angesehen werden. Als zulässig kann aus unserer Sicht maximal eine Speicherdauer der GPS-Ortungsdaten von 7 Tagen angesehen werden. Dies ist

für die Tourenvermittlung und die Notrufverfolgung ausreichend. Für den Zweck der Abrechnung ist eine Speicherung der Ortungsdaten wie dargelegt grundsätzlich gar nicht erforderlich.
Für den Zweck der Kundenbeschwerden ist eine Speicherung über einen Zeitraum von 7 Tagen hinaus ebenfalls nicht erforderlich.

Zudem überwiegen bei einer Speicherung von mehr als 7 Tagen die Interessen der Fahrerinnen und Fahrer am Ausschluss der Speicherung der Ortungsdaten, weil bei der GPS-Ortung aller Taxen wesentlich mehr Ortungsdaten gespeichert werden, als für die Erfüllung des Zweckes der Bearbeitung von Beschwerden erforderlich ist und das Verhalten sowie der Aufenthaltsort während der gesamten Arbeitszeit lückenlos überwacht und nachvollzogen werden kann.

Aus den Antworten der Taxi-Zentralen ergibt sich schließlich, dass keine Weitergabe der GPS-Ortungsdaten an die angeschlossenen Taxi-Unternehmen erfolgt. Eine solche würde auch gegen § 28 Abs.1 Satz 1 Nr. 2 BDSG verstoßen, weil schutzwürdige Interessen der Fahrerinnen und Fahrer überwiegen, und wäre nicht zulässig.

Die Taxizentralen wurden aufgefordert, unter Berücksichtigung dieser Bewertung eine datenschutzkonforme Verarbeitung personenbezogener Daten sicherzustellen und nach oben dargelegten Vorgaben umzusetzen. Die Taxizentralen haben jetzt Gelegenheit, zu dieser Bewertung und deren Umsetzung Stellung zu nehmen. Einige Stellungnahmen stehen noch aus; wir werden über den Fortgang berichten.

7.3 Datenerhebung bei Ausgabe verbilligter Zeitkarten durch die Hamburger Hochbahn AG

Die Hamburger Hochbahn AG verzichtet in Zukunft auf die Befragung zum Fahrverhalten von Beziehern verbilligter Zeitkarten im Ausbildungsverkehr.

Im Zusammenhang mit der Ausgabe von verbilligten Zeitkarten im Ausbildungsverkehr forderte die Hamburger Hochbahn AG (Hochbahn) die Bezieher dazu auf, einen Fragebogen auszufüllen, in dem detaillierte Angaben zum Fahrverhalten verlangt wurden. Diese betrafen nicht nur den Weg zur Ausbildungsstätte und die dafür genutzten Linien bzw. Verkehrsmittel, sondern auch die zu privaten Zwecken genutzten Linien. Hiergegen hatten sich mehrfach Auszubildende oder deren Eltern gewandt mit der Befürchtung, dass die Hochbahn die Daten zur Erstellung von personenbezogenen Bewegungsprofilen nutzen könnte.

Unsere Überprüfung ergab, dass die Verkehrsunternehmen für die Ausgabe verbilligter Zeitkarten im Ausbildungsverkehr Ausgleichszahlungen nach §45 a Personenbeförderungsgesetz (PBefG) und § 6a Allgemeines Eisenbahngesetz (AEG) durch die Bundesländer erhalten. Für diese Ausgleichszahlungen sind Faktoren wie Fahrtenzahl, Fahrtenweite und ein Verbundfaktor (Summe der genutzten Linien einzelner Verkehrsunternehmen) maßgebend, wobei der Gesetzgeber hierzu Werte vorgegeben hat. Im PBefG wird eine individuelle Fahrtenzahl von 2,3 am Tag angesetzt.

Nach Angaben der Hochbahn müssen höhere Werte nachgewiesen werden, wenn ein Unternehmen höhere Ausgleichszahlungen erhalten wolle. Für diesen Nachweis würde die Erhebung im Ausbildungsverkehr durchgeführt. Aufgrund der Befragung hätten einige Unternehmen im Hamburger Verkehrsverbund (HVV) eine höhere Fahrtenzahl nachweisen können. Dabei seien auch die sonstigen Fahrten mit eingeflossen. Würden diese Fahrten nicht mit in die gesetzlichen Ausgleichszahlungen einfließen, wären die Fahrkarten alternativ nur für den Schulverkehr gültig. Dies sei politisch nicht gewollt und zudem schwierig zu kontrollieren. Um die von den Behörden vorgegeben Quoten bezüglich der Stichprobengröße einhalten zu können, sei die Ausgabe neuer Fahrkarten an die Rückgabe des Fragebogens gekoppelt. Bei der Rückgabe würde mittels des Fragebogens und des Berechtigungsscheines der Eingang des Fragebogens vermerkt. Bei Schülerinnen und Schülern der Grundschulklassen ohne Berechtigungsscheine sei unten im Fragebogen die Abonnentennummer vermerkt. Nach Eingang der Fragebögen würden diese von den Berechtigungsscheinen getrennt bzw. die Abonnentennummer vom Fragebogen abgetrennt und sodann statistisch ausgewertet. Eine Zuordnung des Fragebogens zu einem Kunden sei dann nicht mehr möglich. Der Fragebogen enthalte einen entsprechenden Hinweistext für die Bezieher. Diese Form der Erhebung und Auswertung von Daten gebe es so nur bei den Zeitkarten im Ausbildungsverkehr.

Unter Berücksichtigung dieser Sach- und Rechtslage war nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG die Erhebung von Daten über das Fahrverhalten von Auszubildenden in dem beschriebenen Umfang nicht zu beanstanden. Dabei war das berechtigte Interesse des Unternehmens an höheren Ausgleichszahlungen zu berücksichtigen, dem keine überwiegenden schutzwürdigen Interessen der Bezieher der Wertmarken gegenüberstanden, da die Auswertung anonym erfolgte.

Zwischenzeitlich hat die Hochbahn mitgeteilt, dass in Zukunft auf die Befragung verzichtet werden könne, da es nach langen Verhandlungen zwischen den Bundesländern zu einer Einigung über eine Pauschalierung der Ausgleichszahlungen gekommen sei.

8. Videoüberwachung

8.1 Videoüberwachung des öffentlichen Straßenraums

Einer weitreichenden Überwachung des öffentlichen Straßenraums zur Abschreckung und zur Sicherung von Beweismaterial stehen die überwiegenden schutzwürdigen Interessen der von der Überwachung betroffenen Passanten entgegen.

Im Berichtszeitraum haben uns zahlreiche Beschwerden zur Videoüberwachung öffentlicher Fußwege und Straßen durch private Unternehmen und Einzelkaufleute erreicht. In einem Fall hat uns ein Petent auf die Außenkameras einer Juwelierfiliale am Jungfernstieg aufmerksam gemacht, da er eine Überwachung des öffentlichen Fußweges befürchtete.
Zur Überprüfung der Beschwerde haben wir das Unternehmen zu einer Stellungnahme aufgefordert und um die Übersendung der Überwachungsbilder gebeten. Eine Überprüfung der zur Verfügung gestellten Bilder ergab, dass die Außenkameras nicht nur das Schaufenster, sondern auch in großem Umfang den öffentlichen Fußweg vor dem Schaufenster und sogar Teile der gegenüberliegenden Straßenseite erfassten.

Nach § 6b BDSG ist eine Beobachtung öffentlich zugänglicher Räume, hierzu zählen auch öffentliche Wege, Straßen und Plätze, mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Grundsätzlich halten wir eine Videoüberwachung innerhalb und außerhalb von Juweliergeschäften aufgrund der Gefahr von Raubüberfällen, Einbrüchen und Diebstählen für datenschutzrechtlich zulässig. Der Umfang der Überwachung muss dabei aber räumlich und zeitlich auf das unbedingt erforderliche Maß beschränkt werden und darf nicht zu einer unverhältnismäßigen Beeinträchtigung des informationellen Selbstbestimmungsrechts der von der Überwachung betroffenen Personen führen.

In einer Stellungnahme teilte uns das Unternehmen mit, die weiträumige Überwachung des Außenbereichs sei zur Identifizierung von verdächtigen Personen notwendig, die sich vor einem Überfall auch im weiteren Umfeld der Filiale aufhalten würden, um diese auszuspähen.

Wir haben bereits Zweifel, ob diese Argumentation ein berechtigtes Interesse des Unternehmens darstellt. Generalpräventive Maßnahmen und die Strafverfolgung sind öffentliche Aufgaben. Daher obliegt es den Sicherheitsbehörden, also in erster Linie der Polizei unter den engen gesetzlichen Voraussetzungen im Polizeirecht, eine Video-

Überwachung des öffentlichen Raumes vorzunehmen. Würden wir die Überwachung und Identifizierung verdächtiger Personen, die sich auf öffentlichen Wegen und Straßen aufhalten, als berechtigtes Interesse privater Unternehmen und Einzelkaufleute anerkennen, so wäre es praktisch jeder verantwortlichen Stelle gestattet, Passanten im öffentlichen Straßenraum zu überwachen. Eine Totalüberwachung der Hamburger Innenstadt könnte das Ergebnis sein. Dies wäre mit der vom Gesetzgeber beabsichtigten begrenzenden Wirkung des § 6b BDSG nicht zu vereinbaren.

Zweifelhaft ist ebenso die Erforderlichkeit einer solchen umfangreichen Videoüberwachung öffentlicher Straßen und Wege, da den zur Verfügung gestellten Bildern entnommen werden konnte, dass sich alle von dem Unternehmen als verdächtig eingestuften Personen zumindest zeitweilig direkt vor den Schaufenstern aufgehalten haben. Eine in ihrem Umfang deutlich auf den unmittelbaren Bereich vor dem Schaufenster beschränkte Videoüberwachung wäre somit mit Blick auf die Grundsätze der Datenvermeidung und Datensparsamkeit (§ 3a BDSG) ebenso zur Identifizierung von verdächtigen Personen geeignet gewesen.

Aber selbst wenn eine Erforderlichkeit anzunehmen wäre, scheitert die Zulässigkeit dieser umfänglichen Überwachung im Außenbereich der Filiale im Ergebnis an den überwiegenden schutzwürdigen Interessen der Passanten, sich weitestgehend überwachungsfrei im öffentlichen Raum bewegen zu können. Wir verkennen bei unserer Abwägung nicht, dass sich hier hohe Rechtsgüter gegenüber stehen. Auf der einen Seite das Grundrecht der Passanten auf informationelle Selbstbestimmung und auf der anderen Seite das Eigentumsrecht des Unternehmens sowie, mit Blick auf die Beschäftigen des Juweliers, das Recht auf Schutz von Leib und Leben.

Allerdings ist zu berücksichtigen, dass es sich bei der Videoüberwachung öffentlicher Wege wie dem Hamburger Jungfernstieg um eine Maßnahme mit großer Streubreite handelt. Durch die vorgefundene Ausrichtung der Kameras erfolgte anlasslos eine Speicherung von Überwachungsbildern einer Vielzahl von Passanten, ohne dass diese durch ihr Verhalten einen Anlass hierfür gaben. Während Passanten direkt vor dem Geschäft und dem Schaufenster aufgrund der entsprechenden Videoüberwachungshinweise damit rechnen müssen, Gegenstand einer Videoüberwachung zu werden, trifft dies in weiterer Entfernung von dem Geschäft nicht zu. Es ist den Passanten auch nicht zuzumuten, aufgrund der Videoüberwachung die Straßenseite zu wechseln.

Wir haben das Unternehmen zur Sicherstellung einer datenschutzkonformen Videoüberwachung daher aufgefordert, die Kameras im Außenbereich so auszurichten, dass lediglich ein maximal ein Meter breiter Streifen der vor den Schaufenstern und Eingängen liegenden öffentlichen Flächen beobachtet und aufgezeichnet wird. Ebenso haben wir auf die gesetzliche Verpflichtung aufmerksam gemacht, deutlich sichtbare Hinweise auf die Videoüberwachung anzubringen und auf diesen Hinweisen die verantwortliche Stelle zu benennen.

8.2 Videoüberwachung in und an Taxis

Die Datenschutzaufsichtsbehörden der Länder haben einen Beschluss zur Videoüberwachung in und an Taxis gefasst. Die Durchführung von Kontrollen videoüberwachter Taxis gestaltet sich schwierig.

In unserem 23. Tätigkeitsbericht haben wir bereits über die Videoüberwachung in Taxis berichtet. Zwischenzeitlich hat der Düsseldorfer Kreis zu diesem Themenfeld einen Beschluss gefasst, der im Volltext auf der Seite des Bundesbeauftragten für Datenschutz und Informationsfreiheit (www.bfdi.bund.de) im Bereich Entschließungen zur Verfügung steht.

Neben der Videoüberwachung im Innenraum eines Taxis, die in engen Grenzen zur Abwehr von Leben, Gesundheit und Freiheit der Taxifahrer datenschutzrechtlich zulässig sein kann (vgl. 23. TB, IV.1.7), greift der Beschluss auch den Betrieb von Außenkameras auf.

Ziel des Einsatzes der auch als Unfallkameras oder Dashcams bezeichneten Geräte ist die Erstellung von Aufnahmen im Straßenraum, um diese bei strittigen Schadensfällen zur Klärung von Verantwortlichkeiten und Haftungsfragen der Verkehrsteilnehmer heranzuziehen. Auch wenn KfZ-Versicherer den Einsatz der Kameras empfehlen und diesen ggf. sogar mit einem Beitragsrabatt honorieren, müssen nicht nur Taxi-Unternehmer berücksichtigen, dass sie die datenschutzrechtliche Verantwortung für den Betrieb der Außenkameras tragen. Für die Beobachtung und Aufzeichnung des öffentlichen Straßenraums gibt es jedoch keine Rechtsgrundlage. Dieses gilt auch für eine durch einen Außenkameraeinsatz mögliche und in dieser Form nicht zulässige Verhaltens- und Leistungskontrolle der angestellten Taxifahrer.

Leider konnten wir unser Vorhaben, im Verlaufe des Berichtszeitraums den Einsatz von Videoüberwachungskameras in Taxis stichprobenartig zu prüfen, nicht umsetzen. Zum einen fehlte uns die personelle Kapazität und zum anderen führten die an uns herangetragenen Beschwerden über einzelne Taxi-Unternehmer letztendlich nicht zu einer Kontrolle, da die zur Stellungnahme aufgeforderten Taxi-Unternehmer in allen Fällen mitteilten, dass es sich bei den in den Taxis installierten Kameras um Attrappen handelte und diese zwischenzeitlich abgebaut seien. Wir appellieren an alle Taxi-Unternehmer, die Videoüberwachungstechnik einsetzen, die Voraussetzungen einer datenschutzkonformen Videoüberwachung zu beachten und eine Kontrolle der Datenschutzaufsichtsbehörde als Chance anzusehen, die Rechtmäßigkeit der Videoüberwachung in ihren Taxis sicherzustellen.

Taxi-Unternehmer sollten sich überdies der Wirkung von Attrappen bewusst sein. Da

die Funktionsunfähigkeit der Kamera nicht erkennbar ist, kann ein Überwachungsdruck hervorgerufen werden und somit zu einer Beeinträchtigung des allgemeinen Persönlichkeitsrechts der Fahrgäste führen.

8.3 Videoüberwachung in einem Medizinischen Versorgungszentrum

Die falschen Auskünfte eines Geschäftsführers zum Betrieb einer Videoüberwachungsanlage in einem Medizinischen Versorgungszentrum wurden mit einem Bußgeld geahndet. Die streitige Kamera wurde abgebaut.

Aufgrund einer Beschwerde sind wir im Berichtszeitraum an einen Geschäftsführer eines Medizinischen Versorgungszentrums (MVZ) herangetreten, um Auskünfte über den Zweck und den Umfang der dort eingesetzten Videoüberwachungsanlage einzuholen. Private Stellen sind nach § 38 Abs. 3 BDSG verpflichtet, der Datenschutzaufsichtsbehörde auf Verlangen die notwendigen Auskünfte unverzüglich zu erteilen.

Der Geschäftsführer begründete die Notwendigkeit der Videoüberwachung des Empfangsbereiches des MVZ sowohl mit präventiven als auch mit repressiven Zwecken, da es in der Vergangenheit zu Übergriffen und Bedrohungen des Personals gekommen sei. Die Kamera solle zum einen abschreckend wirken und so zukünftig Übergriffe und Bedrohungen verhindern sowie das Sicherheitsgefühl der Beschäftigten erhöhen. Zum anderen solle das aufgezeichnete Videomaterial bei entsprechenden Vorfällen als Beweismittel dienen.

Im Verlauf der datenschutzrechtlichen Kontrolle teilte uns der Geschäftsführer schriftlich mit, dass durch große Hinweisschilder in der Praxis auf die Videoüberwachung hingewiesen werde, die von uns geforderte schriftliche Information der Patienten über den Zweck der Videoüberwachung erfolge, alle Beschäftigten über den Einsatz und den Leistungsumfang des Überwachungssystems informiert und diverse technische und organisatorische Maßnahmen umgesetzt seien, um zu gewährleisten, dass nur berechtigte Personen auf das gespeicherte Bildmaterial zugreifen können.

Vor diesem Hintergrund und der Maßgabe, dass sich die hinter dem Empfangstresen arbeitenden Beschäftigten nicht im Erfassungsbereich der Kamera befinden dürfen, haben wir die Videoüberwachung des öffentlich zugänglichen Empfangsbereichs des MVZ aufgrund der vorgetragenen Gefahrenlage ausnahmsweise für zulässig erachtet.

Nach Abschluss des aufsichtsbehördlichen Verfahrens haben wir leider bei einer unangekündigten Nachkontrolle vor Ort festgestellt, dass alle oben dargestellten schriftlichen Auskünfte nicht zutreffend waren. So haben wir u.a. weder die Hinweisschilder und die

schriftliche Patienteninformation in dem MVZ auffinden können, noch waren nach unseren Feststellungen alle Beschäftigten über das Überwachungssystem informiert.
Unmittelbar nach unserem Kontrollbesuch hat uns der Geschäftsführer aus eigener Veranlassung über den Abbau der Kamera informiert. Wir haben aus diesem Grund auf die Verhängung eines Bußgeldes wegen einer nicht zulässigen Videoüberwachung verzichtet. Ein Bußgeld ist dem Geschäftsführer dennoch nicht erspart geblieben. Die Erteilung falscher Auskünfte stellt nach § 43 Abs. 1 Nr. 10 BDSG ein ordnungswidriges Verhalten dar, welches von den Datenschutzaufsichtsbehörden mit einem Bußgeld bis zu 50.000 € geahndet werden kann.

9. Wohnungswirtschaft

9.1 Datenerhebung bei der Vermietung von Wohnraum – Informationsschrift für Vermieter und Mietinteressenten

Einer uneingeschränkten Datenerhebung durch den Vermieter steht das Recht der Mietinteressenten auf informationelle Selbstbestimmung entgegen. Wir haben zu diesem Themenfeld eine umfangreiche Informationsschrift veröffentlicht.

In den vergangenen Jahren haben wir zahlreiche Beschwerden von Mietinteressenten erhalten. Die Beschwerden richteten sich zum einen gegen einzelne Fragestellungen der Vermieter und zum anderen gegen die Praxis, schon vor einem Besichtigungstermin einen umfangreichen Fragebogen zur eigenen Person ausfüllen zu müssen und Nachweise etwa zum Gehalt herauszugeben. Betroffene, die sich weigerten, Fragen bzw. auch nur einzelne Fragen zu beantworten oder geforderte Nachweise schon zu diesem Zeitpunkt vorzulegen, wurden regelmäßig bei der Vergabe der Wohnung nicht mehr berücksichtigt. Mietinteressenten sind vor dem Hintergrund des angespannten Wohnungsmarktes in Hamburg und der existentiellen Bedeutung einer (bezahlbaren) Wohnung somit faktisch gezwungen, alle geforderten Auskünfte zu erteilen, wenn sie den Abschluss eines Mietvertrages anstreben.

Vermieter lassen bei dieser Praxis außer Acht, dass Eingriffe in das Recht der Mietinteressenten auf informationelle Selbstbestimmung nach den Bestimmungen des Bundesdatenschutzgesetzes auf das unbedingt erforderliche Maß zu beschränken sind.

Wir haben die Beschwerden zum Anlass genommen, uns eingehender mit der Erhebung personenbezogener Daten bei der Vermietung von Wohnraum auseinanderzusetzen. Zu diesem Zweck haben wir im Berichtszeitraum etwa 20 Fragebögen hamburgischer Genossenschaften, Wohnungsunternehmen und Makler analysiert und die datenschutzrechtliche Zulässigkeit der vorgefundenen Fragestellungen geprüft. Bei der datenschutzrechtlichen Beurteilung der Zulässigkeit ist es nicht ausreichend, nur

auf die eigentlichen Inhalte der Fragen abzustellen. Vielmehr sind auch die Zeitpunkte der Erhebung und der Vermietungskontext zu berücksichtigen. Während der Vermieter also vor dem Besichtigungstermin von den Mietinteressenten noch keinen Gehaltsnachweis als Beleg für deren Bonität verlangen darf, ist die Forderung eines solchen Nachweises unmittelbar vor Vertragsabschluss datenschutzrechtlich zulässig. Vermieter müssen für jede Phase des Vermietungsprozesses prüfen, welche persönlichen Informationen des Mietinteressenten zu dem jeweiligen Zeitpunkt erforderlich sind. Hierbei kann beispielsweise das Fragerecht bei der Vermietung einer Einliegerwohnung in einem Einfamilienhaus aufgrund des besonderen Näheverhältnisses zwischen Vermieter und Mieter weitergehen als das Fragerecht einer Baugenossenschaft, die eine Wohnung in einer großen Wohnanlage vermieten will. Eine Datenerhebung „auf Vorrat" ist nicht zulässig, auch wenn die Daten in einer späteren Phase, z.B. beim Abschluss des Mietvertrages, benötigt werden könnten.

Das Ergebnis unserer Fragebogenanalyse hat uns veranlasst, eine Informationsschrift mit dem Titel „Fragerecht des Vermieters" zu erstellen, die auf unserer Homepage www.datenschutz-hamburg.de kostenlos zum Download zur Verfügung steht. Die Broschüre erhebt aufgrund der rechtlichen Komplexität des Themenfeldes und der Vielfältigkeit des Wohnungsmarktes nicht den Anspruch, dass sie für die abschließende datenschutzrechtliche Beurteilung aller denkbaren Anwendungsfälle herangezogen werden kann. Eine abschließende Beantwortung der Frage, welche personenbezogenen Daten des Mietinteressenten zu welchem Zeitpunkt datenschutzkonform erhoben werden dürfen, bedarf immer einer Würdigung der konkreten Umstände des Einzelfalls. Die Informationsschrift soll jedoch den Rahmen einer zulässigen Datenerhebung bei der Vermietung von Wohnraum aufzeigen und so Vermietern und Mietinteressenten im Vermietungsprozess eine Orientierung bieten.

Wir fordern die Wohnungswirtschaft auf zu prüfen, ob ihre Praxis bei der Vermietung von Wohnraum den von uns aufgezeigten datenschutzrechtlichen Anforderungen entspricht. Einzelne Unternehmen haben bereits Kontakt mit uns aufgenommen. Dass hier ein Handlungsbedarf besteht, hat ein Vorfall kurz nach der Veröffentlichung unserer Informationsschrift belegt. Eine Wohnungsbaugesellschaft hatte Mietinteressenten zu einer Informationsveranstaltung über ein Neubauprojekt eingeladen und dazu aufgefordert, bei Interesse an einer Anmietung einen umfangreichen Fragebogen ausgefüllt auszuhändigen und Gehaltsnachweise zu hinterlegen, auch wenn aufgrund weiterer Informationsveranstaltungen an diesem Tag noch keine Vertragszusage möglich sei. Nach unserer Intervention verkürzte der Konzern den Fragebogen in erheblichem Umfang und verzichtete auch auf die Hinterlegung von Gehaltsnachweisen.

Die Veröffentlichung unserer Informationsschrift hat dazu geführt, dass wir weitere Beschwerden von Mietinteressenten erhalten haben. Wir gehen diesen nach, stehen aber gleichzeitig für die Beratung der Wohnungswirtschaft sowie für einen konstruktiven Dialog mit Vertretern der Wohnungswirtschaft zur Verfügung.

9.2 Veröffentlichung von personenbezogenen Daten im Internet

Eine Veröffentlichung von personenbezogenen Daten der Mitgliedervertreter einer Genossenschaft im Internet darf nur mit Einwilligung der Betroffenen erfolgen.

Im Berichtszeitraum veröffentlichte eine Genossenschaft die Namen und Adressen ihrer Mitgliedervertreter auf ihrer Internethomepage. Eine Vertreterin hatte Zweifel, ob die Veröffentlichung ihrer personenbezogenen Daten ohne ihre Einwilligung datenschutzkonform sei und wandte sich zur Klärung dieser Frage an uns. Sie hatte gegenüber der Genossenschaft bereits erklärt, dass sie mit einer Veröffentlichung ihres Namens und ihrer Adresse im Internet nicht einverstanden sei.

Die Regelungen des Genossenschaftsgesetzes sehen als dem BDSG vorrangige Rechtsvorschriften vor, dass eine Liste mit den Namen und Anschriften der gewählten Vertreter und Ersatzvertreter mindestens zwei Wochen lang in den Geschäftsräumen der Genossenschaft zur Einsichtnahme für die Mitglieder auszulegen ist. Weiterhin ist die Auslegung der Liste in einem öffentlichen Blatt bekannt zu machen. Hieraus ergibt sich nur die Befugnis der Genossenschaft, den Umstand der Auslegung in einem öffentlichen Blatt bekannt zu machen, aber nicht die Liste als solche in einem öffentlichen Blatt zu publizieren.

Die Genossenschaft konnte die Veröffentlichung der Namen und der Adressen der Mitgliedervertreter im Internet somit nur auf die Einwilligung der Mitgliedervertreter oder auf eine Vorschrift des BDSG stützen. Eine Einwilligung der Mitgliedervertreter lag unbestritten nicht vor.

Die Genossenschaft hätte die Veröffentlichung im Internet daher ausschließlich bei Vorliegen der Voraussetzungen des § 28 Abs. 1 Satz 1 Nr. 2 BDSG vornehmen dürfen. Danach ist das Übermitteln personenbezogener Daten zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse Betroffener an dem Ausschluss der Übermittlung überwiegt.

Eine Erforderlichkeit der Veröffentlichung der Mitgliedervertreterdaten im Internet ist nur dann anzunehmen, wenn das mit der Veröffentlichung verfolgte Ziel erreicht werden kann und hierfür mit Blick auf die informationelle Selbstbestimmung der betroffenen Mitgliedervertreter kein milderes, gleich wirksames Mittel zur Verfügung steht.

Da die Genossenschaft durch die Auslegung der Vertreterliste in den Geschäftsräumen ihren gesetzlichen Informationsverpflichtungen nachkommt und alle Mitglieder nach den Bestimmungen des Genossenschaftsgesetzes eine Abschrift der Liste mit

Anschriften verlangen können, haben wir bereits eine Erforderlichkeit der Veröffentlichung der Vertreterdaten im Internet verneint. Die Veröffentlichung von Angaben im Internet führt zu einer unbegrenzten, unbeherrschbaren und nach dem heutigen Stand der Technik irreversiblen Öffentlichkeit. Die mit der Publizierung im Internet verbundene Eingriffsintensität in die Persönlichkeitsrechte der Betroffenen ist daher im Vergleich zu einer Listenauslegung bzw. der Weitergabe von Abschriften an einzelne Mitglieder deutlich höher einzustufen. Insofern stellen die Auslegung der Liste und die Möglichkeit der Mitglieder, Abschriften der Vertreterliste zu erhalten, gleich wirksame, aber mit Blick auf die informationelle Selbstbestimmung der betroffenen Mitgliedervertreter mildere Veröffentlichungswege dar.

Weiterhin haben wir in diesem Fall auch ein Überwiegen der schutzwürdigen Interessen der betroffenen Mitgliedervertreter angenommen. Auch wenn nur wenige Mitgliedervertreter der Veröffentlichung ihrer Daten im Internet widersprochen haben sollten, so stellen diese Widersprüche einen Anhaltspunkt dafür dar, dass entgegenstehende Interessen der Betroffenen bestehen. Mit der Übernahme der Mitgliedervertreterfunktion geben die Betroffenen lediglich zu erkennen, dass sie mit der Veröffentlichung ihres Namens und ihrer Anschrift per Auslegung der Liste in den Geschäftsräumen der Genossenschaft oder auf entsprechenden Abschriften für Mitglieder einverstanden sind, also mit der Bekanntgabe gegenüber einem sehr eingeschränkten Personenkreis, namentlich den der anderen Mitglieder. Ein gewichtiges Interesse der Genossenschaft, die Namen und Adressen der Mitgliedervertreter auch über den Kreis der Genossenschaftsmitglieder hinaus bekanntzugeben, ist nicht erkennbar.

Im Ergebnis ist eine Veröffentlichung von personenbezogenen Daten der Mitgliedervertreter im Internet nur mit Einwilligung der Betroffenen zulässig. Wir haben aus diesem Grund die Genossenschaft aufgefordert, zukünftig die datenschutzrechtlichen Bestimmungen bei der Veröffentlichung von Mitgliederdaten im Internet zu beachten. Da das strittige Dokument schon vor Abschluss unserer Kontrolle von der Homepage der Genossenschaft entfernt wurde, haben wir darauf verzichtet, diesen datenschutzrechtlichen Verstoß mit einem Bußgeld zu ahnden.

9.3 Übermittlung von Kündigungsschreiben an öffentliche Stellen

Vermieter müssen ihre Mieter über die Weiterleitung eines Kündigungsschreibens an die Fachstellen für Wohnungsnotfälle informieren und eine Widerspruchsfrist einräumen.

Es ist gängige Praxis einer großen Hamburger Wohnungsgesellschaft, bei fristlosen Kündigungen aufgrund von Mietrückständen oder nicht gezahlten Kautionen die Fachstellen für Wohnungsnotfälle der Bezirke zu informieren. Die Information erfolgt durch

Übersendung einer Kopie des Kündigungsschreibens. Die Fachstellen für Wohnungsnotfälle beraten Menschen, die vom Verlust ihrer Wohnung bedroht sind, um das noch bestehende Mietverhältnis zu sichern. Bei bestehenden Mietschulden kann ein Darlehen vergeben werden. Vielfach wird die Fachstelle auch von Gerichten und anderen Dienststellen darüber informiert, dass ein Mietverhältnis in Gefahr ist. Sie kann dann unmittelbar Kontakt zu dem betroffenen Mieter aufnehmen.

Die Weitergabe von Kopien der Kündigungsschreiben an die Fachstelle für Wohnungsnotfälle ist ein Übermitteln personenbezogener Daten i.S.d. § 3 Abs. 4 Nr. 3 BDSG. Diese Übermittlung ist nach dem BDSG nur gestattet, wenn eine Vorschrift des BDSG oder eine andere Rechtsvorschrift dies erlaubt oder soweit der Betroffene eingewilligt hat.

Die Umsetzung einer Einwilligungslösung, zum Beispiel durch die Unterzeichnung einer entsprechenden Erklärung bei Vertragsabschluss, kommt bei der vorliegenden Konstellation nicht in Betracht. Das BDSG fordert für die Wirksamkeit einer Einwilligung, dass diese auf der freien Entscheidung des Betroffenen beruhen muss. Ein Mietinteressent müsste vor dem Hintergrund der schwierigen Wohnungsmarktlage bei Verweigerung der Einwilligung befürchten, die gewünschte Wohnung nicht zu erhalten. Eine solche Lage lässt keine freie Entscheidung des Betroffenen zu. Aufgrund der Drucksituation können Mieter auch nicht zu einem späteren Zeitpunkt, wenn bereits ein Konflikt aufgrund ausstehender Mietzahlungen besteht, wirksam in die Übermittlung einwilligen.

Als Erlaubnisnorm für die Weitergabe der Kündigungsschreiben kommt daher nur die allgemeine Rechtsvorschrift des § 28 Abs. 1 Nr. 2 BDSG in Betracht. Danach ist das Übermitteln personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Übermittlung überwiegt.

Dem Vermieter steht das Recht zu, Mietzahlungen von seinen Mietern für die Überlassung der Wohnung zu erhalten. Mit der Übermittlung der Kündigungsschreiben verfolgt der Vermieter insbesondere das Ziel, seine Mieteinnahmen zu sichern. Bei einem Verzicht auf die Übersendung des Kündigungsschreibens an die Fachstellen für Wohnungsnotfälle steht dem Vermieter zur Durchsetzung seiner Rechte nur die Möglichkeit offen, Räumungsklage einzureichen, sofern die Mieter auch nach dem Kündigungsschreiben ihre Mietrückstände nicht umgehend begleichen. Die zuständigen Amtsgerichte informieren dann die Fachstellen für Wohnungsnotfälle entsprechend der Anordnung über Mitteilungen in Zivilsachen über eingegangene Klagen wegen Zahlungsverzugs.

Wir haben vor diesem Hintergrund das berechtigte Interesse des Vermieters, seine Mieteinnahmen zu sichern, anerkannt und die Erforderlichkeit der Übermittlung der

Kündigungsschreiben an die Fachstellen für Wohnungsfälle bejaht. Anhaltspunkte für ein Überwiegen der schutzwürdigen Interessen der betroffenen Mieter liegen in der Regel ebenfalls nicht vor. Es ist sogar davon auszugehen, dass die Information der Fachstellen im Interesse der Mieter liegen wird, da hierdurch ggf. der Verlust der Wohnung verhindert werden kann. Weiterhin ist aus der Perspektive der betroffenen Mieter zu berücksichtigen, dass ihre Daten spätestens dann an die Fachstellen übermittelt werden, wenn eine Räumungsklage bei Gericht eingeht.

Mit Blick auf das informationelle Selbstbestimmungsrecht der betroffenen Mieter halten wir es aber für geboten, dass die Mieter in den Kündigungsschreiben über den beabsichtigten Versand des Kündigungsschreibens an die Fachstellen informiert werden und den Mietern eine Widerspruchsmöglichkeit gegen die Übersendung des Kündigungsschreibens eingeräumt wird.

Der betroffene Vermieter steht unserer zweiten Forderung, eine Widerspruchsfrist einzuräumen, kritisch gegenüber. Eine solche Frist würde nach der Argumentation des Vermieters dazu führen, dass mit hoher Wahrscheinlichkeit weitere Rückstände auflaufen und sich hiermit die Möglichkeiten der Fachstellen reduzieren würden, im Sinne der Mieter wohnungssichernd tätig zu werden. Wir werden uns mit dieser Argumentation auseinandersetzen und über den Fortgang berichten.

10. Werbung

10.1 Der große E-Mail-Verteiler

Der für alle Empfänger offene E-Mail-Verteiler kann teuer werden.

Einer der wichtigsten und meistgenutzten Dienste im Internet ist heute ohne Zweifel die elektronische Post, kurz „E-Mail" genannt. Schnell und bequem ist eine E-Mail verfasst, dann noch schnell die Empfänger hinzufügen, ein Klick, und schon hat die Nachricht ihre Empfänger erreicht. Woran viele nicht denken: Auch bei E-Mails kann der Datenschutz verletzt werden. Das kann dann der Fall sein, wenn eine E-Mail an mehrere Empfänger versandt wird und die Liste der Empfänger für jeden sichtbar ist. Sofern nicht nur Funktionspostfachnamen wie beispielsweise info@..., service@..., poststelle@... oder ähnliche Adressen genutzt werden, handelt es sich datenschutzrechtlich um eine unbefugte Datenübermittlung, soweit nicht alle Betroffenen in die Preisgabe ihrer E-Mail-Adresse eingewilligt haben. Die E-Mail-Adressen, die Vor-, zumindest aber Nachnamen enthalten, sind personenbezogene Daten im Sinne des Datenschutzrechts.

Im Sommer 2013 hat das Bayerische Landesamt für Datenschutzaufsicht ein Bußgeld

gegen eine E-Mail-Absenderin verhängt, weil der umfangreiche E-Mail-Verteiler für alle Empfänger sichtbar war, ohne dass Einwilligungen vorlagen oder eine gesetzliche Grundlage gegeben war (http://www.lda.bayern.de/lda/datenschutzaufsicht/p_archiv/2013/pm004.html).
Auch bei der hamburgischen Aufsichtsbehörde beschweren sich oft Empfänger von Mails mit demselben Hintergrund. Wir prüfen ebenfalls regelmäßig, ob fahrlässig unbefugt personenbezogene Daten übermittelt wurden und ein Ordnungswidrigkeitentatbestand nach § 43 Abs. 2 Nr. 1 BDSG vorliegt.

Ein derartiger Verstoß kann sehr schnell und fahrlässig geschehen, wenn man die E-Mail-Adressen in das „AN-Feld" oder das „CC-Feld" einträgt und nicht in das „BCC-Feld". Bei Eintragung der E-Mail-Adressen in das „AN-Feld" oder das „CC-Feld" sehen sowohl die unmittelbaren Empfänger („AN-Feld") als auch die Empfänger der Kopien („CC-Feld") dieser Mail, an wen die Mail sonst noch geschickt wurde. Nur bei Eintragung der E-Mail-Adressen in das „BCC-Feld" (englisch: Blind Carbon Copy, dt. sinngemäß: Blindkopie) wird die Übertragung der E-Mail-Adressen an die Empfänger unterdrückt, so dass nicht erkannt werden kann, an wen diese Mail sonst noch geschickt wurde.

Die Unternehmensleitungen müssen dafür Sorge tragen, dass entsprechende Anweisungen erteilt und befolgt werden.

10.2 Anwendungshinweise

Die meisten Auslegungsfragen bei der Verwendung personenbezogener Daten zu Werbezwecken werden nun beantwortet.

Der Düsseldorfer Kreis hat eine Ad-hoc-Arbeitsgruppe „Werbung und Adresshandel" unter Leitung des Bayerischen Landesamtes für Datenschutzaufsicht eingerichtet und diese mit der Erarbeitung von Anwendungshinweisen zu den BDSG-Regelungen für den werblichen Umgang mit personenbezogenen Daten beauftragt. In zwei Sitzungen und nachfolgendem schriftlichen Verfahren wurden Anwendungshinweise formuliert, die in diesem Dokument abgedruckt und als beschlossen anzusehen sind. Sie sind zu finden unter http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/Anwendungshinweise_Werbung.pdf.

11. Bußgeldfälle und Anordnungen

11.1 Übersicht

Das Verhängen von Bußgeldern ist nicht überflüssig geworden.

Im Vordergrund unserer aufsichtsbehördlichen Tätigkeit steht zwar nicht, Bußgelder zu verhängen. Dennoch musste die Aufsichtsbehörde wieder in 12 Fällen Datenschutzverstöße mit Bußgeldern ahnden:

Tatbestand § 43 Abs. 1 Nr.	Tatbestand § 43 Abs. 2 Nr.	Sachverhalt	Bußgeld in €	E = Einspruch N= kein Einspruch	Verfahrensausgang vor dem Amtsgericht
	1	unsachgemäße Entsorgung von 18 Aktenordnern durch Kindertagesstätte	300	E	gezahlt
	1	Übermittlung von Forderungsdaten an eine Auskunftei, obwohl die Forderung strittig war	2.500	E	gezahlt
2b		fehlende präzise Festlegung von Gegenstand und Dauer des Auftrags, klare Benennung der Datenarten und des Betroffenenkreises, Festlegung von technischen und organisatorischen Sicherheitsmaßnahmen und der jeweiligen Kontroll- und Weisungsrechte sowie Regelung zur Zulässigkeit von Unteraufträgen sowie erforderliche Schriftform.	7.500	N	gezahlt
10,2b	1	Ortung von Mietfahrzeugen ohne Information und Einwilligung der Mieter in folgenden Fällen: alle 48 Stunden regelmäßig, bei Verlassen der Freifahrtzone, bei Diebstahl und bei der Fahrt in ein Hafengebiet	54.000	N	gezahlt
1			250	N	
10			750	E	eingestellt
	1	Speicherung + Übermittlung von Bonitätsdaten im Rahmen Sammelbestellung	16.000	N	gezahlt
	1	Erhebung und Speicherung von WLAN Payload Daten	145.000	N	gezahlt
10			1.000	E	noch offen
3	5b	Adressdaten trotz bestätigtem Werbewiderspruch für weitere Werbezwecken genutzt	5.500	N	gezahlt
1		Übermittlung an Auskunftei trotz Bestreitens	400	N	
10		falsche Auskünfte	1.250	E	1.200*

*Reduzierung auf 1.200,00 durch Verwaltungsbehörde

Im Berichtszeitraum wurden keine Strafanträge gestellt.

Die Aufsichtsbehörde hat gegenüber drei Unternehmen Anordnungen nach § 38 Abs. 5 BDSG erlassen. Zwei Fälle betrafen Kundendaten, die im Internet öffentlich zugänglich waren, bedingt durch unzureichende technische und organisatorische Maßnahmen nach § 9 BDSG. Ein anderer Fall betraf ein Verfahren, das von Facebook betrieben wurde (vgl. V 7.1).

12. Meldepflicht und Prüftätigkeit

12.1 Bericht über durchgeführte Prüfungen

Selbstverantwortliches Datenschutzmanagement und die Kontrolle der Einhaltung der datenschutzrechtlichen Anforderungen bleiben im Focus der Aufsichtsbehörde für den Datenschutz.

Die im Jahr 2010 (vgl. 23 TB, IV 12.3) begonnene Fragebogenaktion bei Hamburger Unternehmen zum betrieblichen Datenschutzbeauftragten haben wir fortgesetzt. Befragt wurden 465 Apotheken mit folgenden Ergebnissen:

Gesamt	bestellt	keine Bestellpflicht	müssen noch bestellen
465	94	360	11

10 % sind damit der Bestellpflicht nicht nachgekommen. Dieses Ergebnis entspricht den Durchschnittswerten der Fragebogenaktion von 2010/2011. Eine Nachkontrolle bei 10 Apotheken ergab allerdings, dass die Einschätzung zur Bestellpflicht nicht immer den tatsächlichen Gegebenheiten entsprach und damit mehr Apotheken einen betrieblichen Datenschutzbeauftragten bestellen mussten.

Neben dieser Fragebogenaktion bleiben auch weiterhin Vor-Ort-Prüfungen ein Baustein der staatlichen Kontrolle. Ausgelöst oftmals durch einzelne Beschwerden, nahmen wir diese zum Anlass, den Prüfungsgegenstand zu erweitern. Die der Prüfung zugrunde liegenden Eingaben betrafen überwiegend die Beschäftigtendatenverarbeitung, die Kontrolle erstreckte sich dabei zusätzlich auf folgende Themen:

- Technische und organisatorische Maßnahmen nach § 9 BDSG
- Übersicht über Verfahren automatisierter Verarbeitungen nach § 4 g Abs. 2 BDSG
- Auftragsdatenverarbeitung
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten und seine Fachkunde
- Verpflichtung auf das Datengeheimnis
- Meldepflicht

Die dabei festgestellten Defizite der 5 geprüften Unternehmen aus den Branchen Callcenter, Software-Beratung, Industrie, gewerbliche Dienstleistungen und Adresshandel sind nachstehend zusammengefasst:

Besonders auffallend ist, dass in 3 Fällen die vorgelegten Übersichten über Verfahren automatisierter Verarbeitungen (Verfahrensverzeichnis) nicht den Anforderungen entsprachen. Ebenso hat die vertiefte Prüfung der Auftragsdatenverarbeitung bei 3 Unternehmen erhebliche Defizite ergeben. Aufträge, die bereits vor September 2009 erteilt wurden, waren nicht den neuen Regelungen angepasst worden, ein Konzept zur Kontrolle der Auftragnehmer war ebenfalls nicht vorhanden.

Wenn wir bei Kontrollen feststellen, dass der Auftraggeber einen Auftragsdatenverarbeitungsvertrag nicht abgeschlossen hat bzw. dieser Vertrag nicht die erforderlichen Mindestvertragsbestandteile enthält, können wir ein Bußgeld von bis zu 50.000 Euro verhängen (vgl. III, 5.1). Unternehmen sollten die von ihnen abgeschlossenen Verträge daher daraufhin prüfen, ob die gesetzlichen Mindestvertragsbestandteile für eine Auftragsdatenverarbeitung schriftlich festgelegt worden sind. Dies gilt auch für Verträge, die vor September 2009 geschlossen wurden (vgl. 22. TB, IV 11.2). Aufgrund der Verringerung des Personalbestands wird im nächsten Berichtszeitraum mit einem Rückgang der Vor-Ort-Prüfungen zu rechnen sein.

12.2 Meldepflicht nach § 42a BDSG

Die hohe Zahl der angezeigten Datenpannen lassen oftmals auf Mängel in den organisatorischen Abläufen schließen.

Im Berichtszeitraum erreichten uns wieder zahlreiche Meldungen über Datenschutzvorfälle. Die Unsicherheiten, wann ein Ereignis der Aufsichtsbehörde zu melden ist, sind allerdings nicht geringer geworden (vgl. 23. TB, IV 12.1). Die Unternehmen haben erheblich mehr Fälle angezeigt, als tatsächlich nach einer Beurteilung des Sachverhaltes zu melden gewesen wären. Dennoch ist festzuhalten, dass vielfach Mängel bei den Geschäftsprozessen offenbar wurden.

70 Meldungen sind im Berichtszeitraum eingegangen. Spitzenreiter bei den Anzeigen ist der Versand von Briefen an falsche Empfänger. Die nachstehende Übersicht stellt die wichtigsten Sachverhalte dar:

Oftmals wurde die Meldepflicht allerdings verneint, da die Kriterien dafür nicht vorlagen. Zu den Voraussetzungen gehören:

- Wenn bei der nicht-öffentlichen Stelle gespeicherte
  - besondere Arten personenbezogener Daten (rassische, ethnische Herkunft; politische Meinungen; religiöse, philosophische Überzeugungen; Gewerkschaftszugehörigkeit; Gesundheit; Sexualleben),
  - personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
  - personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten beziehen,

- personenbezogene Daten zu Bank- oder Kreditkartenkonten
- unrechtmäßig übermittelt oder
- auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind

und

dadurch schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen.

Selbst wenn eine der Datenkategorien betroffen ist, sind drohende schwerwiegende Beeinträchtigungen aufgrund der Umstände des Einzelfalles oftmals zu verneinen. Dennoch ist eine Meldung im Zweifel für die verantwortliche Stelle der sichere Weg, mit der Meldepflicht umzugehen.

Eine weitere Übersicht über gemeldete Datenpannen findet sich in der Bundestags-Drucksache 17/12319. Daraus ergibt sich, dass Hamburg bei den Meldungen von Vorgängen nach § 42a BDSG im Vergleich der Bundesländer nach Nordrhein-Westfalen und Bayern an dritter Stelle liegt.

12.3 Register

Die Zahl der Meldungen hat sich kaum verändert.

Die Aufsichtsbehörde führt nach § 38 Abs. 2 BDSG ein Register der Stellen, die nach § 4d BDSG der Meldepflicht unterliegen.
§ 4d Abs. 4 BDSG:
Meldepflicht gilt für automatisierte Verarbeitungen, in denen geschäftsmäßig personenbezogene Daten von der jeweiligen Stelle

1. zum Zweck der Übermittlung,

2. zum Zweck der anonymisierten Übermittlung oder

3. für Zwecke der Markt- oder Meinungsforschung gespeichert werden.

52 Unternehmen sind entsprechend den Vorgaben des § 4e BDSG zum Register gemeldet (vgl. 18. TB, 29.1, 19. TB, 27.1, 20. TB 30.1, 21. TB, 30.1, 22. TB 11.1, 23. TB, 12.2). Unterteilt nach der Art der meldepflichtigen Verfahren ergibt sich folgendes Bild:

- Speicherung zum Zwecke der Übermittlung
  Auskunfteien/Warndienste 11
  Informationsdienste 4
  Adresshändler 10
- Speicherung zum Zwecke der anonymisierten Übermittlung oder für Zwecke der Markt- und Meinungsforschung 27

INFORMATIONEN ZUR DIENSTSTELLE VII.

1. Eingabenstatistik 256
2. Presse- und Öffentlichkeitsarbeit beim HmbBfDI 257
3. Aufgabenverteilung 260

1. Eingabenstatistik

Als Eingabe werden beim HmbBFDI die schriftlichen Beschwerden von Bürgerinnen und Bürgern bezeichnet, die sich auf Grundlage des Hamburgischen Datenschutzgesetzes (HmbDSG) oder des Bundesdatenschutzgesetzes (BDSG) an uns wenden, weil sie der Meinung sind, dass öffentliche oder nicht-öffentliche Stellen ihr Recht auf informationelle Selbstbestimmung verletzt haben. Diese Eingaben sind zu einem großen Teil die Basis der datenschutzrechtlichen Überwachung der Hamburger Behörden und Einrichtungen und der Aufsicht über die in Hamburg ansässigen Unternehmen, da oft erst durch die Eingabe umfangreiche Kontrollen und Prüfungen initiiert werden.

Branche/Bereich	2012	2013
Adresshandel	6	12
Auskunfteien	52	64
freie Berufe	21	20
Gastronomie	4	10
Gewerbliche Dienstleistungen	92	73
Heime	0	1
Inkassounternehmen	2	25
Krankenhäuser	22	7
Kreditwirtschaft	2	50
Markt- und Meinungsforschung	34	4
Öffentlicher Nahverkehr	4	5
sonst. Handel und Industrie	5	67
sonst. Verkehrswesen	67	22
sonst. Gesundheitswesen n.-ö.	7	34
sonst. Soziales n.-ö.	35	10
Tele- und Mediendienste	7	153
Telekommunikation	242	36
Vereine und Parteien	32	24
Verlage	16	16
Versandhandel	18	17
Versicherungswirtschaft	25	20
Wohnungswirtschaft	22	38
Sonstiges nicht-öffentl.	27	77
allgem. Bezirksangelegenheit	84	7
andere Sozialbereiche	2	2
Arbeitslosengeld II	12	14
Ausländerwesen	6	3
Bau- und Vermessungswesen	4	4
Bildungswesen	15	19
Feuerwehr	1	1
Gesundheitswesen öffentl.	11	11
Hochschulwesen	5	9
Justiz	0	13
Kinder- und Jugendhilfe	6	7
Kultur	5	0
Medizinischer Dienst der KV MDK	3	1
Parlamentswesen/Bezirksvers.	1	1
Pass- und Meldewesen	21	9
Personenstandswesen	3	1
Polizei	21	20
Sozialhilfe	3	3
Sozialversicherung	10	14
Staatsanwaltschaft	5	2
Statistik	7	2
Steuern und Abgaben	2	5
Strafvollzug	4	4
Umweltschutz	0	1
Verfassungsschutz	4	2
Verkehrswesen öffentl.	6	8
Wahlen und Volksabstimmung	1	2
Wirtschaftsverwaltung	4	6
Sonstiges öffentlich	7	16
Abgaben	103	75
Gesamt:	**1098**	**1047**

Tabelle 1: Eingabe nach Branchen

Im Vergleich zum Berichtszeitraum des 23. Tätigkeitsberichtes (2010/2011) sind die Eingabenzahlen beim HmbBfDI gesunken, was aber insbesondere auf die ungewöhnlichen Umstände der Jahre 2010 und 2011 zurückzuführen ist. Damals war der HmbBfDI die zentrale Anlaufstelle für Bürgerinnen und Bürger aus dem gesamten Bundesgebiet, die sich über den Dienst Google Street View beschwert haben (vgl. I 3.1). Insgesamt haben sich die Eingaben in den vergangenen Jahren auf einem hohen Niveau eingependelt, wie der 10-Jahres-Vergleich zeigt:

Abbildung 1: Entwicklung der Eingaben 2004 - 2013

2. Presse- und Öffentlichkeitsarbeit beim HmbBfDI

Durch das mediale Interesse an datenschutzrechtlichen Themen sind die Anfragen nationaler und internationaler Pressevertreter beim HmbBfDI stark angestiegen. Die qualitativ und quantitativ hohen Anforderungen der Presse- und Öffentlichkeitsarbeit binden weiteres Personal.

Ob Vorratsdatenspeicherung, Videoüberwachung, Soziale Netzwerke oder PRISM, datenschutzrechtliche Themen sind in aller Munde und bewegen die Öffentlichkeit. Indikatoren für diese Entwicklung sind nicht nur die vielfältigen Eingaben von Bürgerinnen und Bürgern beim HmbBfDI, sondern vor allem auch das gesteigerte Interesse der Medien an datenschutzrechtlichen Themen aller Art. Es vergeht kaum ein Tag, an dem der Schutz der persönlichen Daten nicht in den Nachrichten, in den Zeitungen oder den Zeitschriften auftaucht. Dabei steht der Medienstandort Hamburg, nicht

zuletzt auch wegen der deutschen Dependancen von Google und Facebook besonders im Fokus der nationalen und internationalen Presse. Vor diesem Hintergrund ist die Pressearbeit beim HmbBfDI, die in erster Linie durch Anfragen der Medien von außen gesteuert wird, zu einem eigenständigen Arbeitsbereich geworden, der nicht mehr nur „nebenbei" erledigt werden konnte.
Als Reaktion darauf wurde im November 2011 ein Referent für Presse- und Öffentlichkeitsarbeit beim HmbBfDI installiert. Dieser Mitarbeiter ist erster Ansprechpartner für die Presse, er koordiniert die eingehenden Presseanfragen und beantwortet sie teilweise in eigener Verantwortung. Allerdings musste für dieses neue Aufgabengebiet ein Mitarbeiter aus dem operativen Bereich des HmbBfDI abgezogen werden, denn eine solche Stelle ist im Stellenplan des HmbBfDI weder vorgesehen, noch war die Neuschaffung einer Stelle möglich. Diese Neuorganisation führte daher zwangsläufig zu einer erhöhten Belastung der weiteren Mitarbeiter und Mitarbeiterinnen, die aber durch eine deutliche Entlastung der gesamten Dienststelle im Bereich der Pressearbeit und durch weitere organisatorische Maßnahmen weitgehend ausgeglichen werden konnte. Nach über zwei Jahren Erfahrung mit diesem Dienstposten muss festgestellt werden, dass sich diese Maßnahme insgesamt bewährt hat, wobei ein Blick auf die Zahlen des Berichtszeitraums die Notwendigkeit dieser Organisationsmaßnahme nochmals anschaulich macht:

Statistisch betrachtet ging an jedem Arbeitstag des Berichtszeitraums 2012/2013 mindestens eine Presseanfrage bei uns ein. Dabei handelte es sich um Anfragen der regionalen Presse, aber auch im hohen Maße um Anfragen überregionaler und auch internationaler Medien.

Tabelle 1: Presseanfragen beim HmbBfDI

Presseanfragen...	2012	2013	Gesamt
regionaler Medien:	88	80	168
überregionaler Medien:	191	131	322
ausländischer Medien:	24	35	59
Gesamt:	303	246	549

Die verhältnismäßig hohe Anzahl von Anfragen ausländischer Medien ist nicht zuletzt auf die international agierenden Konzerne Google und Facebook zurückzuführen, die mit ihrer jeweiligen Deutschlandvertretung in Hamburg ansässig sind. So bezogen sich rund 41% aller Presseanfragen auf Themen, die in verschiedenen Ausprägungen im Zusammenhang mit diesen beiden Unternehmen standen (Facebook: 127; Google: 96). Auch unsere Teilnahme an der sogenannten Google Task Force (vgl. V 6.1), einer Kooperation europäischer Datenschutzbeauftragter, hat zu vermehrten Rückfragen durch überregionale und internationale Medien geführt.

Während einige der Anfragen durch kurze Auskünfte, Informationen und ergänzende

Angaben beantwortet werden konnten, erforderten andere umfangreiche Prüfungen und Recherchen. Gelegentlich wurden durch die Presseanfragen auch datenschutzrechtliche Prüfungen bei den verantwortlichen Stellen initiiert. Hinzu kamen diverse Interviewanfragen an den Hamburgischen Datenschutzbeauftragten und seine Mitarbeiter und Mitarbeiterinnen von verschiedenen Medien.

Tabelle 2: Presseanfragen nach Medienart

Medienart	2012	2013	Gesamt
Print	120	94	214
Hörfunk	67	41	108
Fernsehen	48	53	101
Online	36	26	62
Agenturen	26	27	53
Sonstiges	6	5	11

Neben der Beantwortung von Presseanfragen, die eine rein reaktive Tätigkeit ist, weil nur auf die Anfrage von außen reagiert wird, wird beim HmbBfDI, wenn auch in weit geringerem Ausmaß, auch eine aktive Pressearbeit betrieben. So wurden vom HmbBfDI im Berichtszeitraum insgesamt 20 Pressemitteilungen veröffentlicht (2012: 13; 2013: 7). Pressekonferenzen wurden dagegen im Berichtszeitraum nicht abgehalten.

Unsere Öffentlichkeitsarbeit ist aus personellen und finanziellen Gründen nur sehr eingeschränkt möglich. Veröffentlichungen stehen zum größten Teil nur als Downloadangebote zur Verfügung oder werden, wenn möglich, in Kooperation mit anderen Behörden oder Institutionen verlegt.

Tabelle 3: Druckerzeugnisse des HmbBfDI 2012/2013

Titel	Erscheinungsjahr	Auflage
Tätigkeitsbericht 2010/2011	2012	1.300
Datenschutz: Fakten - Zahlen - Daten	2012	1.300
Meine Daten kriegt ihr nicht: Unterrichtseinheit Datenschutz (2. Auflage)	2012	500
„selbst & bewusst" – Tipps für den persönlichen Datenschutz bei Facebook	2013	6.000*
Datenerhebung bei der Vermietung von Wohnraum	2013	500
Hamburgisches Datenschutzgesetz – Gesetzestext und Erläuterungen	2013	2.500

* in Kooperation mit dem Schulinformationszentrum der BSB

Weiterer Bestandteil der Öffentlichkeitsarbeit ist die gelegentliche Teilnahme an oder die Ausrichtung von Informationsveranstaltungen. Neben unserer alljährlichen Teilnahme an der „Dataport Hausmesse" seien dabei insbesondere die Veranstaltungen im Rahmen des Projekts „Meine Daten kriegt ihr nicht!" genannt, die in Kooperation mit dem Landesinstitut für Lehrerbildung und Schulentwicklung in Hamburger Schulen stattgefunden haben (vgl. III 7.4). Daneben wurden in der Rudolf-Steiner-Schule Hamburg-Wandsbek (Januar 2013) und in der Verwaltungsschule Hamburg (Mai 2013) auch Veranstaltungen für Schülerinnen und Schüler bzw. Auszubildende der Stadt Hamburg durchgeführt. Der Hamburgische Datenschutzbeauftragte selbst, aber auch einige seiner Mitarbeiter, haben außerdem im Berichtszeitraum an diversen Diskussions- und Vortragsveranstaltungen im In- und Ausland teilgenommen und dabei über datenschutzrechtliche Themen referiert.

3. Aufgabenverteilung

Nach der Umstrukturierung der Dienststelle ergibt sich seit 1. Januar 2014 folgende neue Aufgabenverteilung (siehe dazu I. 3.5):

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Klosterwall 6
20095 Hamburg

Tel.: 040/42854-4040
Fax: 040/42841-4000
E-Mail: mailbox@datenschutz.hamburg.de
Internet-Adresse: www.datenschutz-hamburg.de

Telefonliste:		**040/42854- Durchwahl**
Dienststellenleiter:	Prof. Dr. Johannes Caspar	-4040
Stellvertreter:	[redacted]	-4049
Vorzimmer:		-4040
Verwaltungsleiter, Presse- und Medienreferent		
[redacted]		-4153
Haushalt und Personalwesen		
[redacted]		-4043
Vorzimmer, Geschäftsstelle:	[redacted]	-4040
Registratur, Geschäftsstelle:		-4042

Öffentlichkeitsarbeit -4142
[redacted]

IT-Leitung, Internetangebot des HmbBfDI, Öffentlichkeitsarbeit -4044
[redacted]

Übergreifende Infrastrukturprojekte, Ubiquitous Computing (RFID), technisch-organisatorische Beratung und Prüfung -4053
[redacted]

Technisch-organisatorische Beratung und Prüfung -4055
[redacted]

Netzwerke und mobile Geräte, technisch-organisatorische Beratung und Prüfung -4048
[redacted]

Informationsfreiheit/Transparenz und Videoüberwachung -4047 -4141
[redacted]

Grundsatzfragen des HmbDSG, Sicherheit und Justiz, Waffenrecht, Ausländerwesen, Forschung, Friedhöfe -4049
[redacted]

Verkehr, Wirtschaftsverwaltung, Bezirks- und Parlamentsangelegenheiten, Hochschulwesen, behördliche Datenschutzbeauftragte -4064
[redacted]

Gesundheitswesen und medizinische Forschung, Sozialwesen, Schule und Bildungswesen -4062
[redacted]

Meldewesen, Pass- und Ausweisangelegenheiten, Personenstandswesen, Statistik, Archivwesen -4046
[redacted]

Grundsatzfragen des BDSG, Grundsatzfragen Internationales, Auskunfteien, gewerbliche Dienstleistungen -4058
[redacted]

Beschäftigtendatenschutz, Bauen und Wohnen, Vereine und Gewerkschaften -4060
[redacted]

Finanz-, Steuer- und Rechnungswesen, Handel und Industrie, Geodaten
[redacted] -4052

Versicherungen, Kreditwirtschaft, Versand- und Onlinehandel, Werbung- und Adresshandel, Markt- und Meinungsforschung
[redacted] -4059

Technische Grundsatzfragen der Medien, Telemedien, Telekommunikation und E-Government, Netzwerke, Biometrie
[redacted] -4054

Juristische Grundsatzfragen der Medien, Telemedien, Telekommunikation und E-Government, elektronischer Rechtsverkehr, Kultur
[redacted] -4051

Beratung und Prüfung der Medien, Telemedien, Telekommunikation und E-Government, Technik der Videoüberwachung
[redacted] -4061

VII.

A

Abgabenordnung III 10.3
Abrufverfahren VI 4.2
Abschleppleistungen III 1.8
Adresshandel VI 10.2
Amt für Medien I 3.2
Android II 9, II 8, II 2
Anonymisierung III 16.1.3
Anordnungen nach § 38 Abs. 5 BDSG VI 11.1
Antiterrordatei III 2.2
Anwerbung von V-Leuten III 2.3
Apps II 9, II 8
Arbeitskreis Beschäftigtendatenschutz IV 1
Arztbriefe III 5.13
Arztpraxis III 5.12
Asklepios-Klinik III 5.2, III 5.1
Attrappen VI 8.2
Aufenthaltsgesetz III 3.1
Auftragsdatenverarbeitung VI 12.1, V 9, IV 2, III 10.3, III 5.1
Auskunftei VI 4.2
Auskunfteien VI 6
Auskunftserteilung III 3.2
Auskunftspflicht III 13.1, III 10.1
Ausländer III 3.1
Ausländervereine III 1.6
Ausspähung I 2
Automatisierung der Vollstreckungsaufgaben III 10.3

B

Babylotse III 6.1
Beanstandung III 6.5, III 5.3
Behandlungsvertrag III 5.2
Behörde für Arbeit, Soziales, Familie und Integration III 6.2
Behörde für Schule und Berufsbildung III 7.5
Behördliche Datenschutzbeauftragte III 11.1
Beobachtung III 12.3
Berechtigte Interessen III 16.1.3, III 16.1.2, III 16.1.1
Berufsbildungsmaßnahmen III 7.10
Beschäftigtendatenschutzgesetz IV 4

Bestandsdatenabfrage III 1.2
Betreuungsbehörde III 6.4, III 5.4
Betriebliche Datenschutzbeauftragte VI 12.1, VI 1.1
Bettensteuer III 10.1
Bewährungshelfer III 4.1
Bezirksämter III 20.1
Bezirksversammlung III 16.2, III 16.1.3, III 16.1.2, III 16.1.1
Bezirksverwaltungsgesetz III 16.2, III 16.1
Bildungs- und Betreuungsangebote an Schulen III 7.7
Biometrie V 7.1, III 7.8
BlackBerry II 2
Bonitätsabfrage VI 4.1
Bonitätsprüfung III 5.6
Briefwahlunterlagen III 15.2
Bundeskinderschutzgesetz III 6.1
Bundesmeldegesetz III 19.1
Bußgelder VI 11.1, 8.3, III 5.1
BYOD II 2

C

Content Delivery Network V 8
Cookies V 3
Einwilligung V 2
E-Privacy Richtlinie V 2

D

Data Center Steuern (DCS) III 10.3
Dataport II 1.
Daten verarbeitende Stelle III 7.1
Datenabgleich VI 5.1
Datengeheimnis III 16.1.2, III 16.1.1
Datenpannen VI 12.2
Datenschutz-Grundverordnung VI 1
Datenschutzkompetenz I 2
Datenschutzkonferenz I 2
Datenschutzmanagement VI 12.1
Datenschutzvorfälle VI 12.2
Dating-Portal V 9
Deutschland online KFZ III 12.1
Diskretionsabstand III 6.3

DME Excitor II 2
Dritterhebung III 6.4

E

eCampus-IDMS III 13.2
Eingaben III 16.1.1, III 4.2, I 3.1
Einwilligung VI 9.3, VI 9.2, III 7.10, III 5.6, III 5.2
Elektronisches Personenstandsregister III 18.1
Elternabend III 7.13
E-Mail Adressen V 9
E-Mail-Verteiler VI 10.1
Ende-zu-Ende-Verschlüsselung II 4.
Entsorgung III 5.1
ePass III 20.1
Erhebungswille III 12.3
EU-Datenschutz-Grundverordnung VI 1, IV 4, I 1
EU-Richtlinie Strafverfolgung VI 1.1

F

Facebook
- Anwendbares Recht V 7
- Biometrie V 7.1
- Datenschutzrechtliche Verantwortung V 7
- Social Plugins V 7.2
- Tagging V 7.1

Fahrkarten VI 7.3
Faktisch anonyme Daten III 7.11
Faxen III 5.13
Finanzbehörde II 4., II 3.
Fingerabdruck III 20.1
Forschungsprojekte III 8.1
Forschungszweck III 8.1
Fragerecht des Vermieters VI 9.1
Freunde-Finder Verfahren V 9
Frühe Hilfen III 6.1
Funkzellenabfragen III 1.7
Fußballstadien III 1.4

G

GBS/GTS-Gebühren III 7.7
Geburtsdaten III 5.11
Geldkarte VI 3.1
Gemeinsame Datei III 7.10, III 7.6, III 5.12, III 5.9
Generalregister der Hamburgischen Standesämter III 18.2
Georeferenzierung III 12.4
Gesichtserkennung V 7.1
Gesundheitsamt III 5.11
Google II 9, II 8, II 6
Bußgeld V 6.2
Datenschutzbestimmungen V 6.1
Information V 6.1
Nutzungsbedingungen V 6.1
Profilbildung V 6.1
Speicherfristen V 6.1
Sucheinträge V 6.4
WLAN Scanning V 6.2
GPS-Ortung VI 7.1
Graph Search V 7.3
GRfW III 10.2

H

Hafen- und Schifffahrtsgesetz III 12.5
Hamburg Port Authority III 12.5
Hamburger Hochbahn AG VI 7.3
Hamburger Medienpass III 7.4
Handyparken III 12.2
Hans-Bredow-Institut I 3.2
Hausfassaden III 12.4
Hausrecht III 1.3
HbbTV II 6
Hochschulgesetz III 13.2, III 13.1
Hochschulübergreifendes Identitätsmanagementsystem III 13.2
Hotelier als Steuerschuldner III 10.1

I

Internationaler Datenverkehr VI 2
IServ III 7.3

J

Jagdgenossenschaft III 14.1
Jugendämter III 6.2
Jugendberufsagentur III 7.5
Jugendhilfe III 6.2
JUS-IT III 6.2

K

Kleine Anfrage III 16.1.3
Klinisches Krebsregister III 5.8
Koalitionsvertrag IV 4
Kommunale Mandatsträger V 10
KoPers/ePers IV 3
Körperschaften des öffentlichen Rechts III 14.1
Korruptionsregister III 10.2
Kraftfahrtversicherung VI 4.2
Krankenversicherung VI 4.1
Kreditkarten VI 3.1
kreditorisches Risiko VI 4.1
Kultur- und Tourismustaxe III 10.1
Kundenkarte VI 5.3

L

Landesbetrieb Straßen, Brücken und Gewässer III 12.4
Landesbetrieb Verkehr III 12.1
Landesinformationssystem III 17.2
Langzeituntersuchungen III 7.1
Live-Streaming III 16.2
Löschungsbegehren III 1.5
Luftbildaufnahmen III 9.1

M

Mandantenfähigkeit III 18.1, III 6.2, II 1.
Mandantentrennung III 6.5, III 5.12
MDK-Gutachten III 5.5
MDM II 2
Medienkompetenz III 7.4, III 7.2
Medizinischer Dienst der Krankenkassen (MDK) III 5.5
Meldedatenübermittlungsverordnung III 5.11
Meldepflicht VI 12.3
Meldepflicht nach § 42a BDSG VI 12.2

Melderegisterauskünfte III 19.1
MESTA III 3.2, III 3.1
Mietinteressenten VI 9.1
Minderjährige VI 5.3
Mitarbeiterbefragung III 7.12
Mitarbeiterdatenschutz III 7.12
Mittagessen III 7.8
Mitteilungen in Strafsachen (MiStra) III 3.1
Mobilfunkgeräte III 2.1

N

Nachrichtendienstliche Mittel III 2.1
Near Field Communication VI 3.1
NGN II 5
NSA I
Nutzerprofil V 3

O

Obachtverfahren III 6.2
Öffentliche Toiletten III 16.3
Öffentlicher Gesundheitsdienst III 6.1
One-Stop-Shop I 1
Online-Übertragungen III 16.2
Ordnungswidrigkeit VI 4.1, III 5.1
Orientierungshilfe II 1.
Orthofotos III 9.1
Ortung III 2.1
Ortungsdaten VI 7.1

P

Panoramaaufnahmen III 9.2
Patientendaten im Internet III 5.10
Penetrationstest II 3., II 2
Personalaktendaten IV 2
Personalausweis III 20.1
Personalausweiskopien III 20.2
Personalengpässe I 3.4
Personendatensatz III 13.2
Pixel III 9.1

Polizei III 6.2, III 1.5
Fanpage V 5
Polizeikommissariat III 1.3
Präventiv-Beratung I 3.2
Presse III 4.2
Prism I 2, V 12
Privacy by Default I 1
Privacy by Design I 1
PROJUGA III 6.5
PROSA III 6.5
Protokollierung III 13.2, III 7.9, III 1.1
Pseudonym V 3
Psychiatrie III 5.4

R

Recht auf Vergessenwerden I 1
Rechtliches Gehör III 1.8
Reichweitenmessung V 6.3
Reidentifizierung III 16.1.3
Reisepass III 20.1
Richtervorbehalt III 1.2
Routing V 8

S

Safe Harbor VI 2. 2.1.1
Safe-Harbor-Abkommen VI 2.2
Sanktionen V 6.2
Schiffsverkehr III 12.5
Schufa VI 4.1
Schulinspektion III 7.12
Schulkonflikte III 7.13
Schulstatistik III 7.1
Schwere Verfehlung III 10.2
Scorewert VI 6. 6.4
Secure Service Level Agreement (SSLA) III 10.3
Sicherheitsüberprüfung III 1.8
Sicherungsverwahrung III 4.1
Smart-TV II 6
Snowden I
Social Plugins
Einwilligung V 7.2
Reichweitenanalyse V 7.2

Soziale Netzwerke III 7.2
Soziale Netzwerke
Fanpage V 5
Öffentliche Stellen V 4
Orientierungshilfe V 1
Polizei V 5
Soziales Dienstleistungszentrum III 6.3
Sozialhilfe III 6.2
Spielbank Hamburg III10.4
Staatsanwaltschaft III 4.2, III 3.2, III 3.1
Staatsarchiv III 18.2
Standardvertragsklauseln VI 2. 2.2
Standesamt III 5.11
Statistik III 17.1
Statistikamt III 17.2
Steuerverwaltung III 10.3
Stichprobenkontrolle III 1.1
Stichprobenverfahren VI 6. 6.1
Straßenaufnahmen III 9.2
Straßenunterhaltung III 12.4
Studienabbruch III 13.1

T

Telekommunikationsgeheimnis I 2
Tempora I 2
Tierhalterregister III 5.9
Tracking V 6.3
Transparenzgesetz I 3.4

U

Übersichtsaufnahmen III 12.3
UKE III 5.10, III 5.3
Umstrukturierung I 3.5
Unfallkameras VI 8.2
Unternehmensregelungen VI 2. 2.1.3
Unterrichtsmaterial III 7.4
User contact III 5.3

V

Verarbeitung von Gesundheitsdaten VI 4.3

Verfahrenskataster Polizei	II 7
Verfahrensverzeichnis	VI 12.1
Vergabe öffentlicher Aufträge	III 10.2
Verhaltensregeln	VI 4.4
Verkehrsleitung	III 12.3
Verkehrsleitzentrale	III 12.3
Verkehrslenkung	III 12.3
Vermieter	VI 9.1
Veröffentlichung	III 16.1.3, III 16.1.1
Veröffentlichung im Internet	VI 9.2
Verpixelung	III 12.4
Versandhändler	VI 5.1
Verschlüsselung	II 4,
Versichererwechselbescheinigung	VI 4.2
Verwaltungsabkommen	III 10.2
Videoaufzeichnung	III 7.12
Videoüberwachung	VI 8.3, VI 8.2, VI 8.1, III 16.3, III 14.1, III 12.5, III 12.3, III 10.4, III 5.4, III 4.1, III 1.4, III 1.3
V-Leute	III 2.3
Voice over IP	II 5
Volksabstimmungen	III 15.1
Volksabstimmungsgesetz	III 15.1
Volksabstimmungsverordnung	III 15.1
Volkszählung	III 17.1
Volkszählungsurteil	I 2
Vollstreckungsdienststellen	III 10.3
Vorabkontrolle	III 16.2
VoSystem	III 10.3

W

Wahlfreiheit	III 5.2
Warndatei	VI 5.1
Wartebereich	III 6.3
Werbung	VI 10.2
Widerspruchsrecht	III 5.8
Wildbeobachtungskameras	III 14.1
Wissenschaftliche Forschung	III 14.1
Wohngeld	III 6.2

X

Xing V 8
X-Keyscore I 2

Z

Zahnärzte III 5.6
Zensus 2011 III 17.1
Zentrale Informationsstelle III 10.2
Zentrales Schülerregister III 7.9
Zugangssicherungscodes III 1.2
Zugriffsberechtigung III 1.1
Zugriffsprotokolle III 5.3
Zur Veröffentlichung bestimmt III 16.2
Zuvex II 3.
Zwei-Faktor-Authentisierung II 3.

Herausgeber:
Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Klosterwall 6
20095 Hamburg
Tel.: 040/42854-4040 (Geschäftsstelle)
Fax: 040/42854-4000
E-Mail: mailbox@datenschutz.hamburg.de

Titelbild, Fotos [redacted]
Layout: Kameko Design GbR
Druck: Lütcke & Wulff, Hamburg