DATENSCHUTZ
TÄTIGKEITSBERICHT
2014/2015

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

HmbBfDI

Hamburg

25. Tätigkeitsbericht Datenschutz

des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit
2014 / 2015

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

vorgelegt im Februar 2016
Prof. Dr. Johannes Caspar
(Redaktionsschluss: 31. Dezember 2015)

Auflage: 1.200 Exemplare
Layout: Kameko Design, Inga Below, Fotos: Axel Caro, Druck: print 74

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

INHALTSVERZEICHNIS

VORWORT 8

I. DATENSCHUTZ IM UMBRUCH – DEFIZITE, NEUE HERAUSFORDERUNGEN, LÖSUNGSANSÄTZE

1. Einleitung 12
2. Rechtliche Stärkung der Unabhängigkeit des HmbBfDI – Bestandsaufnahme und Vorschläge 13
   - 2.1 Der Begriff der völligen Unabhängigkeit 14
   - 2.2 Vereinbarkeit der Unabhängigkeit mit dem Prinzip demokratischer Legitimation und Kontrolle 16
   - 2.3. Verfassungsrechtliche Überlegungen zur Unabhängigkeit 18
3. Die EU-Datenschutzgrundverordnung – Neue Herausforderungen und neue Chancen für die Aufsichtsbehörden 19
4. Das Modell Zertifizierung – Datenschutz in der Win-Win-Situation 22
   - 4.1 Die Ausgangssituation 22
   - 4.2 Das zweistufige Audit-Verfahren 23

II. GESUNDHEIT UND SOZIALES

1. Gesundheit 28
   - 1.1 Gesundheitsdienst-Datenverarbeitungsverordnung – GD-DVVO 28
   - 1.2 UKE – Forschung 29
   - 1.3 UKE – Hamburg City Health Studie 30
   - 1.4 MDK Nord – Verlust eines Laptops 31
   - 1.5 MDK Nord – Mailverkehr mit Krankenkassen 32
   - 1.6 National Single Window / Hafenärztlicher Dienst 33
   - 1.7 UKE – Auswertung der Zugriffe auf die elektronische Patientenakte 35
2. Soziales 36
   - 2.1 JUS-IT – keine integrierte Jugend- und Sozialarbeit in Hamburg 36
   - 2.2 Klientendaten von Mitarbeiterinnen und Mitarbeitern in JUS-IT 37
   - 2.3 Berichtswesen SHA 39
   - 2.4 Prüfung ASD – unverschlüsselter Mail-Versand 40
   - 2.5 Kontoabrufverfahren gem. § 93 AO 41
   - 2.6 Formularmäßige Offenlegung des Leistungsbezuges bei BuT-Beantragung 42

III. SCHULE, HOCHSCHULEN UND FORSCHUNG

1. Schule 46
   - 1.1 Abgeschottete Abteilung der Behörde für Schule und Berufsbildung 46
   - 1.2 Schülerdaten im Internet 47
   - 1.3 Hamburger Schreib-Probe 48
   - 1.4 Pilotprojekt „Start in die nächste Generation“ der Behörde für Schule und Berufsbildung 49

III.

1.5 Hamburger Medienpass / Medienkompetenztage 51
2. Hochschulen und Forschung 52
2.1 Koppelung Netzwerke der Universitäten mit dem FHH-Netz 52

IV. INNERES, SICHERHEIT UND JUSTIZ

1. Polizei 56
1.1 Vorratsdatenspeicherung 2.0 56
1.2 Gefahrengebiete 59
1.3 Bodycams 65
1.4 Prüfung der Antiterrordatei beim Landeskriminalamt Hamburg 66
1.5 Verdeckte Ermittlungen im Polizeirecht 71
1.6 Öffentlichkeitsfahndung im Internet durch Sicherheitsbehörden 77
1.7 Öffentlichkeitsarbeit über Social Media (Twitter und Facebook) 79
1.8 Einrichtung und Betrieb eines Rechen- und Dienstleistungszentrums zur Telekommunikationsüberwachung der Polizeien im Verbund der norddeutschen Küstenländer 80
1.9 Regeln zur Identifizierung von abwesenden Petenten bei Auskunftsersuchen 83
1.10 Nutzung von erkennungsdienstlichen Bildern aus dem Polizeilichen Auskunftssystem POLAS für Verkehrsordungswidrigkeitenverfahren 85
1.11 Polizeilicher Informations- und Analyseverbund (PIAV) 86
1.12 Datacenter Polizei 88
1.13 Predictive Policing 90
2. Verfassungsschutz 91
2.1 Datenerfassung aus sozialen Netzwerken im Internet 91
2.2 Eingaben zu Speicherungen beim Landesamt für Verfassungsschutz 92
3. Ausländerwesen 94
3.1 Kompetenzfeststellung von Asylantragstellern: Programm Work & Integration for Refugees (W.I.R.) 94
4. Justiz 95
4.1 Änderung der Bundesnotarordnung 95
4.2 Datenschutz in Rechtsanwaltskanzleien 97
4.3 Protokollierung lesender Zugriffe auf BASIS-Web 100
5. Meldewesen 102
5.1 Hamburgisches Ausführungsgesetz zum Bundesmeldegesetz Meldedatenübermittlungsverordnung / Spiegelmelderegister 102
5.2 Prüfung des Abrufverfahrens aus dem Melderegister für Jobcenter 107
6. Personenstandswesen 110
6.1 Generalregisterverfahren 110
6.2 Automation im Standesamt (AutiSta) 112

IV.

7. Statistik 113
   7.1 Registergestützte Volkszählung Zensus 2011 – Löschung der Hilfsmerkmale 113
   7.2 Landesinformationssystem (LIS) 115
8. Bezirke 117
   8.1 Online-Übertragungen aus Sitzungen der Bezirksversammlungen 117

V. TELEMEDIEN

1. Google 122
   1.1 Suchmaschine/Bearbeitung von Eingaben zu abgelehnten Google-Löschanträgen 122
   1.2 Google Privatsphärebestimmungen 125
   1.3 Google Apps in der Cloud 127
2. Facebook 129
   2.1 Neue Datenrichtlinie von Facebook und anwendbares Recht 129
   2.2 Pseudonyme Nutzung 131
   2.3 WhatsApp 133
3. Xing 134
   3.1 TLS-Verschlüsselung 134
   3.2 Onlinestatus 135
4. Orientierungshilfe Apps 135
5. Orientierungshilfe Cloud Computing 136
6. Stellungnahme zu einer Verfassungsbeschwerde über Pressearchive 137
7. Freies WLAN in Hamburg 138
8. Geltung des Medienprivilegs für Internetforen 139
9. Indoor-Ortung von Personen in Geschäften 141
10. Sportinformationsdienst im Internet 143
11. Prüfung von Partnerschaftbörsen im Internet 145
12. Umsetzung der Cookie-Richtlinie 147
13. Heartbleed Bug - Sicherheitslücke bei Web-Servern 149
14. Datenschutz-Kodex für Geodatendienste 150
15. Geobusiness Code of Conduct 152
16. Kamerafahrten durch Hamburgs Straßen – ein Nachtrag 153
17. Smart-TV und HbbTV, Orientierungshilfe Smart-TV 154

VI. E-GOVERNMENT, IT-VERFAHREN UND INFRASTRUKTUR DER FHH

1. E-Government und IT-Verfahren 160
   1.1 Sicherheit der Kommunikation (NGN, VoIP in der FHH) 160
   1.2 Umgang mit Apps/Mobilgeräten in der FHH 162
   1.3 DME Exciter - Sensible Daten auf unsicheren Geräten? 164

VI.
1.4 Sicherheit der E-Mail-Kommunikation der FHH - ein Schritt vor - mindestens ein Schritt zurück 167
1.5 Community-Cloud Mail Service - alles wolkig 172
1.6 Keine Mandantentrennung im FHHportal umgesetzt 174
1.7 Projekt „Intelligenter Bürgerservice“ (Kita-Gutschein) 176
1.8 Datenträgervernichtung: nur geschreddert und vermischt 178
2. Infrastruktur, Bauen, Wohnen, Energie 179
2.1 Smartes Hamburg, digitale Stadt 179
2.2 Datenschutzgerechte Reisezeitermittlung auf Autobahnen 183
2.3 HVV-Card 187
2.4 Projekte smartPORT 191
2.5 Funkbasierte Ablesegeräte 192
2.6 Übermittlung von Mieterdaten durch Vermieter an Energieversorger 194
2.7 Prüfung der Kundendatenverarbeitung bei einer Wohnungsbaugesellschaft 195

VII. VIDEOÜBERWACHUNG
1. Aktuelle Entwicklungen 200
1.1 Rechtsprechung 200
1.2 Orientierungshilfen und Beschlüsse der Datenschutzaufsichtsbehörden zur Videoüberwachung 201
2. Einzelfälle 202
2.1 Kfz-Kennzeichenerkennung in Parkhäusern am Hamburger Flughafen 202
2.2 Open Library 203
2.3 Videoüberwachung in Fitness- und Wellnessclubs 205
2.4 Videoüberwachung in einer Kindertagesstätte 206
2.5 Polizeiliche Videoüberwachung als automatisiertes Verfahren 207

VIII. WIRTSCHAFT UND FINANZEN
1. Kreditwesen und Auskunfteien 212
1.1 Scoring-Gutachten bei einer Auskunftei 212
1.2 Betrugspräventions-Dateien für Kreditinstitute 213
1.3 Meldung von Forderungen bei Abfrage aus einer Auskunftei 216
1.4 Warndatei im Versandhandel 217
1.5 Warndatei Elektronisches Lastschriftverfahren 219
1.6 Onlineportal zur Kreditvergabe 222
1.7 Bargeldloses Bezahlen in Fußballstadien 223
1.8 Abruf von Angehörigendaten durch Beschäftigte eines Kreditinstituts 224
2. Finanzen, Steuern und Rechnungswesen 225
2.1 Einheitspersonenkontenverordnung 225
2.2 HERAKLES: Freie Suche nach Bankkonten und Privat-Adressen möglich 227
2.3 Automatischer Kirchensteuerabzug vom Kapitalertrag 229

VIII.
3. Versicherungswirtschaft 231
3.1 Meldungen an das Hinweis- und Informationssystem – Sparte Kranken 231
3.2 Einwilligungserklärungen für die Dienste von Versicherungsmaklern 232
3.3 Geplante Datei zur Verhinderung von Tachomanipulationen 233
4. Handel und Werbung 234
4.1 Werbeschreiben eines Versandhändlers 234
5. Unterlassungsklagengesetz 234
5.1 Änderung des Unterlassungsklagengesetzes 234

IX. BESCHÄFTIGENDATENSCHUTZ
1. AK Beschäftigten-Datenschutz 238
1.1 Mitarbeiterüberwachung – Einsatz von Ortungssystemen 228
1.2 Mindestlohn 240
1.3 Arbeitgeberzeitschrift AKTIV 241
2. Workshop für behördliche Datenschutzbeauftragte 242
2.1 KoPers - Sachstand 243
3. Anlassbezogene Prüfungen 243

X. INTERNATIONALES
1. Safe Harbor 248
2. Fluggastdatenübermittlung 251

XI. INFORMATIONEN ZUR DIENSTSTELLE
1. Eingabenstatistik 256
2. Bußgeldfälle und Anordnungen 258
3. Meldepflicht nach § 42a BDSG 260
4. Register 261
5. Presse- und Öffentlichkeitsarbeit 262
6. Aufgabenverteilung (Stand: 1.1.2016) 264

ANHANG 268

STICHWORTVERZEICHNIS 290

Vorwort

Das Leben in der digitalen Welt ist einem ständigen Wandel und Anpassungsdruck ausgesetzt. Die Informationsgesellschaft erfasst alle Ebenen des öffentlichen und privaten Sektors in einer nie gekannten Totalität, beseitigt alte Strukturen und schafft neue Lebensbedingungen in einer Schnelligkeit wie in keiner anderen Epoche der Menschheit.

Daten spielen hierin als Wissens- und Steuerungsressource eine zentrale Rolle, die für wirtschaftliche Erfolge der Marktakteure, aber auch für die soziale Kontrolle und für staatliche Planungen von eminenter Bedeutung sind. Auf der anderen Seite erweisen sich personenbezogene Daten aber auch als Schlüssel zur Identität des Einzelnen und sind für eine freie und selbstbestimmte Lebensführung konstitutiv. In diesem Spannungsverhältnis fällt dem Datenschutz die Aufgabe zu, als regulatives Gegengewicht einer ausschließlich an das technisch Machbare ausgerichteten Strategie der umfassenden Datennutzung Grenzen zu setzen. Es geht dabei um nichts weniger als um die Herstellung der Rahmenbedingungen einer menschengerechten Entwicklung des digitalen Projekts der Moderne.

Die Dimension dieser Aufgabe lässt sich mit einem Vergleich zur Epoche der Industrialisierung verdeutlichen: Damals bestand die historische Herausforderung darin, die Dynamik des Kapitalismus durch soziale Strukturen zu bändigen, um die ökonomische Ausbeutung des abhängig Beschäftigten und seine Verelendung zu verhindern. In der Welt der Digitalisierung, in der mächtige technologische und ökonomische Fliehkräfte die Freiheit und Gleichheit der Menschen bedrohen, stellt sich die Frage nach dem Schutz des Einzelnen vor informationeller Ausbeutung, Fremdbestimmung und Ausgrenzung in ähnlicher Weise. Hier müssen die digitalen Grundrechte vor ihrer Erodierung durch moderne Technologien als Türöffner für alle erdenklichen ökonomischen und sozialen Ziele geschützt werden. Der Begriff des Überwachungskapitalismus, von der Wirtschaftswissenschaftlerin Shoshana Zuboff geprägt, macht diesen Vergleich greifbar. Die Daten werden als Produkte verstanden, die durch immer raffiniertere Überwachungstechnologien den Nutzern entzogen und kapitalisiert

werden. Vor diesem Hintergrund ist die Idee des selbstbestimmten Menschen, die als regulatives Ideal die freien Gesellschaften und den demokratischen Staat auszeichnet, zu schützen und zu bewahren ist, eine eminent wichtige Aufgabe staatlicher Gewährleistungsverantwortung. Sie in der Praxis sicherzustellen, obliegt den mit dem Vollzug des Datenschutzrechts beauftragten unabhängigen Datenschutzbehörden.

Datenschutz ist Grundrechtsschutz, gerade in Zeiten der digitalen Revolution. Das machen in affirmativer Weise zwei Entwicklungen in den letzten beiden Jahren auf der Ebene der EU besonders sichtbar: Die aktuelle Rechtsprechung des Europäischen Gerichtshofs und die Ende 2015 im Trilog beschlossene EU-Datenschutzgrundverordnung. Der Europäische Gerichtshof hat in seinen bahnbrechenden Entscheidungen zur Vorratsdatenspeicherung, zum Recht auf Vergessenwerden und zu Safe Harbor im Berichtszeitraum in eindrucksvoller Weise dokumentiert, dass die Wahrung der Grundrechte des Datenschutzes und auf private Lebensführung einen zentralen Baustein der europäischen Rechtskultur darstellt. Parallel dazu wird die neue EU-Datenschutzgrundverordnung die Rechte Betroffener stärken. Sie ist eine wirksame Antwort auf die modernen Herausforderungen, denen sich ein demokratischer Verfassungsstaat stellen muss, für den die rechtsstaatlichen Garantien und Grundrechte konstitutiv sind.

Es liegt in besonderer Weise an den Datenschutzbehörden, die Rechte Betroffener durchzusetzen. Diese dürfen mit ihrer Aufgabe aber nicht allein gelassen werden. Sie benötigen hierzu eine auskömmliche Ausstattung, um diese Aufgabe in völliger Unabhängigkeit wahrnehmen zu können. Die Haushaltsgesetzgeber in Bund und Ländern haben hierfür im Rahmen ihrer grundrechtlichen Schutzpflichten hinreichend Rechnung zu tragen.

Johannes Caspar
Februar 2016

I. DATENSCHUTZ IM UMBRUCH – DEFIZITE, NEUE HERAUSFORDERUNGEN, LÖSUNGSANSÄTZE

1. Einleitung 12
2. Rechtliche Stärkung der Unabhängigkeit des HmbBfDI – Bestandsaufnahme und Vorschläge 13
3. Die EU-Datenschutzgrundverordnung – Neue Herausforderungen und neue Chancen für die Aufsichtsbehörden 19
4. Das Modell Zertifizierung – Datenschutz in der Win-Win-Situation 22

1. Einleitung

Der Berichtszeitraum 2014 bis 2015 markiert für den Datenschutz eine Umbruchphase. Der Zeitraum leitet eine Entwicklung ein, in deren Verlauf sich die gesamte Struktur des bisher bekannten Datenschutzes auf allen Ebenen massiv verändern wird. Auf der EU-Ebene ging die Diskussion um die EU-Datenschutzgrundverordnung im Dezember 2015 mit den Trilogverhandlungen in die letzte Runde. Das Ergebnis wird das Datenschutzrecht, das bislang weitgehend eine Sache der Mitgliedstaaten war, im Wesentlichen erneuern und vereinheitlichen.

Neben dieser grundlegenden rechtlichen Novellierung hat die digitale Entwicklung auch im vergangenen Berichtszeitraum sowohl in qualitativer als auch in quantitativer Hinsicht die Anforderungen an die Arbeit der Datenschutzbehörden weiter erhöht. Während die digitale Welt sich rasend schnell verändert, stagniert die Ausstattungssituation im Bereich des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit seit mehr als 10 Jahren. Die Behörde ist damit immer weniger in der Lage, die vielfältigen Anforderungen an einen zeitgemäßen Datenschutz technisch und rechtlich zu erfüllen. Dies ist vor dem Hintergrund einer komplexen Neukonstruktion des Datenschutzrechts, die eine Vernetzung und das Zusammenwachsen der Datenschutzbehörden innerhalb der Europäischen Union erfordert, Besorgnis erregend. Das gilt gerade auch wegen des fortlaufend erweiterten Aufgabenspektrums, das in den letzten Jahren im Zuge der Entscheidungen des Europäischen Gerichtshofs und des Bundesverfassungsgerichts entstand: So ist die Behörde des Hamburgischen Beauftragten mittlerweile nicht nur bundesweit zuständig für die Beschwerden von Betroffenen, die gegen die Google-Suchmaschine ihr Recht auf Löschung geltend machen, sondern muss auch die Datenübermittlung zahlreicher Unternehmen in die USA, die nach der Safe Harbor-Entscheidung des EuGH in Frage steht, überprüfen. Schließlich hat auch eine umfassende Kontrolle der Anti-Terror-Dateien der Sicherheitsbehörden zu erfolgen, für deren fristgerechte Überprüfung das Bundesverfassungsgericht ausdrücklich eine verbesserte Ausstattung der Datenschutzbehörden gefordert hatte.

Um die Kluft zwischen gesetzlichem Auftrag und Wirklichkeit zu dokumentieren, wird dem Tätigkeitsbericht ein Bericht über die Ausstattungssituation des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit als Anhang beigefügt, der bereits im Dezember 2015 dem Ausschuss für Justiz und Datenschutz der Hamburgischen Bürgerschaft vorlag. Der Tätigkeitsbericht versteht sich insoweit nicht nur als Bericht über die Tätigkeit der letzten zwei Jahre, sondern soll bewusst auch als Dokument der Auslassung verstanden werden, das die Defizite des letzten Berichtszeitraums beleuchtet und aufzeigt, was in der aufsichtsbehördlichen Tätigkeit aufgrund mangelnder Ressourcen nicht möglich war. Ausgehend von einem durch Erfahrungsberichte der einzelnen Referate unterfütterten Defizitkatalog, der dem Tätigkeitsbericht als Anlage beigefügt wurde, werden im Bericht die Forderungen nach personellen Ressourcen für eine angemessene Ausstattung der Behörde näher skizziert. Im Folgenden gilt es, vor dem Hintergrund bestehender Defizite und der Verbesserung der Ausstattungs-

situation weitere mögliche Strategien aufzuzeigen, die eine Stärkung des Datenschutzes in Hamburg künftig bewirken kann.

2. Rechtliche Stärkung der Unabhängigkeit des HmbBfDI – Bestandsaufnahme und Vorschläge

Eine Stärkung der Datenschutzaufsicht in Hamburg ist nicht allein auf eine materielle Ebene der besseren Ausstattung verwiesen. Vielmehr geht es gerade darum, durch die rechtliche Umsetzung eines Konzepts der Unabhängigkeit dieses Amtes flexible Strukturen zu schaffen, die einen Schutz vor äußerer Einflussnahme in mittelbarer oder unmittelbarer Weise ermöglichen und dem Amtsinhaber insbesondere die Steuerungsinstrumente in die Hand geben, die Belange der Behörde künftig umfassend in eigenständiger Weise zu vertreten. Neben der Möglichkeit, Vorschläge für den eigenen Haushalt in die Haushaltsberatungen des Parlaments einzubringen, spielt die Unabhängigkeit der Behörde eine wichtige Rolle für die künftige Eigenständigkeit im organisatorischen Sinne. So ist zu entscheiden, ob die Anbindung der/des Beauftragten für Datenschutz und Informationsfreiheit an eine andere Stelle der Freien und Hansestadt Hamburg (Senat, Bürgerschaft) künftig angesichts des Unabhängigkeitspostulats des EU-Rechts noch sinnvoll ist oder die Vorgaben letztlich für eine organisatorische Verselbständigung sprechen.

Insoweit sind die Initiativen innerhalb der Hamburgischen Bürgerschaft nachdrücklich zu begrüßen, die eine Verbesserung der Stellung der/des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit vorsehen (siehe Drucksache 20/12758; Drucksache 20/12974; Drucksache 21/315; Drucksache 21/683). Anlässlich einer Expertenanhörung, die im Rahmen der letzten beiden Initiativen im Ausschuss für Justiz und Datenschutz am 1. Dezember 2015 durchgeführt wurde, haben sich verschiedene Vertreter aus Wissenschaft, Rechtsanwaltschaft sowie Behörden zu den Möglichkeiten einer rechtlichen Stärkung der Unabhängigkeit des Amtes der/des Datenschutzbeauftragten geäußert (Protokoll der öffentlichen Sitzung des Ausschusses für Justiz und Datenschutz, 1. Dezember 2015, Nr. 21/4).

Ohne in die Diskussionen über die Ergebnisse der Anhörung im Einzelnen einzutreten, lässt sich feststellen, dass ein weiter politischer Gestaltungsspielraum zur Umsetzung von Konzepten der Unabhängigkeit besteht. Dieser wird rechtlich nach oben hin durch das verfassungsrechtlich vorgegebene Demokratieprinzip begrenzt, das im Grundsatz eine Weisungsgebundenheit der Verwaltung gegenüber der Regierung und zumindest bei der hierarchischen Ministerialverwaltung eine Kontrolle durch Rechts- oder Fachaufsichtsinstrumente erfordert. Nach unten hin wird der Gestaltungsspielraum durch den Begriff der völligen Unabhängigkeit begrenzt und abgesichert, der durch die Rechtsprechung des EuGH der letzten Jahre konkretisiert und fortgeschrieben wurde.

Alle Konzepte der Umsetzung des Unabhängigkeitserfordernisses müssen innerhalb dieses Regelungsspielraums liegen.

2.1 Der Begriff der völligen Unabhängigkeit

Nach Art. 28 Abs. 1 der Richtlinie 95/46 des Europäischen Parlaments und des Rates vom 24.Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281, S. 31) sehen die Mitgliedstaaten vor, dass eine oder mehrere öffentliche Stellen beauftragt werden, die Anwendung der von den Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in ihrem Hoheitsgebiet zu überwachen. Hierzu wird ausdrücklich bestimmt: „Diese Stellen nehmen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahr."

Der Europäische Gerichtshof hat in drei Urteilen zu Vertragsverletzungsverfahren dieser Vorschrift (Kommission-Deutschland, Kommission-Österreich sowie Kommission-Ungarn) den Begriff der völligen Unabhängigkeit näher konkretisiert und dabei die Stellung des Datenschutzbeauftragten nachhaltig gegenüber Einschränkungen durch mitgliedstaatliche Exekutiv- sowie Legislativakte gestärkt.

Danach müssen die für den Schutz personenbezogener Daten zuständigen Kontrollstellen mit einer Unabhängigkeit ausgestattet sein, die es ihnen ermöglicht, ihre Aufgaben ohne äußere Einflussnahme wahrzunehmen (EuGH C – 518/07 Slg. 2010 Rdnr. 30). Dies bedeutet, dass Kontrollstellen jeder äußeren Einflussnahme, sei sie unmittelbar oder mittelbar, entzogen sein müssen, die ihre Entscheidung steuern könnte (a.a.O., siehe Rdnr. 25, 30 und 50). Damit ist bereits „jede Form der mittelbaren Einflussnahme, die zur Steuerung der Entscheidung der Kontrollstelle geeignet wäre" auszuschließen (Kommission gegen Österreich, EuGH C-614/10, Rn. 41, 43). Der EuGH führt weiter aus, dass die funktionelle Unabhängigkeit der Kontrollstellen, in dem Sinn, dass deren Mitglieder bei der Wahrnehmung ihrer Aufgaben an keine Anordnung gebunden sind, eine notwendige Voraussetzung für die nach Art. 28 Abs. 1 der Rl 95/46 bestehende Unabhängigkeit darstelle (Kommission gegen Österreich, EuGH C-614/10, Rn. 42, Kommission gegen Ungarn, EuGH- 288/12, Rn 52). Diese reicht jedoch allein nicht aus, um die Kontrollstelle vor jeder äußeren Einflussnahme zu bewahren. So ist es einem Mitgliedstaat etwa auch grundsätzlich verwehrt, die Amtszeit des Mandats einer Kontrollstelle vorzeitig zu beenden, es sei denn, es wäre ein schwerwiegender und objektiv nachprüfbarer Grund gegeben. Die bloße Umstrukturierung oder eine Änderung des Modelles der Datenschutzaufsichtsbehörde rechtfertigt dies nicht. Denn die „Drohung einer solchen vorzeitigen Beendigung, die dann während der gesamten Ausübung des Mandats über dieser Stelle schwebte", würde zu „einer Form des Gehorsams dieser Stelle gegenüber den politischen Verantwortlichen führen, die mit dem Unabhängigkeitsgebot nicht vereinbar wäre" (Kommission

gegen Ungarn, EuGH- 288/12, Rn.54, 52).

Aus der Gesamtschau der Urteile ergibt sich, dass Datenschutzbehörden weder durch rechtsaufsichtliche noch durch fachaufsichtliche Kontrolle in die Staatsverwaltung integriert sein dürfen. Eine rechtliche Kontrolle sowie eine Kontrolle der Zweckmäßigkeit der Entscheidungen der Datenschutzaufsichtsbehörden durch eine übergeordnete Behörde scheiden damit aus. Gleiches gilt im Grundsatz für eine Dienstaufsicht einer übergeordneten Behörde zur Kontrolle der Einhaltung der Dienstpflichten gegenüber einer unabhängigen Datenschutzaufsichtsbehörde. Hierzu hat der EuGH zwar nicht unmittelbar Stellung bezogen. Unbestritten ist jedoch, dass die Dienstaufsicht ihre Grenze an der Unabhängigkeit der/des Datenschutzbeauftragten hat. Eine umfassende Dienstaufsicht ist jedenfalls mit der Wahrnehmung der völligen Unabhängigkeit des Amts der/des Datenschutzbeauftragten nicht vereinbar.

In diesem Sinne unterstellt § 22 Abs. 1 HmbDSG den HmbBfDI der Dienstaufsicht des Senats und ordnet an, dass die Regelungen über die Dienstaufsicht für Berufsrichterinnen und Berufsrichter entsprechend anwendbar sind. Danach gilt § 26 des Deutschen Richtergesetzes. Diese Vorschrift statuiert für Richter eine Dienstaufsicht vorbehaltlich des Bestehens der richterlichen Unabhängigkeit und umfasst die Befugnis, „die ordnungswidrige Art der Ausführung eines Amtsgeschäftes vorzuhalten und zu ordnungsgemäßer, unverzögerter Erledigung der Amtsgeschäfte zu ermahnen."

Das Modell der beschränkten Dienstaufsicht überführt damit eine Aufsicht, der Berufsrichter unterliegen, auf das Verhältnis zwischen vorgesetzter Stelle und dem Leiter einer unabhängigen Kontrollstelle. Das ist in letzter Konsequenz nicht unproblematisch, da bei Beschwerden - etwa aufgrund zu langer Bearbeitungszeiten - jedenfalls formal die Dienstaufsicht führende Stelle prüfen müsste, ob der jeweilige Vorgang dem Bereich der unabhängigen Amtsführung zuzuordnen ist. Dies kann – wie mitunter die Praxis aus anderen Bundesländern zeigt – durchaus konfliktträchtige Konstellationen zwischen Aufsicht und kontrollierender Stelle herbeiführen. Schließlich ist die Grenze zwischen der nicht näher bestimmten Unabhängigkeit und dem Bereich einer beschränkten Dienstaufsicht gerade mit Blick auf die vielschichtigen Aufgaben der Datenschutzbehörden nur schwer zu bestimmen. Bedacht werden muss, dass die dienstrechtliche Kontrolle eines Richters, dem richterliche Unabhängigkeit nach Art. 97 GG zukommt, nicht gleichzusetzen ist mit der nach Art. 28 Abs. 1 der EU-Datenschutzrichtlinie geforderten vollständigen Unabhängigkeit der Kontrollstelle. Der einzelne Richter ist regelmäßig eingebunden in die Organisation der rechtsprechenden Gewalt. Weil am Ende über die rechtsmäßige Ausübung der Amtsführung Richter entscheiden, ist dieses Verfahren unproblematisch. Die Kontrolle erfolgt hier grundsätzlich „organisationsintern". Die unabhängige Kontrollstelle für den Datenschutz ist demgegenüber dem herkömmlichen Schema der Staatsgewalt gerade nicht zuzuordnen. Als Aufsichtsbehörde ist sie am ehesten der Exekutive ähnlich, von deren hierarchischem Verwaltungsaufbau sie aber aufgrund der europarechtlichen Vorgaben strikt geschieden

sein muss - nicht zuletzt, da sie gerade auch die Exekutive kontrolliert.

Das klarere und den Begriff der völligen Unabhängigkeit deutlicher zum Ausdruck bringende europarechtskonforme Modell der Ausgestaltung der völligen Unabhängigkeit führt daher konsequenterweise zu einem gänzlichen Verzicht auf die Dienstaufsicht. Dieser Weg wurde jüngst durch das Gesetz zur Änderung des Bundesdatenschutzgesetzes – Stärkung der Unabhängigkeit der Datenschutzaufsicht im Bund durch Errichtung einer obersten Bundesbehörde für die Bundesdatenschutzbeauftragte (BT Drucks. 18/2848, vom 13.10.2014) beschritten. Ein derartiges Modell lässt sich bruchlos gerade ohne Anbindung der unabhängigen Kontrollstelle an eine andere Stelle der Freien und Hansestadt Hamburg verwirklichen.

2.2 Vereinbarkeit der Unabhängigkeit mit dem Prinzip demokratischer Legitimation und Kontrolle

Das Absehen von einer auch beschränkten Dienstaufsicht darf letztlich nicht dazu führen, dass der demokratietheoretische Legitimationsgrundsatz in Frage gestellt wird. Soweit einer extensiven Auslegung des Unabhängigkeitsmodells der Datenschutzbehörden das Fehlen eines aus dem Demokratieprinzip folgenden Weisungs- und Kontrollmechanismus entgegengehalten wird, hat sich der EuGH im Verfahren Deutschland -Kommission hierzu in eindeutiger Weise geäußert. In diesem Urteil stellt der EuGH fest, dass

„der Grundsatz der Demokratie zur Gemeinschaftsrechtsordnung gehört und in Art. 6 Abs. 1 EU ausdrücklich als Grundlage der Europäischen Union niedergelegt ist. Als den Mitgliedstaaten gemeinsamer Grundsatz ist er daher bei der Auslegung eines sekundärrechtlichen Aktes wie Art. 28 der Richtlinie 95/46 zu berücksichtigen. Dieser Grundsatz bedeutet nicht, dass es außerhalb des klassischen hierarchischen Verwaltungsaufbaus keine öffentlichen Stellen geben kann, die von der Regierung mehr oder weniger unabhängig sind. Das Bestehen und die Bedingungen für das Funktionieren solcher Stellen sind in den Mitgliedstaaten durch Gesetz und in einigen Mitgliedstaaten sogar in der Verfassung geregelt, und diese Stellen sind an das Gesetz gebunden und unterliegen der Kontrolle durch die zuständigen Gerichte. Solche unabhängigen öffentlichen Stellen, wie es sie im Übrigen auch im deutschen Rechtssystem gibt, haben häufig Regulierungsfunktion oder nehmen Aufgaben wahr, die der politischen Einflussnahme entzogen sein müssen, bleiben dabei aber an das Gesetz gebunden und der Kontrolle durch die zuständigen Gerichte unterworfen. Eben dies ist bei den Aufgaben der Kontrollstellen für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten der Fall.

Gewiss kommt ein Fehlen jeglichen parlamentarischen Einflusses auf diese Stellen nicht in Betracht. Die Richtlinie 95/46 schreibt jedoch den Mitgliedstaaten keineswegs vor, dem Parlament jede Einflussmöglichkeit vorzuenthalten" (EuGH C-518/07, Rn. 41ff).

Bereits gegenwärtig erfolgt die Wahl des Hamburgischen Beauftragten unmittelbar

durch die Bürgerschaft. Dieses Verfahren verbürgt bereits eine direkte demokratische Legitimation bei der Berufung der Person, die dieses Amt ausübt. Die personelle Legitimation könnte noch intensiviert werden, indem auch das Vorschlagsrecht zur Wahl des bzw. der Beauftragten für Datenschutz und Informationsfreiheit vom Senat auf die Bürgerschaft übertragen wird. Damit ist die unabhängige Stellung des Datenschutzbeauftragten bereits mit Blick auf das Berufungsverfahren außerhalb des klassischen Verwaltungsaufbaus anzusiedeln. Durch Schaffung konkreter Kontrollregelungen ist ferner die demokratische Verantwortung bei der Wahrnehmung des Amtes sicherzustellen.

Das Absehen von jeglicher Aufsicht von anderen Stellen kann insbesondere durch ein förmliches Abberufungsverfahren, das etwa im Falle von schweren dienstlichen Verfehlungen durch die Regierung oder durch das Parlament angestoßen und von einer unabhängigen Instanz bestätigt werden muss, kompensiert werden. Dieses Verfahren erweist sich als ein wichtiges Korrektiv demokratischer Kontrolle. Eine sich auf die gesamte ordnungsgemäße Amtsführung im Detail erstreckende beschränkte Dienstaufsicht ist dem gegenüber nicht erforderlich. In diesem Sinne bestimmt § 23 BDSG, dass die oder der Bundesbeauftragte auf Vorschlag der Bundesregierung entlassen wird, wenn Gründe vorliegen, die bei einem Richter auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen.

Die parlamentarische Kontrolle durch die Bürgerschaft wird bereits nach derzeit geltender Rechtslage mit Blick auf die Gutachten- und Berichtspflichten der/des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit sowie mit Blick auf die Aufstellung von dessen Haushalt ausgeübt. Diese Vorschriften könnten insbesondere durch weitere abschließende bereichsspezifische Regelungen, etwa zum Ausschluss bzw. zur Anzeige- bzw. Genehmigungspflicht bei Nebentätigkeiten, verdichtet werden.

Weitere wichtige Kontroll- und Einflussmöglichkeiten bestehen darüber hinaus bereits gegenwärtig durch die gerichtliche Überprüfbarkeit von Entscheidungen der unabhängigen Kontrollstelle. Dies gilt für die von der Datenschutzaufsichtsbehörde verhängten Anordnungen oder Bußgelder. Durch die EU-Datenschutzgrundverordnung wird die gerichtliche Kontrolle künftig noch erweitert. Danach können auch Betroffene eine inhaltliche Überprüfung der Ablehnungsentscheidung einer Kontrollstelle durch Gerichte vornehmen lassen.

Insgesamt ist es daher mit dem Demokratiegrundsatz vereinbar, den Beauftragten von einer Dienstaufsicht insgesamt zu befreien. Dies entspricht auch einer Stärkung des Amts gegenüber einer potentiellen unmittelbaren und mittelbaren Einflussnahme. Zur Vermeidung einer statischen und in ihrer Dimension nicht klar definierbaren Dienstaufsicht, die unter einem allgemeinen Vorbehalt der Beeinträchtigung der Unabhängigkeit steht, erscheint es daher sinnvoll, hiervon zugunsten eines Sets klar umrissener Kontrollregelungen abzusehen.

2.3. Verfassungsrechtliche Überlegungen zur Unabhängigkeit

Die rechtliche Verpflichtung zur Schaffung vollständig unabhängiger Kontrollstellen für den Datenschutz ist nicht nur durch Art. 28 RL 95/46 vorgegeben. Sie ist daneben auf der EU-Ebene unmittelbar im Primärrecht verankert. Die Grundrechtecharta der EU enthält in Art. 8 ein Grundrecht auf Datenschutz. Abs. 3 enthält folgende Formulierung: „Die Einhaltung dieser Vorschriften wird durch eine unabhängige Stelle überwacht". Der Vertrag über die Arbeitsweise der Europäischen Union sieht in Art. 16 ebenfalls ein Recht auf Datenschutz vor, das von unabhängigen Behörden kontrolliert wird.

Insoweit sind sowohl die Bundes- als auch die Landeregelungen an die Gewährleistung einer vollständig unabhängigen Datenschutzaufsicht durch vorrangiges europäisches Recht gebunden. Die Stellung von Datenschutzbehörden außerhalb der hierarchischen Ministerialverwaltung ist daher nicht nur ein denkbares politisches Ziel, sondern rechtlich gefordert. Die Besonderheit von senatsunabhängigen Kontrollstellen ist bislang mit der Landesverfassung noch nicht in Einklang gebracht worden. Art. 33 Abs. 2 der Hamburger Verfassung bestimmt für den Hamburger Senat, dass dieser die Verwaltung führt und beaufsichtigt. Die Beaufsichtigung umfasst sowohl die Rechts- als auch Fachaufsicht über die gesamte Verwaltung. Der Hamburger Senat übt jedoch lediglich eine beschränkte Dienstaufsicht, jedoch weder eine Rechts- noch eine Fachaufsicht über die/den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit aus. Insoweit liegt hierin eine tatsächliche Abweichung vom in Art. 33 Abs. 2 HV enthaltenen Grundsatz einer Kontrollverantwortung des Senats.

Damit aber läuft Art. 33 Abs. 2 LV mit Blick auf die/den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit gegenwärtig faktisch leer. Das kann im Rahmen einer europarechtskonformen Auslegung sicherlich so hingenommen werden. Danach ermöglicht die Geltung dieser Bestimmung aufgrund höherrangiger Vorschriften des EU-Rechts die Existenz einer unabhängigen Aufsichtsbehörde. Um dieses Ergebnis unmittelbar mit der Landesverfassung zu harmonisieren, bedarf es jedoch einer ausdrücklichen landesverfassungsrechtlichen Ausnahmeregelung, die die besondere Stellung der Datenschutzbehörde nach dem EU-Recht im Verfassungsgefüge der Freien und Hansestadt Hamburg erwähnt. Damit wäre im Übrigen ein Schritt vollzogen, den bereits neun andere Bundesländer in den dortigen Landesverfassungen gegangen sind: Bayern (Art. 33a), Berlin (Art. 47), Brandenburg (Art. 74), Mecklenburg-Vorpommern (Art. 37), Niedersachsen (Art. 62), Nordrhein-Westfalen (Art. 77a), Sachsen (Art. 57), Sachsen-Anhalt (Art. 63) und Thüringen (Art. 69).

Schließlich enthält die neue EU-Datenschutzgrundverordnung in Art. 53 Abs. 1 b weitergehende Befugnisse der Kontrollstellen gegenüber den für die Datenverarbeitung verantwortlichen Stellen. Hierzu zählen künftig gerade auch öffentliche Stellen, da die Datenschutzgrundverordnung die grundsätzliche Unterscheidung zwischen Behörden und privaten Stellen, die derzeit noch nach Bundes- und Landesrecht besteht, nicht mehr fortschreibt. Damit gehen die aufsichtsbehördlichen Befugnisse gegenüber öffentlichen Stellen künftig über die bloße Beanstandung hinaus und ermöglichen

zumindest rechtlich verbindliche Anordnungen gerade auch gegen Behörden der unmittelbaren und mittelbaren Senatsverwaltung. Auch dies spricht ebenfalls dafür, den besonderen Status der Kontrollstelle außerhalb der hierarchischen Senatsverwaltung landesverfassungsrechtlich deutlich zum Ausdruck zu bringen.

3. Die EU-Datenschutzgrundverordnung – Neue Herausforderungen und neue Chancen für die Aufsichtsbehörden

Seit die damalige EU-Justizkommissarin Viviane Reding 2012 den ersten Entwurf einer Datenschutzgrundverordnung vorlegte, sind vier Jahre vergangen. In dieser Zeit wurde die Debatte um eine Neufassung des europäischen Datenschutzes auf allen Ebenen der EU geführt. Am Ende durchliefen die Entwürfe der Datenschutzgrundverordnung den sog. Trilog zwischen Europäischem Parlament, dem Rat und der Kommission. Das Ergebnis, das im Dezember 2015 gefunden wurde, ist im Großen und Ganzen zu begrüßen. Auf Seiten des Datenschutzes war naturgemäß nicht alles durchzusetzen, was für einen einheitlichen europäischen Datenschutz auf hohem Standard zuvor gefordert wurde (dazu Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen zur Datenschutz-Grundverordnung, Konferenz der Datenschutzbeauftragten des Bundes und der Ländern, vom 14. August 2015). So fehlt etwa ein Recht auf pseudonyme Nutzung für europäische Nutzer und auch das Erfordernis einer expliziten Einwilligung für die Datenverarbeitung. Eine wirksame Begrenzung der Profilbildung wird weitgehend verfehlt.

Auf der Habenseite steht, dass die Datenschutzgrundverordnung für einen Einzugsbereich von einer halben Milliarde Menschen gemeinsame Bestimmungen zum Datenschutz bringt, die künftig unmittelbar gelten. Ihre Auswirkungen sind sowohl auf Landes- als auch auf Bundesebene bereits jetzt spürbar. Hervorzuheben ist, dass künftig das Marktortprinzip maßgebend sein wird, wonach die Regelungen des europäischen Datenschutzrechts schon dann anwendbar sind, wenn Unternehmen sich mit ihren Angeboten an Kunden innerhalb der EU wenden. Ob diese eine Niederlassung in der EU haben oder die Daten in der EU verarbeiten, ist hierfür unerheblich. So sind dann auch Dienste wie Whatsapp in Zukunft unmittelbar an das EU-Datenschutzrecht gebunden, selbst wenn diese keine Niederlassung in der EU haben und dort auch keine Daten verarbeiten.

Daneben gilt künftig die Regelung des „One-Stop-Shop". Bürger sollen sich unabhängig vom Sitz des Unternehmens immer direkt an ihre lokale Aufsichtsbehörde wenden können. Daten verarbeitende Unternehmen sollen ebenfalls nur eine Anlaufstelle in der EU haben, die dann grundsätzlich als Aufsichtsbehörde für deren Datenverarbeitung europaweit zuständig ist. Um zu verhindern, dass die Unternehmen aufgrund dieser Regelung in einen Wettlauf an den Ort der schwächsten Behörde eintreten, sieht die Datenschutzgrundverordnung durch das sog. Kohärenzverfahren ein gemeinsames

Clearingverfahren auf Ebene der EU vor. Dieses wird vor dem EU-Datenschutzausschuss geführt, wenn es zwischen der federführenden und den ebenfalls betroffenen anderen Aufsichtsbehörden zu unterschiedlichen Sichtweisen hinsichtlich eines aufsichtsbehördlichen Vorgehens kommt. Am Ende entscheidet dann der EU-Datenschutzausschuss – ein Gremium, das aus dem Leiter bzw. der Leiterin einer Aufsichtsbehörde jedes Mitgliedstaates der EU und dem oder der Europäischen Datenschutzbeauftragten zusammengesetzt ist und seine Beschlüsse nach dem Mehrheitsprinzip fasst.

Durch den politischen Kompromisscharakter einzelner terminologisch unbestimmter materieller Datenschutzregelungen wird deren Vollzug in der Praxis nicht leicht fallen. Das aufwändige aufsichtsbehördliche Konsultations- und Abstimmungsverfahren wird ein Höchstmaß an Kommunikation zwischen den nationalen Aufsichtsbehörden erfordern. Dabei muss sich erst noch erweisen, ob und inwieweit der Kohärenzmechanismus am Ende einen Datenschutz mit hohem Vollzugsstandard ermöglicht. Zudem bedeuten neue Pflichten der verantwortlichen Stellen einen zusätzlichen Aufwand für die Aufsichtsbehörden. So macht die künftige Datenschutz-Folgeabschätzung unterschiedliche Maßnahmen der Behörden erforderlich, die von der Erstellung einer Liste von Verarbeitungsvorgängen für die Durchführung von Folgeabschätzungen bis hin zu Beurteilungen im Rahmen von Konsultationsverfahren reichen. Datenschutz wird also ein Stück bürokratischer.

Innerhalb eines Übergangszeitraums von zwei Jahren, nach denen die Datenschutzgrundverordnung durch Veröffentlichung im Amtsblatt in Kraft tritt, gilt es, in den Aufsichtsbehörden erhebliche Anpassungsbedarfe an die neue Rechtslage zu bewältigen. In digitalen Kategorien sind zwei Jahre zwar eine lange Zeitspanne, in rechtlicher Hinsicht jedoch eher knapp bemessen: Im Detail sind viele Regelungen als Formelkompromisse konzipiert und lassen jeweils unterschiedliche Interpretationen zu. Die Vorschriften und die neue Struktur der künftigen Datenschutzaufsicht sind in dieser Zeit im nationalen sowie supranationalen Bereich zu diskutieren sowie umzusetzen. Es gilt zu klären, in welcher Weise nationale Regelungen und solche auf Länderebene weiter gelten können und wo es Anpassungsbedarfe gibt. Gerade Daten verarbeitende Unternehmen werden bereits vorab erheblichen Aufklärungsbedarf über die neue Rechtslage geltend machen, dem sich die Aufsichtsbehörden nicht verweigern können.

Während andere nationale Aufsichtsbehörden bereits Stellenforderungen für die Zeit des Übergangs und danach aufstellen und teilweise schon umgesetzt bekamen, besteht für den Bereich des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit noch immer eine uneingelöste offene Forderung nach einer angemessenen Ausstattung für den bisherigen Rechtszustand, die zunächst einmal umzusetzen ist.

Die Komplexität der neuen Rechtslage wird noch dadurch erhöht, dass parallel zu der Datenschutzgrundverordnung die Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck

der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (sog. JI-Richtlinie) auf den Weg gebracht wurde, deren Umsetzung durch die Mitgliedstaaten erfolgen muss. Das Nebeneinander zwischen unmittelbar geltender Datenschutzgrundverordnung und mitgliedstaatlich umzusetzender Richtlinie wird den Implementierungsprozess erschweren.
Trotz aller Schwierigkeiten, die sich im Übergangszeitraum bis voraussichtlich spätestens Mitte 2018 stellen, muss die neue Situation als Chance für einen effizienten Datenschutz gesehen werden. Bereits in den letzten Jahren hat sich gezeigt, dass die Zusammenarbeit mit anderen europäischen Aufsichtsbehörden, gerade im Rahmen der Google Task-Force und der Facebook-Kontaktgruppe, bei der der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit beteiligt ist, den Druck gerade auf überregional agierende Unternehmen zur Einhaltung der Regelungen des Datenschutzes verstärkt hat. Dieser Effekt wird unter der Geltung einheitlicher EU-Datenschutzregelungen noch zunehmen, zumal die Anhebung des Sanktionsrahmens für Bußgelder auf bis zu 4% des weltweiten Jahresumsatzes eines Unternehmens nun auch eine Stärkung der aufsichtsbehördlichen Durchsetzungsinstrumente gegenüber globalen Internetdienstleistern schafft.

Die neuen Regelungen sehen aber nicht nur eine Stärkung der Instrumente zur Überwachung nicht-öffentlicher Stellen vor, sondern schaffen einen effizienteren Rahmen für die rechtliche Durchsetzung der Anforderungen des Datenschutzes auch gerade gegenüber der öffentlichen Verwaltung. Unabhängig davon, ob künftig die Mitgliedstaaten von der Kompetenz Gebrauch machen werden, ihren Aufsichtsbehörden die Befugnisse zu verleihen, Geldbußen auch gegenüber Behörden festzusetzen, stehen den Kontrollstellen künftig rechtsverbindliche Verfahren zur Durchsetzung des Datenschutzrechts auch gegenüber der Verwaltung zur Verfügung. Dies ist gegenüber dem bislang schärfsten Schwert, der für die jeweiligen öffentlichen Stellen bloßen formalen Beanstandung nach § 25 HmbDSG, zweifellos eine Stärkung. Es ist davon auszugehen, dass die Möglichkeit der rechtlichen Durchsetzung von Datenschutzanforderungen durch Anweisungen und Anordnungen dazu beitragen wird, ihnen auch bei öffentlichen Stellen stärker und schneller Gehör zu verschaffen. Angesichts zahlreicher Verfahren auch mit Blick auf langwierige Datenschutzanforderungen gegenüber öffentliche Stellen, die in erheblichem Maße Kapazitäten der Behörde binden, ist die Schärfung der Vollzugsinstrumente nachdrücklich zu begrüßen.

4. Das Modell Zertifizierung – Datenschutz in der Win-Win-Situation

4.1 Die Ausgangssituation

Insbesondere in der IT-Branche werden nicht selten Geschäftsmodelle entwickelt, deren Umsetzung den datenschutzrechtlichen Vorgaben widerspricht. Dies geschieht allerdings häufig nicht aus mangelnder Gesetzestreue, sondern aufgrund fehlender Kenntnis oder falscher Einschätzung der gesetzlichen Vorgaben. Eine vorherige Beratung könnte Fehlentwicklungen vermeiden und dadurch die Compliance und somit auch das Datenschutzniveau erhöhen. Gütesiegelverfahren könnten in Abgrenzung dazu datenschutzfreundliche Produkte „belohnen" und die Entwicklung des Marktsegments in den Bereichen der Datensicherheits- und Datenschutztechnologie fördern.

In jüngster Zeit treten immer häufiger Unternehmen an uns mit der Bitte heran, datenschutzrechtlich beraten zu werden. Die Aufgabe der Beratung der verantwortlichen Stellen hat der HmbBfDI aufgrund von § 38 BDSG i.V.m § 24 HmbDSG. Diese Aufgabe können wir aufgrund der defizitären Personalausstattung nur in dem begrenzten Umfang wahrnehmen, den der enge Rahmen der vorhandenen personellen Kapazitäten ermöglicht.

Eine in dem gesetzlich vorgesehenen Rahmen durchgeführte Beratung hat zudem für die Unternehmen mitunter den Nachteil eines hohen Grades an Unsicherheit und mangelnder Verbindlichkeit. Fragen werden hier zumeist nur mündlich erörtert. Neue Geschäftsmodelle lassen sich in derartigen Verfahren aus Sicht der Unternehmen nicht in der für die Herstellung eines belastbaren Vertrauenstatbestands erforderlichen Dokumentationstiefe analysieren und bewerten.

Nicht zuletzt deshalb besteht häufig ein weitergehender Wunsch seitens der Wirtschaft und Teilen der öffentlichen Verwaltung nach rechtsverbindlicher Beratung, die insbesondere gegenüber Dritten verwendbare Ergebnisse, wie z.B. Gütesiegel oder Auditierungen, erbringen kann. Diesem Anliegen kann und darf der HmbBfDI aktuell aufgrund einer fehlenden Rechtsgrundlage nicht nachkommen. Das Defizit trifft vor allem Startup-Unternehmen sowie kleine und mittelständische Unternehmen mit neuen Ideen zu Geschäftsmodellen, die in der Regel keine oder nur sehr geringe Ressourcen für rechtliche Beratungen aufbringen können.

IT-Produkte und Dienstleistungen in einem rechtlich vorgegebenen Verfahren verbindlich überprüfen zu lassen, ist ein Anliegen, das für alle Akteure, die verantwortliche Stelle, ihre Kunden wie auch für die Aufsichtsbehörde Vorteile bringt:

Unternehmen können über Zertifizierungsverfahren das Thema Datenschutz freiwillig und selbstbestimmt ansteuern. Ein erfolgreiches Verfahren ermöglicht ihnen, ihre

Produkte offensiv zu bewerben und dadurch Vertrauen bei den Nutzern herzustellen.

Gerade im Bereich digitaler technischer Entwicklungen lassen sich allzu oft Risiken und Chancen durch die **Verbraucher** selbst nicht hinlänglich einschätzen. Durch Zertifizierungen werden Nutzer in die Lage versetzt, zwischen Nutzen und Risiken von IT-Produkten mit Blick auf den Schutz ihrer Privatsphäre abzuwägen.

Aus der Sicht der **Aufsichtsbehörden** wird mit der Möglichkeit der freiwilligen Auditierung durch Unternehmen eine Verbesserung des Datenschutzniveaus erreicht und damit der Vollzugsdruck gemindert.
Bislang hat die Hamburgische Wirtschaft keinen Ansprechpartner für Datenschutzfragen vor Ort, um Produkte, Verfahren oder Geschäftsmodelle in einem proaktiven Verfahren datenschutzrechtlich verbindlich beurteilen und bewerten zu lassen. Interessierte Stellen müssen für diese Leistungen auf Zertifikate anderer Länder (z.B. das Gütesiegel der Aufsichtsbehörde in Schleswig-Holstein) oder auf Angebote von privaten Stellen ausweichen, denen ganz unterschiedlich weit reichende Voraussetzungen zugrunde liegen. Für die öffentliche Verwaltung ist dieser Weg ohnehin versperrt.

Damit verbleiben die Unternehmen in der Situation, in der sie aufsichtsbehördliche Verfahren u.a. bei der Neuentwicklung von Verfahren und Geschäftsmodellen riskieren müssen, anstatt diesen durch die Vermeidung datenschutzrechtlicher Fehlentwicklungen vorab begegnen zu können. Denn Gütesiegel privater Unternehmen oder die Beratung anderer Aufsichtsbehörden binden den Hamburgischen Datenschutzbeauftragten in seiner aufsichtsbehördlichen Tätigkeit nicht. Zudem sind vor allem Startups sowie kleine Unternehmen nur selten aus betriebswirtschaftlicher Sicht in der Lage, eine qualifizierte kommerzielle Beratung finanzieren zu können. Insoweit besteht ein Bedürfnis nach einem Modell der freiwilligen Selbstkontrolle, wonach auf Antrag von Unternehmen IT-Produkte durch einen unabhängigen, von der Datenschutzbehörde anerkannten Sachverständigen überprüft und durch die Datenschutzbehörde ggfs. durch die Erteilung eines Siegels bewertet werden.

4.2 Das zweistufige Audit-Verfahren

Maßgebend für Beratung wie auch für Auditierungsverfahren ist nicht das klassische hierarchische Kontrollverfahren der Verwaltung. Vielmehr gilt es, private, aber auch öffentliche Stellen bei der Entwicklung und dem Einsatz von IT-Produkten zu unterstützen und zu fördern.

Der HmbBfDI besitzt die technische und rechtliche Sachkompetenz und Fachkunde für erweiterte Beratungsleistungen. Theoretisch besteht insoweit die Möglichkeit, diese Situation zugunsten der für die Datenverarbeitung verantwortlichen Stellen zu verbessern. Dazu wären i.W. folgende Instrumente erforderlich:

Durch eine Erweiterung der Kompetenzen und Aufgaben des HmbBfDI durch Änderung

des Hamburgischen Datenschutzgesetzes könnten verbindliche Beratungs- und Zertifizierungsleistungen angeboten werden. Dazu ist eine Änderung von Bundesrecht, insbesondere des Bundesdatenschutzgesetzes, nicht erforderlich. Die Aufgabenzuschreibung liegt in der Gesetzgebungszuständigkeit der Hamburgischen Bürgerschaft und ergibt sich vor dem Hintergrund einer Beratungsaufgabe der Datenschutzbehörde über den Einsatz datenschutzgerechter und sicherer IT-Produkte für die öffentlichen Stellen der Hamburgischen Verwaltung. Eine Vorrangklausel im Landesrecht, wonach zertifizierte Produkte durch öffentliche Stellen prioritär eingesetzt werden sollten, könnte dafür sorgen, dass dort künftig derartig geprüfte Angebote stärker nachgefragt werden.
Die EU-Datenschutzgrundverordnung sieht in Art. 39, Art. 39 a ebenfalls das Instrument der Zertifizierung vor. Der Regelung, die erst Mitte 2018 in Kraft treten dürfte, liegt jedoch ein weiter Umsetzungsspielraum zugrunde. Hiernach kann entweder die Zertifizierung durch eine akkreditierte Stelle, durch den Europäischen Datenschutzausschuss oder unmittelbar durch die nationale Aufsichtsbehörde selbst vorgenommen werden (Art. 39 Abs. 2a). Die nähere Ausgestaltung wird von der Datenschutzgrundverordnung offengelassen. Sie kann zum einen durch delegierte Rechtsakte der Kommission (Art. 39 a Abs. 7) oder – solange keine europaweiten Vorschriften erlassen werden – durch Ausgestaltung des nationalen Gesetzgebers erfolgen.

Die Einheitlichkeit im Rahmen des gemeinsamen Marktes, auch EU-weit einheitliche Zertifizierungsregeln zu haben, spricht langfristig für ein europäisches Verfahren. Ob und wann dies kommt, steht jedoch derzeit in den Sternen. Angesichts der großen Herausforderungen, die die Umsetzung des Projekts der Datenschutzgrundverordnung insgesamt darstellt, dürfte damit jedenfalls kurzfristig nicht gerechnet werden. Aus der Perspektive des Landesgesetzgebers sollte daher die Chance auf eine eigenständige Regelung nicht mit dem Blick auf eine theoretisch mögliche EU-Regelung ab frühestens Mitte 2018 ungenutzt bleiben. Dies gilt umso mehr, als ein funktionierendes System der Zertifizierung sich durchaus an verschiedene Rechtsvorgaben anpassen lässt und eine anschlussfähige nationale Regelung zunächst einmal wichtige praktische Erfahrungen und Fachkenntnisse generiert, die dann durch die Datenschutzbehörde weiter genutzt werden kann.

Inhaltlich könnten spezifische Regeln über die entsprechenden Beratungsleistungen und deren rechtliche Verbindlichkeit sowie die Ausgestaltung eines Gütesiegelverfahrens auf Landesebene normiert werden. Dies ist durch eine Verordnung möglich, soweit eine entsprechende Ermächtigungsgrundlage im Hamburgischen Datenschutzgesetz aufgenommen wird. Zudem müssten ein Kriterienkatalog für Zertifizierungen und ein entsprechender Gebührentatbestand für die Zertifizierung und Beratungsleistung geschaffen werden.

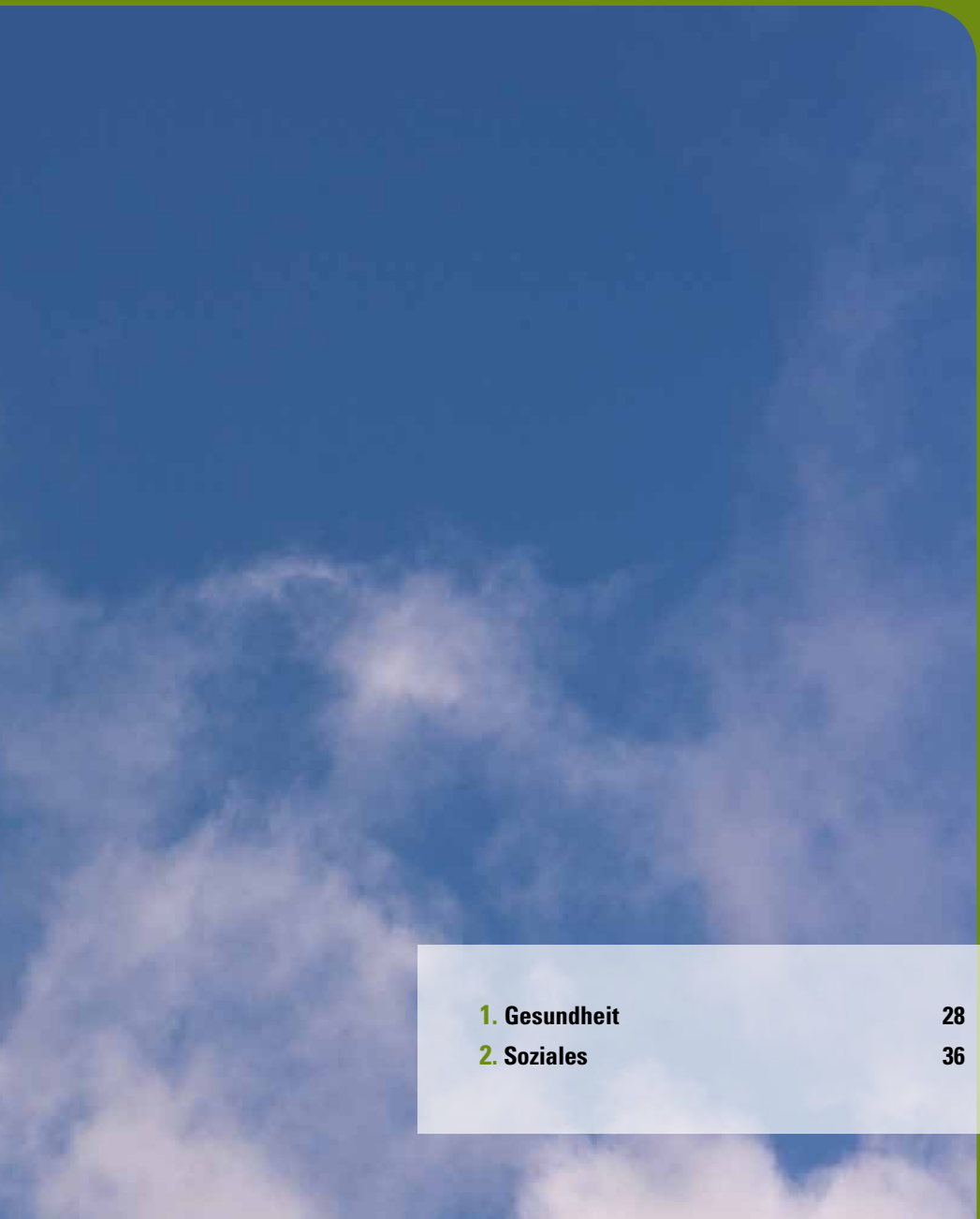
Der HmbBfDI müsste mit den erforderlichen sachlichen und personellen Ressourcen ausgestattet werden, um die neuen gesetzlichen Aufgaben durchführen zu können.

Dazu gehört z.B. die Erweiterung des Personals, um eine rechtsverbindliche, ressourcenintensive Beratung zu gestalten. Von großer Bedeutung ist dies vor allem für neue Geschäftsmodelle, bei denen nicht allein eine Bewertung bestehender Strukturen im Vordergrund steht, sondern z.B. alternative Handlungsstrategien entwickelt werden müssen, um die Umsetzung einer Geschäftsidee datenschutzkonform zu realisieren. Dies gilt im Übrigen auch vor dem Hintergrund, dass die Zertifizierung nicht mit dem Personal aus dem Bereich der aufsichtsbehördlichen Tätigkeit erfolgen sollte. Hier ist vielmehr eine strikte Aufgabentrennung erforderlich, da es sich bei den unterschiedlichen Aufgaben der Zertifizierung und Prüfung um grundsätzlich inkompatible Tätigkeiten handelt.
Die Zertifizierung von IT-Produkten und Dienstleistungen sollte zudem nicht unmittelbar durch den HmbBfDI vorgenommen werden. Vorzugswürdig ist ein zweistufiges Verfahren: Dabei wird das eigentliche Gutachten durch einen vom HmbBfDI zugelassenen und vom Unternehmen selbst gewählten Gutachter erstellt. Die Einhaltung der Zertifizierungsvoraussetzungen wird in einer zweiten Stufe durch den HmbBfDI durch Begutachtung des Zertifizierungsgutachtens gewährleistet und danach die Zertifizierung durch den HmbBfDI durchgeführt. Neben der Vermeidung von Interessenskollisionen auf Seiten der zertifizierenden Stelle ist dieses Verfahren ressourcenschonender für die öffentliche Hand.

Insgesamt dürfte eine derartige Zertifizierung ein Erfolgsmodell darstellen, das den Datenschutz mit dem Gedanken des Standort- und Wettbewerbsvorteils verknüpft. Es erscheint durchaus sinnvoll, die mögliche Chance hierzu zügig zu ergreifen und einen entsprechenden gesetzlichen Rahmen hierfür zu schaffen.


UNIVERSITÄT
HAMBURG
DER FORSCHUNG
I UKE

II. GESUNDHEIT UND SOZIALES



1. Gesundheit 28
2. Soziales 36

1. Gesundheit

1.1 Gesundheitsdienst-Datenverarbeitungsverordnung – GD-DVVO

Mit der GD-DVVO wurde die rechtliche Grundlage dafür geschaffen, dass die Dienststellen des öffentlichen Gesundheitsdienstes personenbezogene Daten in einem gemeinsamen IT-Verfahren verarbeiten können.

Mit Projekteinsetzungsverfügung vom 15. April 2010 wurde das Projekt „Standardsoftware für die Hamburger Gesundheitsämter" eingesetzt; Ziel war es, eine einheitliche IT-Lösung einzuführen, um hierdurch u.a. die Effektivität der Dienststellen des öffentlichen Gesundheitsdienstes zu steigern und eine zukunftsfähige Softwarelösung zu etablieren. Bis zum Jahre 2014 wurden bis zu 15 unterschiedliche IT-Verfahren zur technischen Unterstützung der dortigen Aufgabenerfüllung eingesetzt.

Ein wesentlicher Parameter der neuen Software sollte darin bestehen, dass eine bezirksübergreifende Stammdatensicht möglich ist, so dass z.B. in Fällen eines Umzuges der Betroffenen, eines Zuständigkeitswechsels oder einer bezirksübergreifenden Fallkonstellation keine redundante Stammdatenspeicherung erforderlich wird; hierdurch sollte gleichzeitig auch einer unkontrollierten Auseinanderentwicklung getrennter Stammdatenbestände entgegengewirkt werden. Demgegenüber verbleiben inhaltliche Informationen zu den jeweiligen Vorgängen allein in der Zugriffsberechtigung der fallbearbeitenden Behörde.

Bereits frühzeitig haben wir darauf hingewiesen, dass es für eine solche bezirksübergreifende Softwarelösung, bei der mehrere Dienststellen auf dieselben Stammdaten Zugriff haben, der ausdrücklichen Zulassung durch eine Rechtsvorschrift im Sinne des § 11a Abs. 1 Satz 1 Hamburgisches Datenschutzgesetz (HmbDSG) bedarf. Hintergrund ist, dass es sich bei den einzelnen Dienststellen des öffentlichen Gesundheitsdienstes jeweils um eigene Daten verarbeitende Stellen handelt.

Entscheidender Ansatzpunkt ist hierbei § 2 Abs. 1 Satz 1 Nr. 1 HmbDSG, der als „Stelle" auch die „Behörden" benennt. Eine weitergehende Definition erfolgt zwar nicht. In der Gesetzesbegründung ist hierzu aber ausgeführt, dass – wie das Hamburgische Verwaltungsverfahrensgesetz auch – von dem Begriff der Behörde als jener Stelle auszugehen ist, die selbständig und eigenverantwortlich Verwaltungshandlungen vornehmen kann (vgl. Bü.-Drs. 13/3282 zu § 2). Angesichts der Tatsache, dass zum einen die Bezirke gemäß Hamburgischem Bezirksverwaltungsgesetz ihre Aufgaben grundsätzlich selbständig durchführen und dass zum anderen die Dienststellen des öffentlichen Gesundheitsdienstes eigenverantwortlich Verwaltungshandlungen vornehmen, ergibt sich aus dieser Herleitung des Begriffs der Behörde, dass auch die Dienststellen des öffentlichen Gesundheitsdienstes als eigene Daten verarbeitende Stellen anzusehen

sind. Dies entspricht dem datenschutzrechtlich anerkannten funktionalen Behördenbegriff, der an der konkreten Aufgaben- und Zweckerfüllung zur Abgrenzung einzelner Daten verarbeitender Stellen ansetzt.
Die Behörde für Gesundheit und Verbraucherschutz hat unsere diesbezügliche Stellungnahme aufgegriffen und eine Verordnung über die gemeinsame Verarbeitung von Daten des öffentlichen Gesundheitsdienstes erstellt, die den Anforderungen des § 11a HmbDSG entspricht.

1.2 UKE – Forschung

Das Universitätsklinikum Hamburg-Eppendorf (UKE) entwirft ein Grundkonzept, das den Forscherinnen und Forschern die datenschutzkonforme Ausgestaltung ihrer jeweiligen Forschungsprojekte erleichtern soll. Leider sind wir personell derzeit nicht in der Lage, die Vielzahl bereits existierender Bio-/Datenbanken im UKE datenschutzrechtlich zu überprüfen.

Die medizinische Forschung ist eine der wesentlichen Aufgaben des UKE. Regelmäßig werden wir bei der datenschutzrechtlichen Bewertung beteiligt. Hierzu prüfen wir die jeweiligen, von den Forscherinnen und Forschern bereits erstellten Forschungskonzepte bzw. Studienprotokolle; anschließend weisen wir die jeweiligen Forscherinnen und Forscher auf Änderungsbedarfe und datenschutzkonforme Lösungen hin. Hierbei wurde zunehmend deutlich, dass allgemein gültige datenschutzrechtliche Aspekte oftmals für jedes Forschungsvorhaben erneut dargestellt und deren Implementierung und Beachtung veranlasst werden mussten. In einem Gespräch mit dem Forschungsdekanat des UKE haben wir daher die Erstellung eines datenschutzrechtlichen Grundkonzeptes angeregt, das den Forscherinnen und Forschern als individuell anzupassende Grundlage für eine datenschutzkonforme Ausgestaltung ihrer Vorhaben dienen soll. Ziel soll es sein, dass die Berücksichtigung datenschutzrechtlicher Anforderungen gewährleistet und deren Anwendung sichergestellt ist; gleichzeitig dürfte dies auch zu einer schnelleren Umsetzung von Forschungsideen führen, da die bisher teilweise erforderlichen umfangreichen datenschutzrechtlichen Anpassungsarbeiten entfallen könnten.

Das UKE hat unsere Anregung aufgenommen und erstellt derzeit ein entsprechendes Konzept. Um auch sicherzugehen, dass die Forscherinnen und Forscher das erstellte Konzept zur Kenntnis nehmen werden, plant das UKE, einen kurzen Film zu erstellen, in dem den zukünftigen Anwenderinnen und Anwendern die datenschutzrechtliche Notwendigkeit und der Nutzen vorgestellt werden sollen.

Leider ist es uns neben diesem strukturellen Fortschritt jedoch nicht möglich, auch nur ansatzweise die erforderlichen Prüfungen in konkreten Anwendungsfällen der medizinischen Forschung durchzuführen. Dies betrifft insbesondere den großen Bereich der Bio-/Datenbanken:

Die in Bio-/Datenbanken gesammelten Gesundheitsdaten bilden oftmals über Jahre hinweg ein gesundheitliches Profil des Betroffenen ab. Hinzu kommt, dass die gesammelten Bioproben meistens dazu geeignet sind, das gesamte Genom des Betroffenen und damit einen unveränderlichen Teil der Identität zu entschlüsseln. Kommt es bei dem Betrieb einer Bio-/Datenbank zu Datenschutzverletzungen, z.B. durch den Zugriff Unbefugter auf die Daten und das genetisch auswertbare Material, entstehen hierdurch erhebliche Beeinträchtigungen der Rechte und schutzwürdigen Interessen der Betroffenen einerseits und ein enormer Schaden für den Forschungsstandort Hamburg andererseits. Eine Überprüfung der existierenden Bio-/Datenbanken UKE muss jedoch wegen fehlender personeller Kapazitäten bereits seit Jahren stetig vertagt werden. Hieran wird beispielhaft die dringende Notwendigkeit deutlich, unsere Behörde mit ausreichenden personellen Kapazitäten auszustatten.

1.3 UKE – Hamburg City Health Studie

Das Universitätsklinikum Hamburg-Eppendorf (UKE) startet eine hamburgweite Beobachtungsstudie zu häufigen Volksleiden; nachdem wir zuvor jahrelang die Studienkonzeptionierung datenschutzrechtlich begleitet haben, wurde ein Studienkonzept entwickelt, das die Belange des Datenschutzes und der Forschung berücksichtigt.

Das UKE hat sich entschlossen, eine hamburgweite Beobachtungsstudie durchzuführen, durch die ein besseres Verständnis von Häufigkeiten, Ursachen und Verlauf von Erkrankungen erlangt werden soll. Zu diesem Zweck sollen rund 45.000 Bürgerinnen und Bürger untersucht werden, um Risikofaktoren für die häufigsten Volksleiden (Herz-Kreislauf-Erkrankungen, Schlaganfall, Demenz und Krebserkrankungen) und Todesursachen zu identifizieren. Datenschutzrechtlich ist dabei zu beachten, dass die Teilnehmerinnen und Teilnehmer zwar keine Patientinnen und Patienten sind, es sich bei deren Informationen aber dennoch um Gesundheitsdaten mit einem hohen Schutzbedarf handelt.

Über einen Zeitraum von mehr als zwei Jahren standen wir in Kontakt mit dem UKE, um die datenschutzrechtliche Planung dieser Hamburg City Health Studie zu begleiten. Die Studie wird umfassend von fast 30 Kliniken und Instituten des UKE einschließlich des Universitären Herzzentrums und der Martini-Klinik durchgeführt. Neben einer Vielzahl von medizinischen Untersuchungen gehört zu diesem Forschungsvorhaben auch die genetische Untersuchung von Blut und sonstigem Biomaterial sowie deren Sammlung in einer Biomaterialbank. Über mehrere Jahre und Jahrzehnte hinweg sollen hier personenbezogene Daten verarbeitet werden. Hinzu kommt die Erweiterung des auszuwertenden Datenmaterials dadurch, dass Informationen auch von dritter Seite hinzugezogen werden sollen, z.B. von Hausärztinnen und Hausärzten, Fachärztinnen und Fachärzten, Krankenhäusern, aber auch von der Krankenversicherung, Rentenversiche-

rung und dem Krebsregister. Hierneben kooperiert das UKE in diesem Zusammenhang mit weiteren Partnern, so dass die Daten ggf. auch international verarbeitet werden. Unsere datenschutzrechtliche Begleitung beinhaltete hier eine detaillierte Betrachtung der einzelnen Datenverarbeitungsschritte von der Datenerhebung über die Speicherung bis hin zur Nutzung bzw. Übermittlung an andere Stellen. Kern der datenschutzrechtlichen Sicherung personenbezogener Daten ist ein umfangreiches und weit verzweigtes Pseudonymisierungsverfahren, das seinerseits technisch unterstützt ist. Hier wird sichergestellt sein, dass die Forscherinnen und Forscher auf der Grundlage einer wirksamen Einwilligung zwar die erforderlichen Daten nutzen können; die jeweilige konkrete Person der Studienteilnehmerin bzw. des Studienteilnehmers ist jedoch für die Forschungstätigkeit nicht von Bedeutung, so dass hier mittels Pseudonymisierung die Kenntnis von Namen und sonstigen direkt identifizierenden Informationen der Studienteilnehmerinnen und Studienteilnehmer ausgeschlossen wird. Nach über zwei Jahren intensiver Diskussionen mit dem UKE genügt das Studiendesign nun einerseits datenschutzrechtlichen Anforderungen und berücksichtigt andererseits auch die Forschungsinteressen. Nun muss das UKE die datenschutzrechtlichen Anforderungen in der Praxis umsetzen, damit der Schutz der hoch sensiblen Gesundheitsdaten auch realisiert wird. Korrespondierend hierzu wurde die erforderliche Einwilligungserklärung formuliert.

1.4 MDK Nord – Verlust eines Laptops

Nachdem beim Medizinischen Dienst der Krankenversicherung Nord (MDK Nord) ein Laptop mit personenbezogenen Sozialdaten abhandengekommen war, führte der MDK Nord auf unsere Veranlassung hin eine Festplattenverschlüsselung ein.

Führen Gutachterinnen und Gutachter des MDK Nord externe Begutachtungen durch, führen sie Papierakten und ggf. einen Laptop mit sich, um Erkenntnisse direkt speichern zu können. Im Dezember 2014 kam ein Rucksack samt Laptop und Papierakten abhanden. Der MDK Nord zeigte uns gemäß § 83a Zehntes Buch Sozialgesetzbuch (SGB X) den Verlust an und erläuterte hierzu unter anderem, dass auf dem Laptop wahrscheinlich die Begutachtungen von 20 stationären Fällen gespeichert waren und hierneben auch 16 Papierakten betroffen waren. Inhalt waren z.B. Krankenhausentlassungsberichte oder auch die Dokumentation eines gesamten Krankenhausaufenthaltes. Bei diesen personenbezogenen Daten handelt es sich nicht nur um sensible Gesundheitsdaten, sondern auch um Sozialdaten und somit insgesamt um besonders schützenswerte Informationen der betroffenen Patientinnen und Patienten.

Wir wiesen den MDK Nord darauf hin, dass § 83a SGB X neben einer Mitteilung an die Datenschutzaufsichtsbehörde auch die Information der Betroffenen vorsieht, wenn

besondere Arten personenbezogener Daten (§ 67 Abs. 12 SGB X) Dritten unrechtmäßig zur Kenntnis gelangt sind und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Gerade bei einem Verlust von Laptops und Akten liegen tatsächliche Anhaltspunkte dafür vor, dass Dritte mit hoher Wahrscheinlichkeit Kenntnis von den Sozialdaten nehmen können. Auch wenn ein Softwareprogramm mittels Passwort geschützt ist, können die Sozialdaten dennoch ausgelesen werden, wenn nicht eine hinreichend sichere Festplattenverschlüsselung genutzt wird; dies war vorliegend nicht der Fall. Daher sahen wir die Notwendigkeit der Benachrichtigung auch hinsichtlich der auf dem Laptop gespeicherten Sozialdaten.

Der MDK Nord teilte uns anschließend mit, dass die Betroffenen ebenfalls über den Verlust der Sozialdaten informiert wurden; deren Nachfragen konnten allesamt zufriedenstellend beantwortet werden. Somit hat der MDK Nord seine Informationspflicht nach § 83a SGB X erfüllt.

Hierneben musste der MDK Nord sich aber um diejenigen Mängel kümmern, durch die sich im geschilderten Vorfall die unrechtmäßige Kenntniserlangung durch Dritte realisieren konnte: die fehlende Festplattenverschlüsselung. Der MDK Nord führte umgehend eine Pilotierung auf unterschiedlichen Rechnern durch, um die Wirksamkeit und Handhabbarkeit einer Festplattenverschlüsselung zu testen. Anschließend wurde die Verschlüsselung der Laptop-Festplatten veranlasst. Datenschutzfreundliche Folge hiervon ist zugleich, dass die Sozialdaten nicht nur im Falle eines Verlustes des Laptops oder des Ausbaus der Festplatte geschützt sind, sondern dass auch die IT-Abteilung des MDK Nord selbst keine Zugriffsmöglichkeiten mehr auf die verschlüsselten Sozialdaten hat.

1.5 MDK Nord – Mailverkehr mit Krankenkassen

Der Medizinische Dienst der Krankenversicherung Nord (MDK Nord) veranlasst anlässlich einer Überprüfung durch uns die Verschlüsselung der E-Mail-Kommunikation mit seinen Auftraggebern.

Anlässlich einer Bürgereingabe und der damit verbundenen Prüfung des MDK Nord wurden wir darauf aufmerksam, dass der MDK Nord personenbezogene Sozialdaten per Fax an die jeweilige Krankenkasse übermittelte. Zunächst stand die Frage im Mittelpunkt, inwieweit ein Faxversand erforderlich war; hierzu haben wir grundsätzliche Anforderungen bereits im 24. Tätigkeitsbericht (vgl. 24. TB, III 5.13) dargestellt. Während der Prüfung stellte sich heraus, dass der Faxversand zumindest zum Teil aber auch per E-Fax erfolgt.

Aus technischer Sicht ist eine unverschlüsselte E-Fax-Kommunikation ebenso unsicher wie eine unverschlüsselte E-Mail-Kommunikation; dies ist das Ergebnis einer weiteren von uns durchgeführten Prüfung (vgl. VI. 1.1). Auch wenn die Datenübermittlung an sich zulässig ist, bedarf es daher technischer Sicherungsmaßnahmen, die gewährleisten, dass die Sozialdaten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (vgl. Satz 2 Nr. 4 der Anlage zu § 78a SGB X). Erfolgt davon abweichend jedoch eine unverschlüsselte Kommunikation, kann gerade nicht ausgeschlossen werden, dass auch Unbefugte den Inhalt der Kommunikation zur Kenntnis nehmen können.

Wir wiesen den MDK Nord daher darauf hin, dass bei der Nutzung von elektronischen Kommunikationswegen eine Verschlüsselung dringend geboten ist, zumal es sich vorliegend um Gesundheits- und Sozialdaten der Betroffenen handelt. Ebenso legten wir die Entschließung „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. März 2014 vor, die unter anderem diese technische Anforderung auch an die öffentlichen Stellen richtet. Hieraufhin teilte uns der MDK Nord Mitte 2015 mit, dass die Nutzung einer verschlüsselten E-Mail-Kommunikation in der Zusammenarbeit mit den Auftraggebern forciert werde und bereits mit den ersten fünf größeren Krankenkassen eine verschlüsselte Leitung eingerichtet wurde. Bis November 2015 hat der MDK Nord die Möglichkeit geschaffen, bereits mit 56 Krankenkassen mittels verschlüsselter E-Mail zu kommunizieren. Kontinuierlich kommen weitere Krankenkassen hinzu.

Da der MDK Nord seinerseits zum Teil an enge Fristen für die Erledigung seiner Aufträge gebunden ist, stellt die Möglichkeit, Informationen per E-Mail zu versenden, einen alltäglichen Kommunikationsweg dar. Dadurch, dass der MDK Nord unkompliziert die Verschlüsselung der elektronischen Kommunikation weiter vorantreibt, konnten wir anlässlich unserer Prüfung erreichen, dass der MDK Nord mit dieser vergleichsweise einfachen technischen Maßnahme die Gewährleistung des informationellen Selbstbestimmungsrechtes einer Vielzahl von Bürgerinnen und Bürgern sicherstellt.

1.6 National Single Window / Hafenärztlicher Dienst

Die Erhebung von personenbezogenen Daten, insbesondere auch von Gesundheitsdaten durch Hamburger Stellen beim National Single Window (NSW) setzt datenschutzrechtliche Regelungen voraus, auf deren Grundlage eine Datenerhebung bei einer dritten Stelle zulässig ist.

Bisher war die Schifffahrt verpflichtet, vor dem Anlaufen eines deutschen Hafens bestimmte Daten an verschiedene Stellen zu übermitteln. Hierbei handelt es sich u.a. um Informationen nach der Hafenverkehrsordnung, der Gefahrgut- und Brandschutzver-

ordnung und der Durchführungsverordnung zum Hafensicherheitsgesetz; hinzu kommt eine Seegesundheitserklärung nach dem Gesetz zur Durchführung der Internationalen Gesundheitsvorschriften, die bei Bedarf Gesundheitsdaten von Passagieren oder Besatzungsmitgliedern beinhaltet. Um diese unterschiedlichen, zum Teil auch redundanten Datenlieferungen für den Seeverkehr zu erleichtern, wurde die Richtlinie 2010/65/EU des Europäischen Parlamentes und des Rates erlassen, die die Meldeformalitäten für Schiffe beim Einlaufen in Häfen regelt. Auf dieser Grundlage sind die Mitgliedsstaaten verpflichtet, es bis zum 1. Juni 2015 der Schifffahrt zu ermöglichen, sämtliche für einen Mitgliedsstaat bestimmte Daten nur an eine einzige Stelle – das NSW – übermitteln zu können, die ihrerseits die Daten den zuständigen Stellen weiterleitet. Diese Stelle ist beim Bund eingerichtet worden; für die zuständigen Hamburger Stellen sind Schnittstellen eingerichtet worden.

Ende 2014 wurden wir von den zuständigen Hamburger Stellen eingebunden, da es sich bei den durch das NSW verarbeiteten Informationen zum Teil auch um personenbezogene Daten handelt. Datenschutzrechtlich ist hierbei darüber hinaus zu beachten, dass die zuständigen Hamburger Stellen die erforderlichen Daten zukünftig nicht mehr direkt bei den Schifffahrtsunternehmen erheben, sondern bei einer dritten Stelle, dem NSW. Wir wiesen daher darauf hin, dass es entsprechender Rechtsgrundlagen gerade auch für die geplante Datenverarbeitung zwischen dem NSW und den Hamburger Stellen bedarf. Hier sehen wir in erster Linie den Bundesgesetzgeber in der Pflicht, auch die erforderlichen datenschutzrechtlichen Grundlagen für die Tätigkeit des NSW zu schaffen.

Da absehbar war, dass bis zum europarechtlich vorgesehenen Start keine bundesgesetzliche Regelung verabschiedet war, die auch datenschutzrechtliche Aspekte beinhaltet, haben wir den Hamburger Stellen empfohlen, zumindest im Rahmen der Gesetzgebungskompetenz der Freien und Hansestadt Hamburg (FHH) datenschutzrechtliche Regelungen zu schaffen, auf deren Grundlage eine Datenerhebung beim NSW zulässig ist. Unserer Empfehlung folgend wurden die oben genannten drei Verordnungen entsprechend angepasst; sie enthalten nunmehr jeweils auch eine Grundlage für die Datenerhebung beim NSW.

Im Hinblick auf die Verarbeitung von Gesundheitsdaten konnte die FHH jedoch selbst keine entsprechenden Regelungen schaffen. Insoweit wurde von der Behörde für Gesundheit und Verbraucherschutz die „Bekanntmachung der Zulassung eines elektronischen Übermittlungsweges für die Abgabe der Seegesundheitserklärung von Seeschiffen“ veröffentlicht. In der dortigen Ziffer 3 ist festgelegt:

„Die Übermittlung der Seegesundheitserklärung an das Einzige Nationale Fenster - NSW - setzt voraus, dass alle Gesundheitsfragen der Seegesundheitserklärung mit „nein“ beantwortet wurden und insofern keine Veranlassung besteht, den „Anhang zur Gesundheitserklärung“ auszufüllen. Anderenfalls sind die Seegesundheitserklä-

rung einschließlich des Anhangs zur Gesundheitserklärung durch den Schiffsführer ausschließlich per Telefax oder E-Mail direkt an den Hafen- und Flughafenärztlichen Dienst des Hamburg Port Health Centers oder seinen Beauftragten zu übermitteln."

Hierdurch wird übergangsweise sichergestellt, dass nur dann ein Informationsfluss über das NSW erfolgt, wenn sämtliche Gesundheitsfragen mit „nein" zu beantworten sind. Sind hingegen personenbezogene Gesundheitsdaten zu übermitteln, muss dies direkt gegenüber dem Hafenärztlichen Dienst erfolgen. Somit erfolgt derzeit in diesen Fallgestaltungen keine Erhebung gesundheitlicher und damit sensibler Daten bei Dritten.

Mittlerweile soll der Entwurf eines entsprechenden Bundesgesetzes existieren. Uns wurde zugesagt, dass wir im Rahmen der Länderbeteiligung ebenfalls einbezogen werden; wir werden auch in diesem Rahmen die von uns für erforderlich gehaltenen datenschutzrechtlichen Regelungen einfordern.

1.7 UKE – Auswertung der Zugriffe auf die elektronische Patientenakte

Auch wenn das Universitätsklinikum Hamburg-Eppendorf (UKE) bei der anlassunabhängigen Auswertung der Protokolldaten zu den Notzugriffen auf dem richtigen Weg ist, fehlt es leider weiterhin gänzlich an einer solchen Auswertung hinsichtlich der Normalzugriffe auf die elektronische Patientenakte.

Bereits in den vergangenen Tätigkeitsberichten (zuletzt: 24. TB, III 5.3) haben wir über die Auswertung der Protokolldaten bei Notzugriffen berichtet; bestimmten Berufsgruppen steht hierbei ein Zugriff auf die elektronische Patientenakte außerhalb der eigenen Zugriffsberechtigung zu. Die bisher dargestellte positive Tendenz der gesunkenen Zugriffshäufigkeit hat sich im Berichtszeitraum verfestigt. Anhand der Protokollauswertungen für den Notzugriff ergeben sich immer wieder Anhaltspunkte dafür, dass z.B. nach einer personellen Entscheidung (Neueinstellung oder Versetzung) die Zugriffsberechtigung angepasst werden muss.

An die Auswertung der Protokolldaten müssen sich bei Auffälligkeiten weitere Maßnahmen anschließen: So sind die betroffenen Mitarbeiterinnen und Mitarbeiter danach zu befragen, inwieweit der Zugriff für die Erfüllung ihrer dienstlichen Aufgaben erforderlich war. Verbleiben danach Zweifel an der Zulässigkeit des Zugriffs, muss dies weiter erforscht und bewertet werden; ggf. müssen sich weitere Maßnahmen anschließen wie z.B. gemäß § 42a Bundesdatenschutzgesetz (BDSG) die Information unserer Behörde und derjenigen Patientinnen und Patienten, die von einem unzulässigen Zugriff betroffenen sind. Während einzelne Aspekte dieses Prozesses vom UKE erfüllt wurden, mussten wir die konsequente Analyse und Bewertung der datenschutz-

rechtlichen Zulässigkeit bei zweifelhaften Einzelfällen als Folgemaßnahme zur Protokollauswertung in der Vergangenheit anmahnen. Das UKE hat zwischenzeitlich eine zusätzliche Vollzeitstelle geschaffen, die diesen datenschutzrechtlich erforderlichen Prozess weiter vorantreiben soll.

Neben den Notzugriffen wird auch jeder normale Zugriff auf die elektronische Patientenakte protokolliert. Diese Protokolldaten wurden bisher zwar anlassbezogen ausgewertet, wenn der Verdacht eines missbräuchlichen Zugriffs im Raume stand; eine anlassunabhängige, routinemäßige Auswertung erfolgte bisher jedoch nicht. Auch eine solche Auswertung ohne vorausgehenden Anlass ist aber erforderlich, da ggf. erst hierdurch fehlerhafte Zugriffe ermittelt werden und sich die oben geschilderten Maßnahmen anschließen können. Nur so kann eine Daten verarbeitende Stelle ihrer datenschutzrechtlichen Verantwortung für die Zulässigkeit der internen Datenverarbeitung gerecht werden. Wir haben daher bereits mehrfach gegenüber dem UKE darauf gedrungen, auch die Protokollauswertung der Normalzugriffe durchzuführen. Laut Aussage des UKE scheitert diese Auswertung bisher daran, dass der nicht-wissenschaftliche Personalrat die hierfür erforderliche Dienstvereinbarung nicht unterschreibe; das UKE sei mehrfach auf den nicht-wissenschaftlichen Personalrat zugegangen, um ihm die datenschutzrechtliche Notwendigkeit auch der anlassunabhängigen Protokollauswertung zu erläutern. Wie uns in der letzten Besprechung mit dem UKE im November 2015 mitgeteilt wurde, liegt es ebenfalls in der Zuständigkeit der neuen Vollzeitkraft im UKE, die Voraussetzungen für die Auswertung der Normalzugriffe einschließlich der Dienstvereinbarung unverzüglich zu schaffen und den Auswertungsprozess umzusetzen. Aus diesem Grunde sehen wir vorerst noch von einer förmlichen Beanstandung ab, solange diese Aktivitäten im ersten Halbjahr 2016 sichtbare Erfolge bringen.

2. Soziales

2.1 JUS-IT – keine integrierte Jugend- und Sozialarbeit in Hamburg

Statt eines gemeinsamen Verfahrens werden separate IT-Lösungen für die Bereiche Jugend, Soziales und Wohngeld realisiert.

Das Projekt JUS-IT hatte den Auftrag, die Entwicklung einer weitgehend integrierten Softwarelösung für die Bereiche Jugend, Soziales und Wohnen unter der Berücksichtigung der Organisation der Sozialen Dienstleistungszentren fachlich, organisatorisch und unter Absicherung der erforderlichen Ressourcen umzusetzen. Mit Hilfe der neuen IT-Lösung sollte ein integriertes Eingangs- und Fallmanagement für diese Aufgabenfelder unterstützt und die Geschäftsprozesse aus einem Guss bearbeitet werden. Damit

wurden u. a. die Ziele verfolgt, die kundenzentrierte Hilfestellung unter dem Stichwort „Integrierte Hilfe“ zu verbessern, die Bearbeitung zu vereinfachen und durch eine Entlastung von Verwaltungstätigkeiten die kundenbezogene Betreuungskapazität zu erhöhen.

Wir haben von Beginn an darauf hingewiesen, dass die Nutzung einer gemeinsamen Datenbasis für die unterschiedlichen Aufgabenbereiche rechtlich nur zulässig ist, wenn die Voraussetzungen, die hierfür im Sozialgesetzbuch festgeschrieben sind, eingehalten werden (Vgl. 23. TB, III 7.1). Nach der Ablösung der IT-Lösung im Bereich Jugend und bei der Konzeptionierung des Bereichs Soziales gewann die Beantwortung der Fragen immer mehr an Bedeutung, ob eine gemeinsame Stammdatenbasis für diese Bereiche und die damit verbundenen Übermittlungen in den jeweils anderen Bereich durch die Vorschriften des Sozialgesetzbuches (SGB) datenschutzrechtlich zulässig sind und ob die Voraussetzungen bestehen, diese Daten nicht bei den Betroffenen direkt zu erheben. Hierzu haben wir auch in diesem Berichtszeitraum mit dem Projekt wieder intensive Gespräche geführt.

Dabei konnte das Projekt die Erforderlichkeit dieser Informationsaustausche ohne Mitwirkung der Betroffenen in der Mehrzahl weder nachweisen, noch anhand von Fallzahlen aus ausgewählten Pilotbereichen plausibel darlegen. Überlegungen, die Integrierte Hilfe gesetzlich zu verankern, wurden vom Projekt bisher nicht weiter verfolgt. Auch konnten wir deutlich machen, dass dem Direkterhebungsgebot nach § 67a Abs. 3 SGB X beispielsweise im Zuge der Antragstellung mit milderen Mitteln entsprochen werden kann, ohne zusätzlich das informationelle Selbstbestimmungsrecht der Betroffenen zu beeinträchtigen. Vor diesem Hintergrund hat das Projekt eine Anforderungsspezifikation erstellt, durch welche technischen Maßnahmen die IT-Lösung der Bereiche Jugend und Soziales getrennt werden sollen. Diese Spezifikation werden wir weiterhin zur Grundlage unserer Beurteilung machen, sofern mehrere Bereiche innerhalb einer IT-Lösung verarbeitet werden sollen.

2.2 Klientendaten von Mitarbeiterinnen und Mitarbeitern in JUS-IT

Die Sicht auf die Stammdaten von Mitarbeiterinnen und Mitarbeitern eines Jugendamtes, die zugleich selber auch Klientinnen und Klienten eines Jugendamtes sind, ist in der hamburgweiten Stammdatensicht in JUS-IT nicht eingeschränkt, so dass Kolleginnen und Kollegen im „eigenen“ Jugendamt diese Tatsache „Klient“ erkennen können. Eine Verbesserung des Datenschutzes scheitert derzeit an fehlenden finanziellen Ressourcen.

Sind Beschäftigte eines bezirklichen Jugendamtes zugleich selbst auch Klientinnen und Klienten des Jugendamtes, ist organisatorisch festgelegt, dass diese Angelegen-

heit im Jugendamt eines anderen Bezirksamtes bearbeitet wird. Die Dokumentation des Falles erfolgt in JUS-IT; die Kolleginnen und Kollegen dieser Beschäftigten haben keinen Zugriff auf die Inhaltsdaten zum Fall.

Mehrere Beschäftigte von Jugendämtern haben sich an uns gewandt, da über die hamburgweite Stammdatensicht in JUS-IT die Kolleginnen und Kollegen dennoch die Stammdaten dieser Beschäftigten – bestehend u.a. aus Name, Vorname, Geburtsdatum und Adresse – sowie die Zuordnung zu bestimmten Falltypen einsehen können. Insofern können Kolleginnen und Kollegen Informationen über betroffene Beschäftigte und Anhaltspunkte über deren Kontakt mit einem Jugendamt erhalten. Nach unserer Recherche war eine solche Suche auch vor JUS-IT bereits möglich. Unseres Erachtens stellt sich dennoch die Frage, warum sich die eingangs dargestellte organisatorische Entscheidung, die Fallbearbeitung in einem anderen Bezirksamt durchzuführen, nicht auch in der Stammdatensicht bei JUS-IT wiederfindet. Dies könnte z.B. dadurch realisiert werden, dass die Berechtigung für den Zugriff auf die Stammdaten in solchen Fällen, in denen die Klientinnen oder Klienten gleichzeitig Beschäftigte eines Jugendamtes sind, nur dem jeweils fallbearbeitenden Jugendamt zugewiesen ist. Hierdurch kann auch eine Verwechselungsgefahr ausgeräumt werden: Bei der fachlichen Dokumentation in JUS-IT wurden in der Vergangenheit bereits versehentlich die privaten Klienten-Daten von Beschäftigten verwendet, obwohl diese im konkreten Fall als Beschäftigte des Jugendamts tätig geworden sind.

Daher baten wir die Fachliche Leitstelle um Prüfung, inwieweit dem Datenschutz durch eine eingeschränkte Freischaltung der Stammdatensicht besser Rechnung getragen werden kann. Die Fachliche Leitstelle teilte uns mit, dass auch sie eine besondere Schutzwürdigkeit dieser Daten sieht und technische Umsetzungsmöglichkeiten prüfen werde. Nachdem uns zwischenzeitlich in Aussicht gestellt wurde, dass diese Prüfung im Rahmen der Analyse zum Release 2.3 mit dem Ziel April 2016 erfolgen werde, haben wir nun erfahren, dass mangels finanzieller Ressourcen die Analyse möglicher Lösungen derzeit zurückgestellt wurde; ggf. könne eine entsprechende Umsetzung im Rahmen des geplanten Projekts zur Erstellung einer Lösung für den Bereich Wohngeld eingeplant werden, da in diesem Zusammenhang eine Anpassung der Fall- und Personensuche erfolgen müsse. Wir werden weiterhin auf eine Verbesserung des Datenschutzes hinwirken und erneut berichten.

2.3 Berichtswesen SHA

Das Berichtswesen konnte letztlich datenschutzfreundlich so ausgestaltet werden, dass die Daten der Betroffenen von den einzelnen Trägern ohne einzelfallbezogenes Pseudonym an den öffentlichen Jugendhilfeträger übermittelt werden; das informationelle Selbstbestimmungsrecht der Betroffenen konnte hierdurch stärker geschützt werden.

Im Rahmen der Globalrichtlinie „Sozialräumliche Angebote der Jugend- und Familienhilfe" prüft der öffentliche Jugendhilfeträger die Erreichung der Ziele wie z.B. die Entwicklung von bedarfsgerechten Angeboten, um Anpassungen vorzunehmen und die Angebotsstruktur weiterzuentwickeln. Grundlage ist die Erfassung der Daten kommunaler und freier Träger in einem entsprechenden Bericht.

Anlässlich der Prüfung in einem Jugendamt wurden wir auf die Berichterstattung der Leistungsbereiche „Sozialräumliche Hilfen und Angebote" (SHA) aufmerksam gemacht verbunden mit der Frage, ob die Datenerhebung des öffentlichen Jugendhilfeträgers datenschutzrechtlich vor dem Hintergrund zulässig ist, dass die Datenlieferung derzeit über die Lawaetz-Stiftung – eine gemeinnützige Stiftung des bürgerlichen Rechts – durchgeführt wird. In einer Besprechung u.a. mit Vertretern der Behörde für Arbeit, Soziales, Familie und Integration und der Lawaetz-Stiftung wurde klargestellt, dass es sich bei den seinerzeit von den Trägern gelieferten Informationen um personenbezogene Daten handelt; über eine eigene Teilnehmernummer war ein Personenbezug vorgesehen, um Rückfragen beim Träger zu ermöglichen und die Anzahl der Betroffenen mehrerer Hilfeleistungen ermitteln zu können. Die Lawaetz-Stiftung konnte für den öffentlichen Jugendhilfeträger als Auftragsdatenverarbeiter tätig werden. Als Rechtsgrundlage für die Erhebung personenbezogener Daten kam §§ 62, 64 Abs. 3 i.V.m. § 80 Achtes Buch Sozialgesetzbuch (SGB VIII) in Betracht; die Jugendhilfeplanung gehört ausdrücklich zu den Aufgaben des Trägers der öffentlichen Jugendhilfe und beinhaltet u.a., den Bedarf zu ermitteln und die zur Befriedigung dieses Bedarfs notwendigen Vorhaben rechtzeitig und ausreichend zu planen. Eine fortlaufende Verknüpfung der Daten zu Profilen musste jedoch angesichts des Grundsatzes der Erforderlichkeit und der in § 64 Abs. 3 SGB VIII gesetzlich festgelegten Anonymisierungspflicht ausgeschlossen sein, da es insoweit nicht auf den einzelnen Hilfefall an sich ankommt.

Im Ergebnis hat die Lawaetz-Stiftung schließlich ein Konzept vorgelegt, bei dem die personenbezogenen Daten der Betroffenen lokal beim jeweiligen freien Träger gespeichert werden; für die Berichtszwecke werden die für den jeweiligen Berichtszeitraum relevanten Daten bereits beim freien Träger anonymisiert und erst dann zu festgelegten Zeitpunkten verschlüsselt übertragen. Somit konnte ein Berichtswesen erstellt werden, das dem Planungsinteresse der Fachbehörde einerseits und dem Datenschutz der Betroffenen andererseits gerecht wird.

2.4 Prüfung ASD – unverschlüsselter Mail-Versand

Es werden regelmäßig unverschlüsselte E-Mails mit personenbezogenen Sozialdaten an Betroffene und freie Träger versendet. Die erforderliche Möglichkeit einer E-Mail-Verschlüsselung bei der Kommunikation mit externen Stellen wird bislang von der Freien und Hansestadt Hamburg nicht zentral bereitgestellt.

Anlässlich der Eingabe eines Bürgers, der eine unverschlüsselte E-Mail von einem Fachamt Jugend- und Familienhilfe erhalten hatte, führten wir am 9. Dezember 2014 eine Prüfung der E-Mail-Kommunikation eines Allgemeinen Sozialen Dienstes (ASD) mit Externen durch. Beinhaltet eine E-Mail personenbezogene Daten, sind im Rahmen der Tätigkeiten eines Fachamtes Jugend- und Familienhilfe in der Regel Sozialdaten und damit Informationen mit hohem Schutzbedarf betroffen.

Bei einer an sich rechtlich zulässigen Datenübertragung sind die gesetzlichen Anforderungen zu beachten, die den Schutz des informationellen Selbstbestimmungsrechtes während der Datenverarbeitung gewährleisten sollen. Hierzu gehören die technischen und organisatorischen Maßnahmen gem. der Anlage zu § 78a Zehnten Buch Sozialgesetzbuch (SGB X): Es ist zu gewährleisten, dass Sozialdaten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (vgl. Satz 2 Nr. 4 der Anlage zu § 78a SGB X). Werden diese Anforderungen nicht erfüllt, kann nicht ausgeschlossen werden, dass Unbefugte die Inhalte der E-Mails zur Kenntnis nehmen können.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 27. März 2014 eine Entschließung gefasst, die die Gewährleistung der Menschenrechte bei der elektronischen Kommunikation betrifft. Auch die Verwaltungen der Länder werden hierin aufgefordert, auf die Durchsetzung der in der Entschließung behandelten Maßnahmen zu dringen. Zu diesen Maßnahmen gehören unter anderem die Verschlüsselung beim Transport sowie der Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verfahren zur Verbindungsverschlüsselung.

Es ist nachvollziehbar, dass eine E-Mail eine günstige und schnelle Möglichkeit des Informationsaustausches darstellt. Dennoch dürfen datenschutzrechtliche Anforderungen nicht zu Lasten der Betroffenen unberücksichtigt bleiben; die Verschlüsselung der elektronischen Kommunikation ist eine der wesentlichen technischen Maßnahmen zur Sicherstellung des Datenschutzes und darüber hinaus Stand der Technik.

Wir haben das Fachamt schriftlich aufgefordert, die Anforderungen an eine datenschutzkonforme E-Mail-Kommunikation zu berücksichtigen und intern auf die

Umsetzung entsprechender technischer Maßnahmen zu dringen. Es liegt in der datenschutzrechtlichen Verantwortung der Freien und Hansestadt Hamburg, eine gesetzeskonforme und sichere Möglichkeit der E-Mail-Kommunikation bereitzustellen, die vor allem die dargestellten Verschlüsselungstechniken bietet (vgl. auch VI. 1.9).

2.5 Kontoabrufverfahren gem. § 93 AO

Die Fachämter Grundsicherung und Soziales der Bezirksämter führen bisher nur sehr wenige Kontoabrufverfahren nach § 93 Abgabenordnung (AO) durch. Bei der stichprobenhaften Überprüfung solcher Kontoabrufe wurden keine Verstöße gegen datenschutzrechtliche Anforderungen festgestellt.

§ 93 Abs. 7 und 8 i. V. m. § 93b Abgabenordnung (AO) räumt auch den für die Verwaltung der Sozialhilfe nach dem Zwölften Buch Sozialgesetzbuch zuständigen Behörden unter bestimmten Voraussetzungen die Möglichkeit ein, das Bundeszentralamt für Steuern zu ersuchen, bei den Kreditinstituten die in § 93b Abs. 1 AO bezeichneten Daten abzurufen; hierbei handelt es sich insbesondere um Kontonummern zu einem bestimmten Namen. Abrufberechtigte Behörden erhalten hierdurch die Möglichkeit, Informationen über bestehende Konten zu erhalten, um die Berechtigung zum Bezug von Sozialleistungen überprüfen zu können.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hatte bei ihrer Prüftätigkeit einen sehr starken Anstieg derartiger vom Gesetz auch anderen Behörden eröffneten Informationsbeschaffung festgestellt. Wir haben dies zum Anlass genommen, das Kontoabrufverfahren durch die bezirklichen Fachämter Grundsicherung und Soziales stichprobenhaft zu prüfen. Zu diesem Zweck erfolgte eine Prüfung in den Fachämtern Grundsicherung und Soziales Eimsbüttel und Altona.

Wir konnten feststellen, dass aus Sicht der Behörden ein Kontoabruf oftmals nicht erforderlich war, weil eventuelle Zweifel direkt mit den Betroffenen geklärt werden konnten. Hinzu kommt, dass die Fachämter vor der Durchführung eines solchen Kontoabrufverfahrens die Freigabe durch den Bezirksamtsleiter einholen müssen (Arbeitshilfe zu § 82 SGB XII i.V.m. § 93 Abs. 8 AO, Ziffer 2.2).

Die dennoch erfolgten wenigen Kontoabrufe waren nicht zu beanstanden; die Vorschriften des § 93 AO wurden berücksichtigt: Zunächst wurde in den geprüften Fällen versucht, bei den Betroffenen selbst die erforderlichen Kontoinformationen zu erheben. Die Darstellungen der Betroffenen erschienen jedoch hinsichtlich der Zeiten, zu denen Konten bestehen sollten, unvollständig. Vor diesem Hintergrund wurden die Betroffenen schriftlich darauf hingewiesen, dass angesichts der aufgezeigten Unstimmigkeiten ein Kontoabrufverfahren erwogen werde. Ohne dass dies nach dem Gesetz erforderlich gewesen wäre, erteilten die Betroffenen hierzu schriftlich sogar

ihre Zustimmung; ihr informationelles Selbstbestimmungsrecht war somit umfassend gewährleistet. Anschließend wurden die Betroffenen über das Ergebnis des Kontoabrufverfahrens benachrichtigt. Erforderlich waren die Datenerhebungen beim Bundeszentralamt, um die Voraussetzungen der Leistungsberechtigung angesichts der dargestellten Unstimmigkeiten prüfen zu können. Der diesbezügliche Vorgang ergab sich auch dokumentiert aus den Unterlagen des geprüften Grundsicherungsamtes.

2.6 Formularmäßige Offenlegung des Leistungsbezuges bei BuT-Beantragung

Im Rahmen der Leistungen zur Bildung und Teilhabe (BuT) können unter anderem auch die Kosten für Schulausflüge übernommen werden, wenn diese zuvor durch den Lehrer auf einem Formular bestätigt wurden. Nunmehr müssen Leistungsberechtigte dem Lehrer gegenüber nicht mehr bei der Aushändigung dieses Formulars schon aufgrund dessen Formulierung offenbaren, dass sie im Leistungsbezug nach dem SGB II stehen.

Im Rahmen von BuT-Leistungen wurde seitens der Behörde für die Übernahme der Kosten eines Schulausfluges ein Antragsformular genutzt, auf dem die Klassenlehrerin oder der Klassenlehrer die Daten zu Tag, Ziel und Kosten des Ausfluges eintragen muss. Dem Formular war der ausdrückliche Hinweis zu entnehmen, dass das Formular „ausschließlich für Leistungsberechtigte nach dem SGB II (ALG II, Sozialgeld)" gilt. Aufgrund dieser Informationen auf dem Formular war somit zu erkennen, dass der dieses Formular verwendende Betroffene im Leistungsbezug nach dem SGB II steht und deshalb eine Kostenübernahme beantragt.

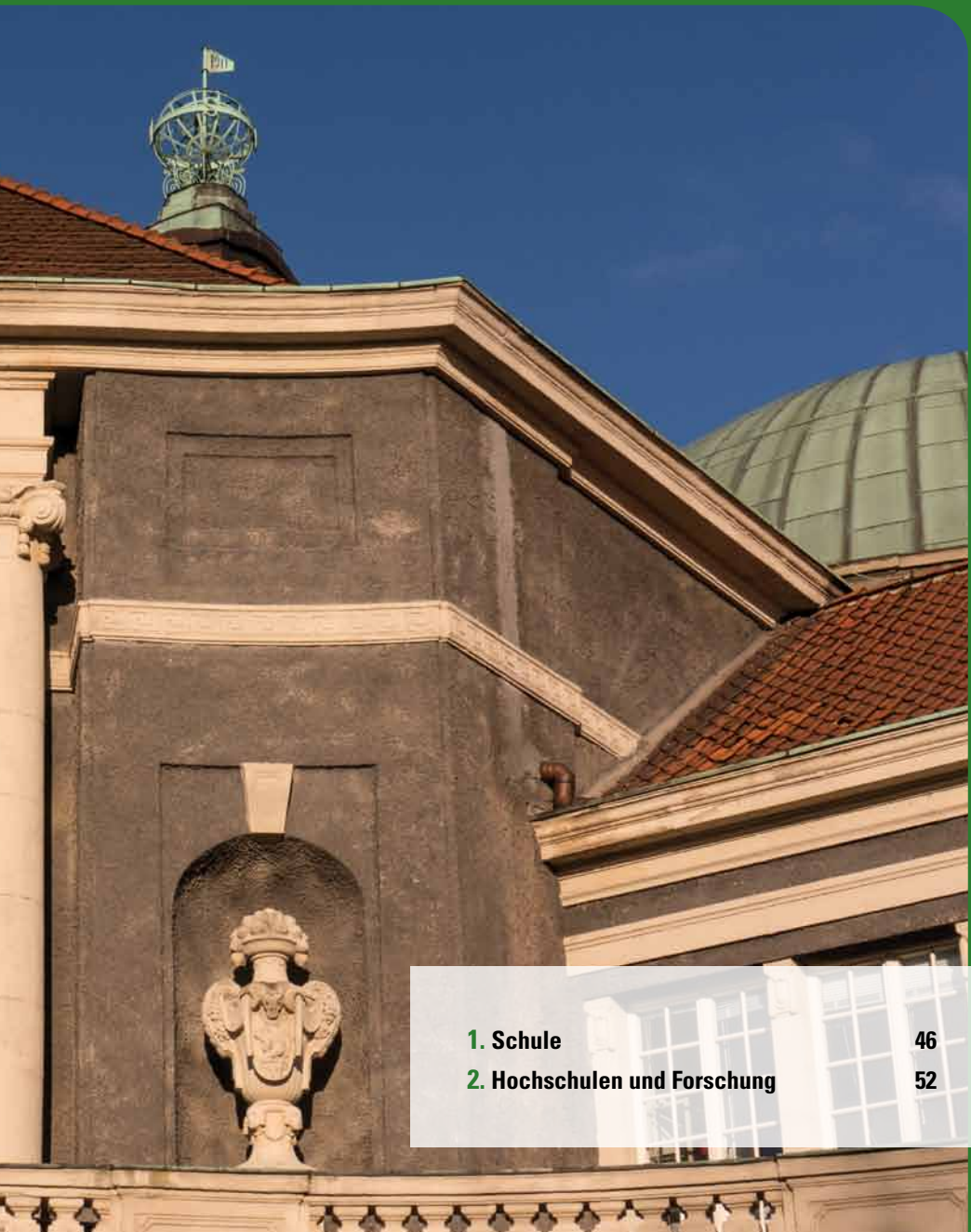
Wir erhielten angesichts dieser Kenntnisnahme des Leistungsbezuges durch die Klassenlehrerin oder den Klassenlehrer eine Bürgereingabe. Mit der Behörde für Arbeit, Soziales, Familie und Integration (BASFI) haben wir sodann die Frage diskutiert, ob das Formular so ausgestaltet sein muss, dass eine Klassenlehrerin oder ein Klassenlehrer durch die dargestellte Formulierung davon Kenntnis erhalten muss, dass ein Leistungsbezug nach dem SGB II besteht.

Auch wenn die Lehrerin oder der Lehrer später ggf. durch die finanzielle Abwicklung ohnehin erfahren würde, dass die Familie der Schülerin oder des Schülers im Leistungsbezug nach dem SGB II steht, kommt es datenschutzrechtlich zunächst auf den Zeitpunkt des lehrerseitigen Ausfüllens des Formulars an. Hier ist es für die Lehrerin oder den Lehrer irrelevant, ob die Unterstützungsbedürftigkeit dem Rechtskreis des SGB II oder des SGB XII zugeordnet wird. Ferner könnte sich zwischenzeitlich ergeben, dass das Kind nicht mitfahren darf; dann erhielte die Lehrerin oder der Lehrer auch später mangels finanzieller Abwicklung keine Kenntnis über den konkreten Leistungs-

bezug. Insoweit hielten wir diese Erkenntnisse aus der Formulierung des Vordruckes zu diesem Zeitpunkt für unnötig und empfahlen, die Formulare entsprechend so anzupassen, dass die Bürgerin oder der Bürger nicht bereits durch die Formulierung gezwungen wird, den konkreten Leistungsbezug zu diesem Zeitpunkt gegenüber der Klassenlehrerin oder dem Klassenlehrer zu offenbaren.

Die BASFI hat unserer Anregung folgend die Formulare inhaltlich umgestaltet. Nunmehr ist sichergestellt, dass die Schule die Kosten des Ausflugs im Vorwege auf der ersten Seite bestätigen kann; erst anschließend kann der Betroffene auf der zweiten Seite seine erforderlichen personenbezogenen Daten eintragen je nachdem, ob der Fall dem SGB II oder SGB XII zuzuordnen ist. Die Schule erhält somit im Zeitpunkt des Ausfüllens keine näheren Informationen mehr über den konkreteren Hintergrund des Leistungsbezuges der Familie.

III. SCHULE, HOCHSCHULEN UND FORSCHUNG



1. Schule 46
2. Hochschulen und Forschung 52

1. Schule

1.1 Abgeschottete Abteilung der Behörde für Schule und Berufsbildung

Wie schon während des letzten Berichtszeitraums arbeitet die Behörde für Schule und Berufsbildung (BSB) weiterhin an dem Entwurf einer gesetzlichen Regelung, die die Rechtsgrundlage insbesondere für Längsschnittuntersuchungen darstellen soll. Der mit solchen Untersuchungen verbundene Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen erfordert eine hinreichend bestimmte Regelung, die auch besondere Schutzvorkehrungen gegen das Gefährdungspotential solcher Datensammlungen trifft.

Bereits im 24. Tätigkeitsbericht (vgl. 24. TB, III 7.1) haben wir darüber berichtet, dass die BSB eine gesetzliche Grundlage schaffen muss, um insbesondere Längsschnittuntersuchungen zukünftig datenschutzkonform durchführen zu können. Um die rechtsstaatlichen Grundlagen möglichst schnell herzustellen, wurde uns bereits Anfang 2014 ein erster Gesetzesentwurf vorgelegt. Hierzu hatten wir ausführlich Stellung genommen und u.a. auf Folgendes hingewiesen: Da es sich bei Längsschnittuntersuchungen um einen besonders intensiven Eingriff in das informationelle Selbstbestimmungsrecht handelt, müssen Schutzvorkehrungen getroffen werden, die u.a. zu einer inhaltlichen und zeitlichen Begrenzung der Untersuchungen führen und die eine Abschottung vom schulischen Verwaltungsvollzug realisieren. Insoweit muss neben weiteren Anforderungen zum einen diejenige Abteilung der BSB, in der die Längsschnittuntersuchungen durchgeführt werden, organisatorisch, personell und räumlich von den Verwaltungsaufgaben der BSB im Übrigen getrennt sein; zum anderen bedarf es der Festlegung der konkreten Daten im Hinblick auf unterschiedliche Verwendungszwecke und deren Folgen (z.B. voneinander abweichende Löschfristen). Bei der seinerzeit vorgelegten Regelung mussten diese und weitere Anforderungen genauer aufgenommen werden, damit von einer hinreichend bestimmten Rechtsgrundlage ausgegangen werden konnte; vor allem die Datentrennung dahingehend, dass keine Informationseinheit zwischen der abgeschotteten Abteilung einerseits und dem Verwaltungsvollzug andererseits besteht, ist datenschutzrechtlich eine zwingende Voraussetzung.

Im Sommer 2015 wurde uns ein neuer Entwurf angekündigt; auf dessen Grundlage fand erneut ein Gespräch mit der BSB statt, in dem wir nochmals die grundlegenden Strukturen insbesondere hinsichtlich der unterschiedlichen Verwendungszwecke der Daten diskutierten und klarstellten. Vor allem sahen wir die Notwendigkeit, die erforderliche Datentrennung nochmals zu betonen. Insoweit ist auch die Frage entscheidend, ob und inwieweit Daten personenbezogen an Stellen außerhalb der abgeschotteten Abteilung weitergegeben werden dürfen, damit dort eine Beurteilung erfolgen und ein Untersuchungsergebnis gefunden werden kann.

Die BSB hat unsere Anmerkungen zur Kenntnis genommen; derzeit liegt ein weiterer Gesetzentwurf zur Abstimmung vor. Wir werden weiterhin darauf dringen, dass möglichst zügig die notwendige Rechtsgrundlage geschaffen wird.

1.2 Schülerdaten im Internet

Auch wenn in einem sportlichen Wettkampf der Vergleich zu anderen Wettkampfteilnehmerinnen und Wettkampfteilnehmern für den einzelnen Betroffenen eine interessante Information darstellen kann, rechtfertigt dies allein nicht, die Wettkampfdaten von Schülerinnen und Schülern ohne deren Einwilligung im Internet zu veröffentlichen.

Aufgrund einer Bürgereingabe wurden wir auf die Internetseite „www.schulsport-hamburg.de" der Behörde für Schule und Berufsbildung aufmerksam. Dort werden Informationen über sportliche Wettkämpfe in Hamburg dargestellt.

Neben allgemeinen Berichten und Mitteilungen wurde auf dieser Internetseite für jedermann einsehbar eine Vielzahl personenbezogener Daten derjenigen Schülerinnen und Schüler veröffentlicht, die an Wettkämpfen teilgenommen haben. Zu den einzelnen Sportarten waren zum Teil umfangreiche Ergebnislisten mit Klarnamen und z.T. weiteren Informationen (z.B. Zeiten bei Lauf-Wettbewerben, Platzangaben, Schulangaben usw.) öffentlich zugänglich.

In der Veröffentlichung im Internet ist eine Weitergabe der Daten unter anderem auch an Private und damit ein rechtfertigungsbedürftiger Eingriff in das informationelle Selbstbestimmungsrecht der Schülerinnen und Schüler zu sehen. Daher benötigte die Behörde für Schule und Berufsbildung für eine derartige Veröffentlichung in datenschutzrechtlicher Hinsicht eine Rechtsgrundlage; vorliegend ist jedoch eine gesetzliche Grundlage nicht ersichtlich. Somit könnte nur die Einwilligung der Betroffenen als Rechtfertigung in Betracht kommen; allerdings soll es sich nach Aussage der Petenten teilweise jedenfalls auch um Pflichtveranstaltungen oder zumindest solche Wettbewerbe gehandelt haben, zu deren Teilnahme sich die Kinder verpflichtet sahen. Daher haben wir die Fachbehörde angesichts der sehr großen Zahl personenbezogener Daten, die auf die beschriebene Weise veröffentlicht wurden, aufgefordert, uns umgehend eine Stellungnahme zukommen zu lassen und Maßnahmen zu ergreifen.

Im Rahmen einer eingehenden Besprechung mit Vertretern der Fachbehörde haben wir die datenschutzrechtliche Erforderlichkeit einer entsprechenden Rechtsgrundlage unterstrichen und gleichzeitig denkbare Lösungswege aufgezeigt, die einen sportlichen

Vergleich und eine Selbsteinschätzung zulassen, die Daten der anderen Teilnehmer jedoch nicht personenbezogen offenbart (vergleichbar einem Notenspiegel nach einer Klassenarbeit). Durch eine hierdurch zu erzielende Aggregierung der Teilnehmerdaten im Übrigen kann sich die einzelne betroffene Schülerin bzw. der einzelne betroffene Schüler dennoch in das Gesamtergebnis einordnen und kann ersehen, zu welcher Leistungsgruppe er gehört.

Im Anschluss hat uns die Fachbehörde mitgeteilt, dass sie eine datenschutzkonforme Lösung des Problems verfolgt. Da eine entsprechende Umsetzung nicht zeitnah erreichbar war, hat die Fachbehörde uns mitgeteilt, dass keine weiteren Listen mit Einzelergebnissen und Klarnamen auf die Internetseite gestellt werden und dass vor allem alle bereits veröffentlichten Einzelergebnisse mit Klarnamen usw., für deren Veröffentlichung keine Einwilligung vorliegt, von der Internetseite gelöscht werden. Unsere stichprobenweise durchgeführte Kontrolle hat dabei ergeben, dass die Fachbehörde dieser Löschverpflichtung nachgekommen ist und somit einen datenschutzkonformen Zustand wieder hergestellt hat.

1.3 Hamburger Schreib-Probe

Die Behörde für Schule und Berufsbildung bietet ihren Lehrkräften für die Auswertung des Rechtschreibtests „Hamburger Schreib-Probe" ein Online-Tool an, das von einem Verlag bereitgestellt wird. Aufgrund unserer Intervention wurde zumindest nachträglich eine datenschutzkonforme Nutzungsmöglichkeit dieser für die Lehrkräfte effizienteren Auswertungsmöglichkeit geschaffen.

Zur Unterstützung der Rechtschreibdiagnostik erklärte die Behörde für Schule und Berufsbildung seit dem Schuljahr 2014/2015 die jährliche Durchführung der Hamburger Schreib-Probe (HSP) bei allen Schülerinnen und Schülern der Jahrgangsstufen 1 bis 10 für verbindlich. Inhaltlich ist die HSP ein Rechtsschreibtest, durch den das Rechtschreibkönnen und die grundlegenden Rechtschreibstrategien der Schülerinnen und Schüler eingeschätzt werden soll. Die Antworten auf die Testfragen tragen die Schülerinnen und Schüler in Testhefte ein. Die Lehrerinnen und Lehrer können zur Auswertung das Online-Portal www.hsp-plus.de nutzen; hierbei handelt es sich um ein Angebot eines Verlages.

Aufgrund einer Lehrereingabe sind wir auf diesen Sachverhalt aufmerksam gemacht worden verbunden mit der Frage, ob die Verarbeitung der personenbezogenen Daten der Kinder in dem Online-Portal datenschutzrechtlich zulässig ist. Die Fachbehörde stellte uns dar, dass die Nutzung der Online-Auswertung nur optional neben einer Auswertung direkt im Testheft angeboten wird, vor allem um für die Lehrkräfte eine zeitliche Einsparung des Kontrollaufwandes zu erzielen. Zunächst wurde angekündigt,

die Verfahrensvorgaben dahingehend anzupassen, dass die Online-Auswertung ohne Angabe eines Namens und einer Klassenstufe erfolgt. Die so eingegebenen Daten sind jedoch anhand des Testheftes weiterhin einem bestimmbaren Kind zuordbar, so dass datenschutzrechtlich immer noch von einer Weitergabe personenbezogener Daten an den Verlag auszugehen war.

Daher bedurfte es des Abschlusses eines Auftragsdatenverarbeitungsvertrages, um eine datenschutzrechtlich zulässige Nutzung der Online-Auswertung sicherzustellen. Rechtlich ist ein Auftragsdatenverarbeitungsnehmer kein Dritter im Verhältnis zum Auftraggeber, so dass es für die Weitergabe von personenbezogenen Daten keiner eigenen Übermittlungsbefugnis bedarf. Dennoch müssen weitere Maßnahmen ergriffen werden, um den Datenschutz zu gewährleisten wie z.B. die Verschlüsselung der Datenübertragung.

Nach längeren Diskussionen konnte die Fachbehörde schließlich mit dem Verlag einen Auftragsdatenverarbeitungsvertrag abschließen, in dem sich der Verlag unter anderem auch dazu verpflichtete, die Daten ausschließlich zum Zweck der HSP zu nutzen; auch die Verschlüsselung der Datenübertragung ist vom Verlag zugesichert. Hierneben arbeitet die Fachbehörde erfreulicherweise an einer eigenen Lösung, da hierdurch selbst die Weitergabe von personenbezogenen Daten vermieden werden kann.

1.4 Pilotprojekt „Start in die nächste Generation" der Behörde für Schule und Berufsbildung

Sollen Schülerinnen und Schüler im Unterricht ihre eigenen Smartphones, Tablets oder Laptops einsetzen, bedarf es nicht nur im Hinblick auf eine transparente Gestaltung, sondern auch mangels gesetzlicher Grundlage für bestimmte Datenverarbeitungsvorgänge einer informierten Einwilligung. Nachdem das Projekt bereits gestartet wurde, hat die Behörde für Schule und Berufsbildung (BSB) unseren Anmerkungen folgend die Einwilligungserklärungen angepasst.

Ziel des von der BSB und der Senatskanzlei entwickelten Projekts „Start in die nächste Generation" ist die Einbindung und sinnvolle Nutzung mobiler Endgeräte im Unterricht. An drei Stadtteilschulen und an drei Gymnasien sollen Schülerinnen und Schüler einzelner Klassen ihre eigenen Geräte einsetzen können; hierfür wird seitens der BSB eine Online-Lernplattform mit Zugangsportal zur Verfügung gestellt, die von Dritten betrieben wird. Im Rahmen eines solchen Projektes sind an mehreren Stellen datenschutzrechtliche Aspekte zu berücksichtigen: So sind z.B. bei einer Auftragsdatenverarbeitung gesetzlich vorgesehene formelle Anforderungen zu berücksichtigen, wobei zunächst die genaue Ausgestaltung der jeweiligen Dienstleistungen geklärt werden

musste. Auch war zu Beginn für uns nicht ersichtlich, inwieweit weitere Stellen in die Verarbeitung personenbezogener Daten eingebunden werden sollen; dies haben wir bei der BSB nachgefragt. Ferner erschienen uns die vorgesehenen Regelungen zur Löschung personenbezogener Daten in der zur Verfügung gestellten Online-Lernplattform nicht schlüssig und mussten analysiert werden. So wurde die einzelnen Schritte der bei einem solchen Vorhaben bestehenden Datenverarbeitungen von uns geprüft, bewertet und mit der BSB besprochen.

Soweit gesetzliche Vorschriften nicht bestehen, bedarf es auch im Rahmen eines solchen Pilotprojektes der Einwilligung der Betroffenen. Dies betrifft z.B. den Bereich des Fernmeldegeheimnisses; hier kann eine Einwilligung in die Speicherung und Auswertung der anfallenden Daten durch die Schule zu Kontrollzwecken und zur Gewährleistung des Kinder- und Jugendschutzes eine rechtliche Grundlage für einen Eingriff in das Fernmeldegeheimnis darstellen. Die uns im Jahr 2014 vorgelegte und von der BSB bereits verwendeten Aufklärungs- und Einwilligungsformulare beinhalteten insoweit jedoch keine Ausführungen.

In einer ersten Reaktion hat die BSB eine Vielzahl unserer konzeptionellen Anmerkungen aufgegriffen. Die Erstellung der Aufklärungs- und Einwilligungsformulare setzte jedoch voraus, dass zunächst die gesamten Prozesse geklärt wurden, damit über den Umfang der Einwilligungserklärung Klarheit geschaffen werden konnte. Letztlich hat die BSB Formulare vorgelegt, die den datenschutzrechtlichen Anforderungen im Hinblick darauf genügen, dass eine Einwilligung nur dann wirksam ist, wenn ihr eine umfassende Information der Betroffenen vorausgeht. Somit kann die BSB zumindest ab dem Schuljahr 2015/2016 für die Datenverarbeitung im Rahmen dieses Projektes die erforderliche Einwilligungserklärung auf Formularen einholen, die datenschutzkonform sind.

Entscheidend für die Wirksamkeit der Einwilligung ist in diesem Rahmen aber vor allem die Freiwilligkeit der Erklärung an sich; nur die freiwillig erteilte Einwilligung kann eine für die Rechtfertigung des mit der Datenverarbeitung einhergehenden Eingriffs in das informationelle Selbstbestimmungsrecht erforderliche Rechtsgrundlage bilden. Wichtig ist insoweit, dass die betroffenen Kinder oder deren Sorgeberechtigten nicht dadurch zur Erteilung der Einwilligung gezwungen werden dürfen, dass das Kind ansonsten nicht am Unterricht teilnehmen kann oder sogar in eine andere Klasse versetzt werden müsste. Daher ist es besonders wichtig, dass das Projekt auf Einwilligungsbasis nur in solchen Klassen durchgeführt werden darf, in denen alle Betroffenen ihre Einwilligung erteilt haben. Das Verfahren zur Einholung der Einwilligungen könnte dabei zwecks Wahrung der Freiwilligkeit so ausgestaltet werden, dass bei allen Betroffenen deren Teilnahmebereitschaft zunächst anonym erhoben wird; dies kann z.B. dadurch erfolgen, dass jeder Betroffene ein entsprechendes Formular nebst Aufklärung erhält, auf dem die Teilnahmebereitschaft oder auch die Ablehnung z.B. durch eine Ankreuzmöglichkeit vermerkt wird, ohne dass aber zugleich der Name

des Betroffenen angegeben wird oder sonst eine Identifizierungsmöglichkeit besteht. Nur wenn hier die Formulare ausnahmslos aller Beteiligten zurückgesandt werden und die Teilnahmebereitschaft ausweisen, wird die personalisierte Einwilligung eingeholt. Wir haben dementsprechend besonderen Wert darauf gelegt, dass auch in den Formularen auf die Freiwilligkeit und die Folgen einer Nicht-Teilnahme und eines späteren Widerrufes ausdrücklich hingewiesen wird. Nach Aussage der BSB wird das Projekt auch tatsächlich nur in solchen Klassen durchgeführt, in denen die Voraussetzung einer vollumfänglichen Zustimmung aller Beteiligten erfüllt ist.

1.5 Hamburger Medienpass / Medienkompetenztage

Datenschutz- und Medienkompetenzbildung stellen eine wichtige Aufgabe dar, um die wirksame Realisierung des Datenschutzes bereits präventiv sicherzustellen. Leider haben wir zwischenzeitlich mangels ausreichender personeller Kapazitäten nicht mehr die Möglichkeit, aktiv an entsprechenden Projekten in Hamburg mitzuwirken.

Bereits im letzten Tätigkeitsbericht (vgl. 24. TB, III 7.4) haben wir über das von der Behörde für Schule und Berufsbildung in Kooperation mit dem Landesinstitut für Lehrerbildung und Schulentwicklung initiierte Projekt „Hamburger Medienpass" berichtet, in dessen Rahmen wir das Unterrichtsmaterial für das Modul „Datenschutz und soziale Netzwerke" entworfen haben. Nachdem im Jahr 2014 weitere inhaltliche Abstimmungen zwischen den beteiligten Stellen stattfanden, steht auch dieses Modul nunmehr seit über einem Jahr zum Download im Internet bereit. Seit seiner Veröffentlichung wird das Modul kontinuierlich aufgerufen und heruntergeladen. Die bisherige insgesamt positive Resonanz bestätigt, dass die zentralen Zielerwartungen in der Praxis erreicht werden; angesichts seines Verbreitungsgrades und der Möglichkeit, die Schülerinnen und Schüler mit Hilfe der bereitgestellten Unterrichtsmaterialien in einem verantwortungsvollen Umgang mit ihren Daten zu schulen, wird das Modul zu einer Steigerung ihrer Medien- und Datenschutzkompetenz führen. Weiterhin muss jedoch das Ziel sein, die Bildung im Bereich Medien- und Datenschutzkompetenz kontinuierlich zu verbessern und z.B. als eigenes Unterrichtsfach verpflichtend vorzuschreiben, damit die Heranwachsenden ihre personenbezogenen Daten effektiv zu schützen lernen.

Im Jahr 2014 initiierte auch die Verbraucherzentrale Hamburg ein Projekt „Medienkompetenztage". Einzelne Jahrgänge in Schulen werden hierbei im gesamten Spektrum der Anwendung digitaler Medien wie z.B. strafrechtliche Komponenten im Zusammenhang mit Urheberrecht und Mobbing, Verbraucherschutzfragen im Zusammenhang mit sogenannten Abo-Fallen und vor allem auch datenschutzrechtliche Themen geschult; anschließend finden Fortbildungen mit gleichen Themenschwerpunkten für die

Lehrerinnen und Lehrer und eine Veranstaltung für die Eltern statt. Ziel ist es hierbei, die Medienkompetenz der Schulungsteilnehmerinnen und Schulungsteilnehmer zu fördern.

Auch dieses Projekt stellt einen guten Beitrag zur Medienkompetenzbildung in Hamburg dar. Daher haben wir eingangs sehr gern unsere Beteiligung zugesagt. Für unseren Beitrag sahen wir den Schwerpunkt ebenfalls in dem für Jugendliche höchst relevanten Bereich Datenschutz und soziale Netzwerke. Nach der Durchführung bereits der ersten Veranstaltung mussten wir jedoch erkennen, dass unsere personellen Ressourcen bei weitem nicht ausreichen, um das Thema Datenschutz in diesem Rahmen zu vermitteln. Wir waren daher gezwungen, unsere weitere Teilnahme an diesem Projekt abzusagen. Angesichts unserer Zuständigkeit und Expertise müssten wir jedoch eine der tragenden aktiven Rollen der Datenschutz- und Medienkompetenzbildung wahrnehmen können. Eine ausreichende personelle Ausstattung ist daher auch für diese Aufgabe zwingend notwendig.

2. Hochschulen und Forschung

2.1 Koppelung Netzwerke der Universitäten mit dem FHH-Netz

Die Finanzbehörde hat mit zwei Hamburger Universitäten eine Koppelung des Netzwerks der Stadtverwaltung mit den Netzwerken der Hochschulen vereinbart. Wir sehen die Gefahr von Sicherheitsrisiken und dem Aufweichen der für das FHH-Netz ursprünglich angedachten Ziele.

Im Januar 2015 hat die Finanzbehörde mit der Universität Hamburg und der Technischen Universität Hamburg-Harburg eine Vereinbarung unterzeichnet, mit der das abgeschottete interne Netzwerk der Stadt, das „FHH-Netz", mit den Netzwerken dieser beiden Hochschulen gekoppelt wird. D.h. es werden Übergänge und Schnittstellen geschaffen, mit der Intention, Rechnern aus den Uni-Netzen heraus Zugriff auf Fachverfahren der FHH zu ermöglichen. Der dahinterstehende Nutzen ist nachvollziehbar, dennoch sehen wir die Vereinbarung aus der Perspektive von Datenschutz und der IT-Sicherheit kritisch.

Beim FHH-Netz handelt es sich um ein stark reglementiertes Netzwerk, in dem überwiegend standardisierte Endgeräte und Netzwerkkomponenten aktiv sind. Diese werden vom beauftragten Dienstleister Dataport mit definierten Verwaltungs- und Administrationsprozessen in Betrieb genommen, gewartet und auch stillgelegt. So wurde gezielt eine Vereinheitlichung der Systemumgebung herbeigeführt, z.B. indem das Konzept des „BASIS-PCs" als einheitlicher Arbeitsplatzrechner für die FHH-Mitar-

beiterinnen und Mitarbeiter geschaffen und umgesetzt wurde.

Die Netzwerke der Universität Hamburg und der Technischen Universität Hamburg-Harburg werden von den Hochschulen selbst betrieben. Auch wenn dort hervorragendes IT-Know-how vorhanden ist, ist anzunehmen, dass in der Praxis zumindest gelegentlich Forscherdrang, Pragmatismus oder Innovationswille vor Sicherheitsaspekten steht. In Hochschulen werden Administrationsaufgaben häufig von wissenschaftlichem Personal „nebenbei" zu ihrer Forschungsaufgabe erledigt, auch haben diese aufgrund befristeter Anstellung oder aus Laufbahngründen (Ausscheiden, Wechsel an andere Fakultäten/Hochschulen o.ä.) die Betreuungsaufgabe häufig nicht lange inne. Mit einem Weggang geht oftmals auch das Know-how oder es wird keine geeignete Dokumentation hinterlassen. Ebenfalls nicht zu vernachlässigen ist, dass an Hochschulen bei der Einstellung von Mitarbeiterinnen und Mitarbeitern, die oftmals bereits als studentische Hilfskraft akquiriert werden, Aspekte wie Eignung für sicherheitsrelevante Tätigkeiten weniger Gewicht haben als bei einem professionellen IT-Dienstleistungsunternehmen wie Dataport.

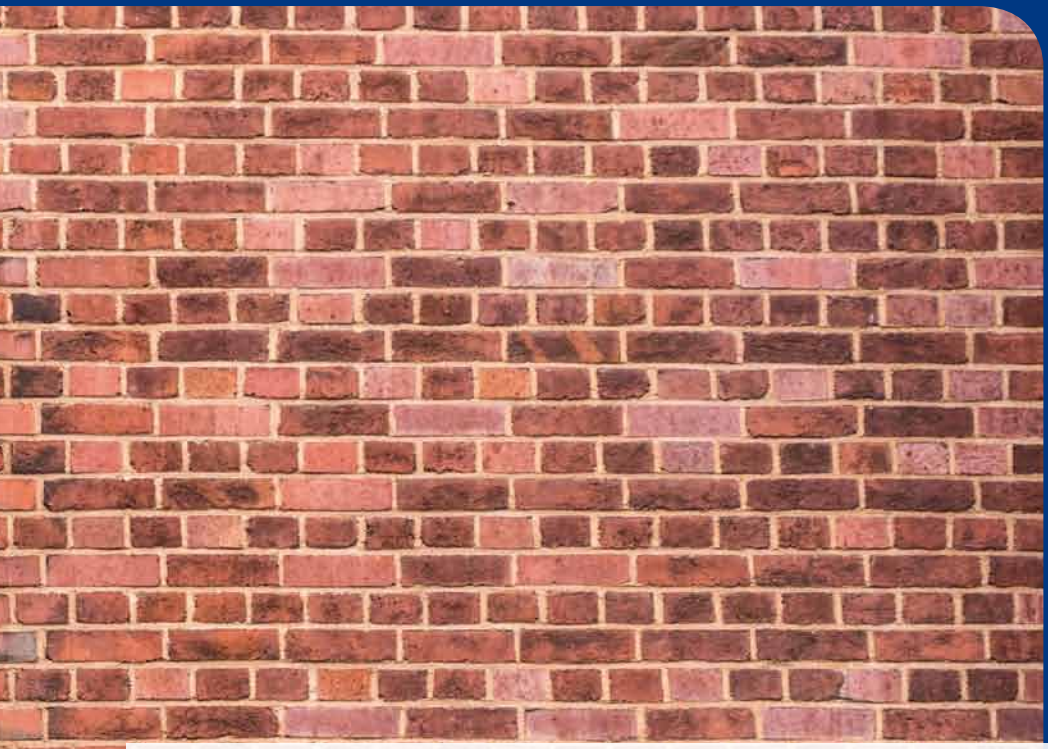
Durch Anbindung der Universitätsnetzwerke an das Verwaltungsnetzwerk ist daher von einer Erhöhung des Risikopotentials vor allem für das bisher abgeschottete FHH-Netz auszugehen. Auch sehen wir die Gefahr, dass schleichend ein Auf- oder Abweichen von Sicherheitsvorgaben oder -zielen stattfindet, die im FHH-Netz bislang konsequent verfolgt und umgesetzt wurden.

Es ist daher wichtig, Gefahren und Risiken durch eine effiziente Absicherung und Überwachung des laufenden Betriebes beider Netzwerke und ihrer Schnittstellen zu senken. Hier lassen die der Vereinbarung zugrundeliegenden Dokumente Optimierungsbedarf erkennen. Beispielweise wird im Text der Vereinbarung den Universitäten die Verantwortung auferlegt, die für das FHH-Netz geltenden Richtlinien und Sicherheitsanforderungen zu erfüllen. Das Sicherheitskonzept der Universitäten hingegen enthält Verweise oder Empfehlungen zu technischen Maßnahmen, die vom Betreiber des Verwaltungsnetzwerkes, also von Dataport, umgesetzt werden sollten. So droht an Stellen wie z.B. Firewall-Regeln oder Zugangskontrolllisten ein Regelungsvakuum. Werden diese Punkte nicht gemeinsam und koordiniert gelöst, können daraus Sicherheitsprobleme für beide Netzwerke erwachsen.

Es ist daher u.a. erforderlich, die Kommunikation zwischen den beiden Parteien, die durch die Koppelung nun auch gemeinsame Risiken tragen, aufrecht zu halten und im Konzept zur Netzkopplung festzuschreiben. Dazu könnte gehören, dass zu den regelmäßigen Treffen der behördlichen Datenschutz- bzw. Informationssicherheitsbeauftragten der FHH auch die jeweiligen Beauftragten der Hamburger Universitäten eingeladen werden. Dies findet bislang nicht statt.


KVÖHL
POLIZEI
WACHE

INNERES, SICHERHEIT UND JUSTIZ IV.



1. Polizei 56
2. Verfassungsschutz 91
3. Ausländerwesen 94
4. Justiz 95
5. Meldewesen 102
6. Personenstandswesen 110
7. Statistik 113
8. Bezirke 117

1. Polizei

1.1 Vorratsdatenspeicherung 2.0

Neuer Name altes Gewand. Auch wenn das Bundesverfassungsgericht und der Europäische Gerichtshof die Speicherung von Telekommunikationsdaten in engen Grenzen für zulässig erachtet haben, bestehen Bedenken, ob die neue gesetzliche Regelung den verfassungsrechtlichen und europarechtlichen Anforderungen genügt.

Am 27. Mai 2015 hat das Bundeskabinett einen Gesetzentwurf zur „Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten" beschlossen und damit eine fast 15-jährige Diskussion über die Speicherung von Telekommunikationsdaten auf Vorrat (Vorratsdatenspeicherung, VDS) wieder aufleben lassen.

Beabsichtigt war zunächst, das Gesetz noch vor der parlamentarischen Sommerpause durch den Bundestag zu bringen. Letztlich sorgte das EU-Notifizierungsverfahren – nach der die Mitgliedstaaten, die Kommission über jeden Entwurf einer technischen Vorschrift vor deren Erlass unterrichten müssen (Richtlinie 98/34/EG) – dafür, dass das Gesetz erst am 16. Oktober 2015 vom Bundestag beschlossen und am 20. November 2015 im Bundesgesetzblatt verkündet wurde. Das Gesetz ist einen Tag nach seiner Verkündung in Kraft getreten. Ab dann haben die Telekommunikationsanbieter 18 Monate Zeit zur Umsetzung.

Das Bundesverfassungsgericht (BVerfG) hatte zuvor bestehende Regelungen bereits für verfassungswidrig erklärt (Urteil v. 02. März 2010 - 1 BVR 256/08, 1 BVR 263/08, 1 BVR 586/08). In der Folge war eine sechsmonatige, vorsorglich anlasslose Speicherung von Telekommunikationsdaten durch private Dienstanbieter nicht mehr möglich. Zudem mussten bereits gespeicherte Daten unverzüglich gelöscht werden.

Trotz seiner Entscheidung war das BVerfG der Auffassung, dass die der VDS zugrunde liegende europäische Richtlinie 2006/24/EG durchaus verfassungskonform umgesetzt werden könne, wobei es die VDS wegen der hohen Eingriffsintensität lediglich in engen Grenzen für zulässig erachtet hat. Der Grundsatz der Verhältnismäßigkeit verlange, dass die gesetzliche Ausgestaltung einer solchen Datenspeicherung dem besonderen Gewicht des mit der Speicherung verbundenen Grundrechtseingriffs angemessen Rechnung trage. Erforderlich seien hinreichend anspruchsvolle und normenklare Regelungen hinsichtlich der Datensicherheit, der Datenverwendung, der Transparenz und des Rechtsschutzes (BVerfG a.a.O., LS 2).

Das BVerfG betonte:

- Datensicherheit: Erforderlich sei eine gesetzliche Regelung, die ein besonders hohes Maß an Sicherheit normenklar und verbindlich vorgebe. Der Gesetzgeber

habe dabei sicherzustellen, dass die Entscheidung über Art und Maß der zu treffenden Schutzvorkehrungen nicht letztlich unkontrolliert in den Händen der jeweiligen Telekommunikationsanbieter liege (BVerfG a.a.O., Rn. 221 ff.).

- Datenverwendung: Angesichts der hohen Eingriffsintensität komme eine Verwendung der Daten nur für überragend wichtige Aufgaben des Rechtsgüterschutzes in Betracht, das heißt zur Ahndung von Straftaten, die überragend wichtige Rechtsgüter bedrohen, oder zur Abwehr von Gefahren für solche Rechtsgüter (BVerfG a.a.O., Rn. 226 ff.).

- Transparenz: Der Gesetzgeber müsse die diffuse Bedrohlichkeit einer heimlichen Speicherung durch wirksame Transparenzregeln auffangen. Eine Verwendung der Daten ohne Wissen des Betroffenen sei nur dann zulässig, wenn andernfalls der Zweck der Untersuchung vereitelt würde. Eine heimliche Verwendung der Daten dürfe bei der Strafverfolgung nur vorgesehen werden, wenn sie im Einzelfall erforderlich und richterlich angeordnet ist. Zudem müsse zumindest eine nachträgliche Benachrichtigung vorgesehen werden (BVerfG a.a.O., Rn. 242 ff.).

- Rechtsschutz: Eine Übermittlung und Nutzung der gespeicherten Daten sei grundsätzlich unter Richtervorbehalt zu stellen. Außerdem müssen wirksame Sanktionen bei Rechtsverletzungen vorgesehen werden (BVerfG a.a.O., Rn. 247 ff.).

Die Datenschutzbeauftragten des Bundes und der Länder haben vor dem Hintergrund des Urteils mit der Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18. März 2010 „Keine Vorratsdatenspeicherung!" http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/79DSK_Vorratsdatenspeicherung.html?nn=5217228 gefordert, dass die Bundesregierung sich für eine Abschaffung der Europäischen Richtlinie zur VDS einsetzen solle.

Die diesem Gesetz zugrundeliegende EU-Richtlinie 2006/24/EG wurde am 08. April 2014 schließlich vom Europäischen Gerichtshof (EUGH C-293/12, C594/12) wegen Verstoßes gegen den in Art. 7 garantierten Schutz der Privatsphäre und den durch Art. 8 garantierten Schutz personenbezogener Daten der Charta der Europäischen Grundrechte für ungültig erklärt.

Die Entscheidung des EuGH erinnert stark an die des BVerfG. Auch wenn es die grundsätzliche Geeignetheit der VDS zur Erreichung des mit der Richtlinie verfolgten Ziels gesehen hat, würden die Bestimmungen der Richtlinie nicht ausreichen, um den Eingriff von großem Ausmaß und von besonderer Schwere zu rechtfertigen.

So moniert der EuGH im Wesentlichen folgende Punkte:

- Betroffen seien generell sämtliche Personen, elektronische Kommunikationsmittel und Verkehrsdaten, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des Ziels der Bekämpfung schwerer Straftaten.

- Eine Einschränkung der schwerwiegenden Straftaten sei nicht vorgesehen, da die Richtlinie allgemein auf die von jedem Mitgliedstaat in seinem nationalen Recht bestimmten „schweren Straftaten" Bezug nehme.

- Es fehlen materiell- und verfahrensrechtliche Voraussetzungen für den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung.

- Der Zugang zu den Daten unterliege zudem keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle.

- Vorgeschrieben sei die Dauer der Vorratsspeicherung der Daten von mindestens sechs Monaten, ohne dass eine Unterscheidung zwischen den Datenkategorien anhand der betroffenen Personen oder nach Maßgabe des etwaigen Nutzens der Daten für das verfolgte Ziel getroffen werde.

- Es fehlen objektive Kriterien, die gewährleisten, dass die Speicherung auf das absolut Notwendige beschränkt werde.

- Es gibt keine hinreichenden Garantien, dass die Daten wirksam vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang und jeder unberechtigten Nutzung geschützt seien. Unter anderem gestattet die Richtlinie den Diensteanbietern, bei der Bestimmung des von ihnen angewandten Sicherheitsniveaus wirtschaftliche Erwägungen (insbesondere hinsichtlich der Kosten für die Durchführung der Sicherheitsmaßnahmen) zu berücksichtigen, und gewährleiste nicht, dass die Daten nach Ablauf ihrer Speicherungsfrist unwiderruflich vernichtet werden.

- Die Speicherung der Daten im Unionsgebiet ist nicht zwingend vorgesehen (EuGH a.a.O. Rn. 58 ff.).

Die Datenschutzbeauftragten des Bundes und der Länder haben stets die anlasslose und massenhafte Speicherung von Verkehrsdaten der Telekommunikation abgelehnt. Nicht zuletzt, weil mit derartigen Maßnahmen massiv in die Freiheitsrechte aller Menschen, unabhängig von einem konkreten Verdacht, eingegriffen wird. Das Urteil des EuGH hatte weitreichende Folgen in Europa und ist ein wichtiger Schritt zur Bekräftigung der informationellen Selbstbestimmung und des Telekommunikationsgeheimnisses. Deswegen setzten sich die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 25. April 2014 für das „Ende der Vorrats-

datenspeicherung in Europa!“ *http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/25042014EndeVorratsdatenspeicherung.pdf?__blob=publicationFile&v=2* ein.

Dieser Appell hatte keinen Erfolg. Unter dem Eindruck der terroristischen Anschläge von Paris im Januar 2015 hat die Bundesregierung das nun scheinbar ausgediente Modell der VDS wieder belebt.
Zentrale Norm für die VDS ist § 113b Telekommunikationsgesetz (TKG). Hiernach sind die Erbringer öffentlich zugänglicher Telefondienste verpflichtet, von allen Teilnehmern – und damit z.B. auch Berufsgeheimnisträgern – Verkehrsdaten und IP-Adressen künftig zehn Wochen, Standortdaten von mobilen Geräten hingegen vier Wochen lang zu speichern. § 113c TKG regelt die Verwendung der nach Maßgabe von § 113b TKG gespeicherten Verkehrsdaten und enthält – laut Gesetzesbegründung – eine enge Zweckbegrenzung. Eine Evaluierung ist zwar nicht vorgesehen, jedoch sieht das Gesetz erstmalig eine statistische Erfassung der vorgenommenen Ermittlungsmaßnahmen vor.

In ihrer Umlaufentschließung vom 09. Juni 2015 haben die Datenschutzbeauftragten des Bundes und der Länder daher erneut betont, dass mit einer VDS massiv in Freiheitsrechte von allen Menschen unabhängig von einem konkreten Verdacht eingegriffen wird. Derartige Maßnahmen, die nur als absolute Ausnahme überhaupt zulässig sein können, seien deshalb einer strengen Erforderlichkeits- und Verhältnismäßigkeitsprüfung zu unterziehen und durch technische, organisatorische und verfahrensrechtliche Vorkehrungen abzusichern. Die Konferenz kann nicht erkennen, dass die Regelungen grundrechtlichen Anforderungen genügen. Dies gelte namentlich für die Kommunikation mit Berufsgeheimnisträgern (z.B. Abgeordneten, Ärzten, Rechtsanwälten und Journalisten) http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/09062015_GesetzesentwurfVorratsdatenspeicherung.html?nn=5217228.

1.2 Gefahrengebiete

Nach Auffassung des Oberverwaltungsgerichts Hamburg verstößt die Regelung zu den Gefahrengebieten gegen das rechtsstaatliche Bestimmtheitsgebot und gegen den Grundsatz der Verhältnismäßigkeit. Trotzdem hält die Behörde für Inneres und Sport an den Gefahrengebieten fest.

2005 wurde § 4 Abs. 2 in das Polizeidatenverarbeitungsgesetz (PolDVG) eingefügt. Hiernach darf die Polizei im öffentlichen Raum in einem bestimmten Gebiet Personen kurzfristig anhalten, befragen, ihre Identität feststellen und mitgeführte Sachen in Augenschein mitnehmen, soweit auf Grund von konkreten Lageerkenntnissen anzunehmen ist, dass in diesem Gebiet Straftaten von erheblicher Bedeutung begangen

werden und die Maßnahme zur Verhütung der Straftaten erforderlich ist.

Gestützt auf diese Regelung wies die Polizei Hamburg ab dem 04. Januar 2014 weite Teile der Stadtteile Sternschanze, St. Pauli, Altona-Altstadt und Altona-Nord (vom Holstenkamp im Nordwesten bis zum U- und S-Bahnhof Landungsbrücken im Südosten, vom U-Bahnhof Schlump im Nordosten bis zur Elbe beim Fischereihafen) als Gefahrengebiete aus. Nach Mitteilung der Behörde für Inneres erfolgte die Einrichtung vor dem Hintergrund der Geschehnisse am

- 12. Dezember 2013: Ausschreitungen im Bereich des Polizeikommissariats 16 (PK 16),
- 20. Dezember 2013: Ausschreitungen im Bereich PK 16 und vor dem PK 15,
- 21. Dezember 2013: Ausschreitungen im Schanzenviertel, St. Pauli und Altona und
- 28. Dezember 2013: Ausschreitungen vor dem und im Umfeld des PK 15,

in deren Verlauf schwerste Straftaten gegen die Gesundheit und das Leben von Menschen sowie gegen Sachen von bedeutendem Wert begangen wurden (vgl. Drucksache 20/10437, S. 1). In einer neuen Lagebeurteilung am 08. Januar 2014 stellte die Polizei Hamburg dann fest, dass die mit der Einrichtung des Gefahrengebietes verbundene Zielsetzung, die Begehung von Straftaten von erheblicher Bedeutung zu verhindern und die öffentliche Sicherheit zu gewährleisten, durch die polizeiliche Maßnahme weitgehend erreicht wurde. Das Gefahrengebiet wurde daher ab dem 09. Januar 2014 verkleinert und auf die -weitere- Umgebung der Polizeikommissariate 15 (Davidswache), 16 (Lerchenstraße) und 21 (Mörkenstraße) und auf die Zeit zwischen 18.00 Uhr und 06.00 Uhr beschränkt. Das Gefahrengebiet wurde schließlich am 13. Januar 2014 aufgehoben.

Das Ergebnis dieser Maßnahme ist in den nachfolgenden Tabellen zu sehen:

Abbildung 1: Maßnahmen im Gefahrengebiet im Zeitraum 04.-08. Januar 2014

Angehaltene Personen	Inaugenscheinnahmen	Identitätsfestellungen	Aufenthaltsverbote	Platzverweise	Gewahrsamnahmen	Straftaten
890	50	Nicht erhoben	190	13	65	35

Quelle: Drucksache 20/10437, S. 5.

Abbildung 2: Maßnahmen im verkleinerten Gefahrengebiet

Angehaltene Personen	Inaugen-scheinnahmen	Identitäts-festellungen	Aufenthalts-verbote	Platzverweise	Gewahrsamnahmen	Straftaten
237	96	237*	23	2	0	22

*Die Identitätsfeststellugen erfolgten durch das Vorzeigen von Ausweisdokumenten

Quelle: Drucksache 20/10446, S. 2.

Bis dato hatte die Polizei Hamburg bereits 51 Gefahrengebiete aus den unterschiedlichsten Gründen eingerichtet (Drs. 20/10437, S. 1), davon drei dauerhaft.

Die Ausweisung der o.g. Gefahrengebiete hat nicht nur zu erheblichen gesellschaftlichen Diskussionen geführt, sondern im Hinblick auf die Rechtsgrundlage und das informationelle Selbstbestimmungsrecht zentrale datenschutzrechtliche Fragestellungen aufgeworfen und war daher Gegenstand einer Prüfung durch unsere Behörde. Wir haben uns umgehend nach Bekanntgabe des ersten Gefahrengebietes an die Polizei Hamburg gewandt und um Darlegung der einzelnen Tatbestandsmerkmale des § 4 Abs. 2 PolDVG gebeten.

Das Ergebnis haben wir ausführlich in unserem Rechtsgutachten vom 02. April 2014 „Datenschutzrechtliche Bewertung des polizeilichen Gefahrengebiets im Bezirk Altona vom 4.-13.1.2014“ *https://www.datenschutz-hamburg.de/uploads/media/Gefahrengebiet_-_Datenschutzrechtliche_Bewertung_HmbBfDI.pdf* dargelegt und haben auf die mangelnde Bestimmtheit und Verhältnismäßigkeit der Rechtsgrundlage hingewiesen. Gleichzeitig haben wir in dem Gutachten aufgezeigt, wie eine verfassungskonforme Regelung aussehen könnte.

Im Hinblick auf die mangelnde Bestimmtheit ist entscheidend:

- Die Ausweisung eines Gefahrengebietes stellt für sich genommen schon ein Grundrechtseingriff dar, denn die Ausweisung eines Gebiets stellt zunächst die rechtlichen Voraussetzungen für einen zielgerichteten individuellen Eingriff in die Grundrechte Betroffener im Einzelfall durch die Polizei vor Ort dar. Die Ausweisung ermöglicht im vorgegebenen räumlichen und zeitlichen Rahmen eine Kontrolle durch die Polizei und eröffnet damit, in die Grundrechte der Freiheit der Person („anhalten“, „befragen“, Inaugenscheinnahme dulden oder ermöglichen) sowie in das Grundrecht der informationellen Selbstbestimmung („Identitätsfeststellung“, Datenerhebung und ggfs. Speicherung) auch verhaltensunabhängig einzugreifen. Damit wird durch die Entscheidung, ein bestimmtes Gebiet als Gefahrengebiet auszuweisen, der in der Norm enthaltene Eingriffstatbestand erst ausgelöst. Die Vorschrift setzt die vorangehende Ausweisung eines Gebiets durch die Polizei

denknotwendig voraus. Ohne Ausweisung eines Gebietes kann es keine erleichterten Identitätskontrollen geben. Die Befugnis zur Gebietsausweisung wird jedoch nicht ausdrücklich vom Gesetzgeber angeordnet. Auch fehlen Vorschriften, die die Rechtsnatur und das zugrundeliegende Verfahren der Ausweisung wie auch die Zuständigkeit der ausweisenden Stelle näher regeln. Die Befugnis, ein Gebiet für anlasslose polizeilichen Kontrollen zu schaffen, hätte der Gesetzgeber daher ausdrücklich in § 4 Abs. 2 PolDVG regeln müssen. Da eine gesetzliche Grundlage fehlt, kann der mit der Gebietsausweisung verbundene Eingriff nach Maßgabe des Vorbehalts des Gesetzes auch nicht lediglich auf eine interne Dienstanweisung gestützt werden.

Neben der nicht vorhandenen Bestimmung des Verfahrens und der Zuständigkeit fehlt insbesondere eine Regelung, wonach die Öffentlichkeit über die Ausweisung eines Gebietes vorab hinreichend informiert wird.

Dies bedeutet nicht, dass die einzelne Ausweisung eines Gebiets zwingend durch eine Rechtsnorm zu erfolgen hätte. Die Ausweisung eines Gebiets mit besonderen Eingriffskompetenzen setzt keine bestimmte Rechtsqualität, etwa eine Rechtsverordnung, voraus. Sie kann daher auch durch Verwaltungsakt in Gestalt einer Allgemeinverfügung erfolgen.

- Der Begriff der Lageerkenntnisse bezieht sich auf Umstände einer Örtlichkeit, die einen tatsächlichen rechtlichen Anknüpfungspunkt – und somit einen Anlass – für ein gesteigertes Risiko der Rechtsgutverletzung oder -gefährdung geben. Das Tatbestandsmerkmal verpflichtet die Polizei zu prüfen, ob tatsächliche Anhaltspunkte für eine gesteigerte Kriminalität bestehen. Es werden für die Bestimmung daher konkrete Umstände und Erkenntnisse vorausgesetzt, die nach polizeilicher Erfahrung darauf schließen lassen, dass in einem begrenzten Gebiet das Risiko der Begehung von Straftaten von noch unbekannten Personen droht bzw. gegenüber anderen Gebieten nachweislich erhöht ist. Bei der Eingriffsregelung des § 4 Abs. 2 PolDVG handelt es sich jedoch um eine Norm, die an Lageerkenntnisse der Polizei anknüpft und vorab eine Bewertung über das auszuweisende „bestimmte" Gebiet voraussetzt.

- Die örtliche und zeitliche Begrenzung, innerhalb derer Bewohner oder Besucher weitergehende Rechtsbeeinträchtigungen hinzunehmen haben, müssen den Normunterworfenen grundsätzlich bekannt werden.
  Dies ließe sich etwa durch eine gesetzliche Pflicht erreichen, die Ausweisung rechtzeitig in der Tageszeitung, im Internet, im Amtsblatt oder im Rahmen einer Verordnung im Gesetz- und Verordnungsblatt zu veröffentlichen. Nur so können die Betroffenen ihr Verhalten darauf abstellen und sich auf anlass- und verhaltensunabhängige Identitätsfeststellungen einschließlich der in der Öffentlichkeit durchführbaren Inaugenscheinnahme von mitgeführten Gegenständen in dem

ausgewiesenen Gebiet vorbereiten.

Im Rahmen der Verhältnismäßigkeit sind nachfolgende Punkte zu beachten:

- Von Kontrollen in Gefahrengebieten darf nicht jede beliebige Person erfasst werden, die sich im öffentlichen Raum bewegt. Die Kontrolle muss sich vorab vielmehr an einer lageabhängigen Zielgruppe orientieren.

  Danach muss eine Ausweisung von Gefahrengebieten bereits vorab eine relevante Gruppe von Zielpersonen benennen, die aufgrund der Ausweisung des Gefahrengebietes in den Fokus polizeilicher Maßnahmen zu nehmen sind.

- Es ist ein Gebot der Angemessenheit, Betroffene von der Ausweisung eines Gebiets so zu informieren, dass diese sich darauf einstellen können. Die fehlende Transparenz einer Regelung zur Gebietsausweisung stellt daher einen unverhältnismäßigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen dar.

- Die Speicherung und weitere Verarbeitung der im Zuge von Identitätsfeststellungen in einem Gefahrengebiet erhobenen Daten nach § 4 Abs. 2 PolDVG ist von den §§ 14, 15, 16 Abs. 1 PolDVG jedenfalls bei unbeteiligten Personen, gegen die sich nach der Identitätsfeststellung und ggf. der Inaugenscheinnahme mitgeführter Gegenstände keinerlei Anlass zu polizeilichen oder strafprozessualen Maßnahmen ergibt, nicht gedeckt.

Das Verwaltungsgericht (VG) Hamburg hat im Zusammenhang der Ausweisung eines Gefahrengebietes im Schanzenviertel anlässlich der sogenannten Walpurgisnacht am 30. April 2011 die Regelung in § 4 Abs. 2 PolDVG alte Fassung – diese entspricht im Wesentlichen der heutigen Fassung, wobei die „vorbeugende Bekämpfung" von Straftaten durch „Verhütung" von Straftaten ersetzt wurde – im Grundsatz bestätigt (Verwaltungsgericht Hamburg, Urteil vom 02. Oktober 2012 – Az.: 5 K 1236/11). Im Ergebnis hat es keine durchgreifenden verfassungsrechtlichen Bedenken gesehen (VG Hamburg, a.a.O, Rn. 43).

Zwar werde nach Auffassung des Gerichts mit der Ermächtigungsgrundlage in das Recht auf informationelle Selbstbestimmung, in das Recht auf Freiheit der Person und in die allgemeine Handlungsfreiheit eingegriffen, diese seien jedoch gerechtfertigt. Überdies sei die Norm noch hinreichend bestimmt, mit dem Wesentlichkeitsgebot vereinbar und verstoße nicht gegen den Grundsatz der Verhältnismäßigkeit (VG Hamburg, a.a.O, Rn. 49 ff.). Im Hinblick auf das Bestimmtheitsgebot sei der Zweck der Datenerhebung – die Verhütung von Gefahren – hinreichend bestimmt (VG Hamburg, a.a.O, Rn. 53). Der Begriff der „erheblichen Straftaten" genüge ebenso wie der der „konkreten Lageerkenntnisse" dem Bestimmtheitsgrundsatz, denn erstere sei in § 1 Abs. 4

PolDVG näher bestimmt und richterlicher Kontrolle zugänglich (VG Hamburg, a.a.O, Rn. 55) und letztere der richterlichen Konkretisierung und Überprüfung zugänglich (VG Hamburg, a.a.O, Rn. 59).

Die Entscheidung des VG Hamburg ist, wie sich im Nachhinein auch durch die Entscheidung des Oberverwaltungsgericht (OVG) Hamburg (Oberverwaltungsgericht Hamburg, Urteil vom 13. Mai 2015 – Az.: 4 Bf 226/12) zeigte, rechtsfehlerhaft.
Unserer Meinung ist auch im Wesentlichen das Oberverwaltungsgericht Hamburg in seiner Entscheidung vom 13. Mai 2015 – Az.: 4 Bf 226/12 gefolgt. Neben der eigentlichen Entscheidung – dass in dem besagten Fall die Identitätsfeststellung und Rucksackkontrolle rechtwidrig waren – ist auch das OVG zu dem Ergebnis gelangt, dass § 4 Abs. 2 S. 1 PolDVG als Rechtsgrundlage für Maßnahmen in Gefahrengebieten wegen Verletzung des Grundrechts auf informationelle Selbstbestimmung verfassungswidrig ist. Das Gericht bemängelte insbesondere, dass die Norm zum einen nicht klar genug die Voraussetzungen für die Ausweisung eines Gefahrengebiets vorgebe. Vielmehr bleibe es weitgehend der Polizei überlassen zu entscheiden, ob und für wie lange ein Gefahrengebiet ausgewiesen und dort Personen verdachtsunabhängig überprüft werden könnten. Auch erlaube das Gesetz Eingriffsmaßnahmen von erheblichem Gewicht zur Abwehr bloß abstrakter Gefahren gegenüber Personen, ohne dass diese zuvor einen konkreten Anlass für eine gegen sie gerichtete polizeiliche Maßnahme gegeben haben müssen.

Allerdings kann das OVG ein Gesetz für nichtig erklären, denn eine entsprechende Verwerfungskompetenz steht nur den Verfassungsgerichten zu. Zu einer Vorlage an das Bundes- bzw. an das Hamburgische Verfassungsgericht kam es in diesem Verfahren jedoch nur deshalb nicht, weil die in Frage stehende Ermächtigungsnorm für die Überprüfung des vorliegenden Rechtsstreits gar nicht entscheidungserheblich war. Mit dem Urteil des OVG wachsen die verfassungsrechtlichen Zweifel an der derzeitigen Ermächtigungsgrundlage zur Ausweisung von Gefahrengebieten in Hamburg. Das Instrument macht Stadtgebiete zu Sonderzonen. Verdachts- und anlassunabhängige Kontrollen von unbescholtenen Bürgerinnen und Bürgern greifen nicht unwesentlich in deren informationelle Selbstbestimmungsrechte ein. Die Gerichtsentscheidung gibt daher weiteren Anlass, die derzeit geltende Norm - wie im aktuellen Koalitionsvertrag vorgesehen - auf den Prüfstand zu stellen.

Schließlich hat die Polizei Hamburg bereits mehrfach geäußert, dass das o.g. OVG Urteil umfangreich geprüft werde (vgl. u.a. Drs. 21/580) und in Abstimmung mit der Behörde für Justiz Vorschläge für eine Neuregelung des § 4 Abs. 2 PolDVG erarbeite (vgl. u.a. Drs. 21/1150).

Diese liegen – wie unsere Anfrage Ende Oktober an die BIS ergeben hat – bislang nicht vor. Gleichwohl existieren weiterhin Gefahrengebiete. Eine zeitnahe Anpassung der Rechtslage ist rechtsstaatlich gefordert.

1.3 Bodycams

Im Berichtszeitraum wurde für Teile der Polizei das Tragen von Schulterkameras eingeführt. Wir haben dies von der Ankündigung über die Schaffung einer Rechtsgrundlage bis zum Test in Einsatzsituationen kontinuierlich begleitet.

Im Jahr 2014 überraschte uns die Polizei mit der Ankündigung, zukünftig sog. Bodycams, also tragbare Kameras auf den Schultern von Polizeivollzugsbediensteten anzubringen, um diese in Konfliktsituationen durch Aufnahmen vor gewalttätigen Übergriffen zu schützen. Hintergrund waren Berichte aus Hessen, wo die Polizei diese Maßnahme angeblich erfolgreich einsetzt. Schnell kam die Polizei zu der Erkenntnis, dass es hierfür einer eigenen Rechtsgrundlage bedarf und man dieses neue technische Instrument nicht auf der Grundlage von § 8 Abs. 5 PolDVG-alt einsetzen kann. Daher wurde der bestehende § 8 Abs. 5 PolDVG geändert, um zukünftig auch den Einsatz von Bodycams zu erlauben. Die neue Vorschrift lautet nun: „Die Polizei darf bei der Durchführung von Maßnahmen zur Gefahrenabwehr oder zur Verfolgung von Straftaten oder Ordnungswidrigkeiten in öffentlich zugänglichen Bereichen personenbezogene Daten durch den offenen Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen erheben, wenn dies nach den Umständen zum Schutz von Vollzugsbediensteten oder Dritten gegen eine Gefahr für Leib oder Leben erforderlich ist. Aufzeichnungen sind unzulässig in Bereichen, die der Ausübung von Tätigkeiten von Berufsgeheimnisträgern nach § 53 Abs. 1 StPO dienen. Absatz 4 Sätze 2 und 4 gilt entsprechend.“ Der dritte Satz bedeutet, dass die Maßnahme auch durchgeführt werden darf, wenn Dritte unvermeidbar betroffen werden und Bild- und Tonaufzeichnungen spätestens nach vier Tagen zu löschen sind, soweit sie nicht für Zwecke der Strafverfolgung benötigt werden.

Wir standen der Einführung dieser neuen Maßnahme von Anfang an nicht ablehnend gegenüber, insbesondere soweit es um die Schaffung einer eigenen Rechtsgrundlage ging. Von der Art der Umsetzung sind wir allerdings nicht überzeugt. § 8 Abs. 5 PolDVG-neu leidet unseres Erachtens unter mehreren Fehlern. Die „technischen Mittel“ im Gesetzestext sind nicht begrenzt auf Bodycams. Die Gesetzesbegründung geht davon aus, dass es sich „gegenwärtig“ um Bodycams handelt. Gleichzeitig soll aber auch der Einsatz von Dashcams in Polizeifahrzeugen dadurch ermöglicht werden. Theoretisch rechtfertigt die Norm auch den Einsatz von Drohnen, Handykameras oder Google Glass. Die deeskalierende Wirkung von Videoaufnahmen ist soweit bekannt noch nie wissenschaftlich untersucht und dann belegt worden. Wir haben uns dem Argument trotzdem nicht verschlossen. Hier kommt der Evaluation eine besondere Bedeutung zu. Diese sollte durch eine unabhängige Stelle erfolgen. Die Anfertigung von Tonaufnahmen halten wir für nicht erforderlich und daher unverhältnismäßig. Es darf

nicht soweit kommen, dass Bürgerinnen und Bürger sich scheuen, Polizeivollzugsbedienstete anzusprechen. Ferner ist unklar, vor welchen Bedrohungen Polizeivollzugsbedienstete durch Tonaufnahmen geschützt werden sollen. Außerdem halten wir in diesem Fall die kurze Speicherfrist von maximal vier Tagen für problematisch. Sie wird in aller Regel verhindern, dass Aufnahmen, die einen disziplinarrechtlichen Vorwurf gegen einen Polizeivollzugsbediensteten belegen können, noch rechtzeitig zu verwerten sind. Auch werden Betroffene wohl nicht von ihrem Auskunftsanspruch Gebrauch machen können, da die Daten so schnell zu löschen sind und aufgrund der strengen Zweckbindung nicht für andere Zwecke - auch nicht im Interesse des Betroffenen - verwendet werden dürfen. Es gibt auch keinen Anspruch auf Herausgabe der Bilder.

Leider sind unsere Bedenken im Gesetzgebungsverfahren nicht aufgenommen und die Norm ist ohne Änderungen verabschiedet worden. Das System wird nun so eingesetzt. Wir werden die Entwicklung weiter kritisch begleiten. Allerdings haben wir bislang noch keine Eingabe wegen eines Bodycam-Einsatzes erhalten.

1.4 Prüfung der Antiterrordatei beim Landeskriminalamt Hamburg

Protokolldaten müssen den Datenschutzbeauftragten so zur Verfügung gestellt werden, dass sie einer datenschutzrechtlichen Kontrolle zugänglich sind. Die Anfragen an die Antiterrordatei innerhalb der Polizei per E-Mail weisen technische Mängel auf, da diese nicht verschlüsselt werden.

Im 24. TB, III.2.2 haben wir ausführlich über die Entscheidung des Bundesverfassungsgerichts (BVerfG) zur Antiterrordatei (ATD) (BVerfG, Urteil v. 24. April 2013 - 1 BvR 1215/07) und ihre Folgen berichtet. Dem Gesetzgeber wurde eine Überarbeitungsfrist der beanstandeten Regelungen nach den Vorgaben des Gerichts bis zum 31.Dezember 2014 eingeräumt.

Zwischenzeitlich wurde das Gesetz zur Änderung des Antiterrordateigesetzes und anderer Gesetze verabschiedet und am 18. Dezember 2014 im Bundesgesetzblatt veröffentlicht (BGBl. I 2014, 2318). Zum 01. Januar 2015 ist das geänderte Gesetz in Kraft getreten.

§ 10 Abs. 2 Antiterrordateigesetz (ATDG) statuiert nunmehr für die Datenschutzbeauftragten des Bundes und der Länder eine verpflichtende, mindestens alle zwei Jahre durchzuführende Datenschutzkontrolle.

Das BVerfG führt in dem o.g. Urteil aus: „In Blick auf den Charakter der Antiterrordatei als eine Bund und Länder übergreifende Verbunddatei […] obliegt deren Kontrolle den Landesbeauftragten. Allerdings entspricht es der Antiterrordatei als Verbunddatei,

dass es den Datenschutzbeauftragten gestattet sein muss, zusammenzuarbeiten und sich etwa im Wege der Amtshilfe durch Delegation oder Ermächtigung bei der Wahrnehmung ihrer Befugnisse gegenseitig zu unterstützen. Ebenfalls ist zu gewährleisten, dass im Zusammenspiel der verschiedenen Aufsichtsinstanzen auch eine Kontrolle der durch Maßnahmen nach dem Artikel 10-Gesetz gewonnenen Daten - die in einer Datei, welche maßgeblich auch vom Bundesnachrichtendienst befüllt wird, besondere Bedeutung haben - praktisch wirksam sichergestellt ist. Wenn der Gesetzgeber eine informationelle Kooperation der Sicherheitsbehörden vorsieht, muss er auch die kontrollierende Kooperation zugunsten des Datenschutzes ermöglichen. (BVerfG, a.a.O. Rn. 216.).

Daher haben die Datenschutzbeauftragten des Bundes und der Länder die Unterarbeitsgruppe „Erfahrungsaustausch Prüfung der Antiterrordatei (AG ATD)“ gegründet, die erstmals im Dezember 2014 in Berlin getagt hat. Diesen Termin konnten wir nutzen, um uns gegenseitig über die Herangehensweise und Strukturierung der Prüfung auszutauschen. Darüber hinaus konnten wir weitere Termine im Arbeitskreis nutzen, um erste Prüfergebnisse auszutauschen.

Anfang November 2014 fand zunächst beim Landeskriminalamt Hamburg (LKA) eine Informationsveranstaltung statt, bei der uns u.a. auch zur Vorbereitung der weiteren Prüfung der Aufbau und die Funktionsweise der ATD sowie die technischen Rahmenbedingungen vor Ort erläutert wurden. Im Anschluss an dieses Gespräch konnten wir uns einen ersten Eindruck der Datei sowie der technisch-organisatorischen Maßnahmen in dem ATD-Betriebsraum – der Raum, in dem das technische Equipment sowie ATD-relevante Unterlagen gesondert aufbewahrt werden – verschaffen.

Bereits zu diesem Zeitpunkt konnten wir festhalten, dass der ATD-Betriebsraum lediglich für besonders ermächtigte Personen im LKA, die über eine gesonderte Zugangsberechtigung und Zugangsdaten sowohl für das Betreten des ATD-Betriebsraumes als auch Nutzung der dortigen Computer verfügen, zugänglich war. Überdies versicherte uns das LKA, dass alle Mitarbeiter den notwendigen Geheimhaltungsgrad haben, bevor sie Zugang zu den ATD-Informationen erhalten, und dass eine Eingabe von Daten in die ATD ausschließlich durch überprüfte und ermächtigte Mitarbeiter des Staatsschutzes erfolge. Letzteres konnten wir anhand der uns zur Verfügung gestellten Protokolldaten bestätigen, denn die Datenverarbeitung erfolgte nach diesen Protokollen ausschließlich durch ermächtigte Personen.

Für problematisch halten wir allerdings, dass Anfragen des LKA Hamburg, ob Informationen zu einzelnen Personen in der ATD gespeichert sind, per E-Mail an die zugriffsberechtigten Mitarbeiterinnen und Mitarbeiter versendet werden. Diese E-Mails werden nicht durch die für den internen Mailverkehr zur Verfügung stehende Ende-zu-Ende-Verschlüsselung geschützt.

Dies führt dazu, dass die Administratoren bei Dataport mit wenigen Klicks Zugriff auf die hoch sensiblen Inhalte dieser Mails nehmen können. Das Risiko, dass ein solcher unzulässiger Zugriff entdeckt werden könnte, ist äußerst gering, da keine automatisiert auswertbare Protokollierung der Zugriffe erfolgt (vgl. VI 1.4). Die Polizei hat uns mitgeteilt, dass sie die Hamburg weite Vorgabe aus der IT-Architekturrichtlinie nicht einhalten wird, an allen IT-Arbeitsplätzen die Verschlüsselungskomponente RMS (Rights Management System) bereitzustellen. Wir haben den Polizeipräsidenten mit der Bitte angeschrieben, den gravierenden Mangel unverzüglich abzustellen.

Für die weitere Prüfung – die Protokollauswertung – forderten wir noch im Dezember 2014 beim LKA die Protokolldaten, die nach § 9 Abs. 1 ATDG für jeden Zugriff für die Datenschutzkontrolle zu erstellen sind, an. Aus unserer AG ATD hatten wir erfahren, dass auf dem Protokollserver des Bundeskriminalamtes (BKA) sogenannte Reports zur Ausweisung bestimmter Auswertungskriterien programmiert wurden, wie neu angelegte Objekte, geänderte Objekte, gelöschte Objekte, angesehene Objekte und Suchanfragen. Ende Dezember 2014 forderten wir diese Protokolle für die letzten fünf Jahre (Zeitraum: 30. November 2009 – 30. November 2014) an, denn aus der Errichtungsanordnung, die uns das LKA zuvor für die Prüfung überlassen hatte, wussten wir, dass bestimmte Protokolle mindestens fünf Jahre aufbewahrt werden. Wegen der anstehenden Feiertage hatten wir dem LKA eine großzügige Frist gesetzt bis Ende Januar 2015.

Am 29. Januar 2015 informierte uns das LKA, dass die Protokolldaten eingetroffen seien. Sie befänden sich auf einer CD, die nach der Verschlusssachenanweisung mit VS-geheim - die zweithöchste Einstufung – eingestuft war, und umfassen ca. 30.000 Seiten. Dies bedeutete für uns, dass wir die Protokolldaten nicht in unseren Räumlichkeiten prüfen konnten, da unsere Dienststelle nicht über die für die ATD erforderliche technische Ausstattung verfügt. Aus Sicherheitsgründen durften die Protokolldaten daher nur in dem ATD-Betriebsraum eingesehen werden. Bereits absehbar war zu diesem Zeitpunkt, dass angesichts des Umfangs die Auswertung der Protokolle kaum machbar sein wird, so dass wir nach erneuter interner Besprechung vier Zeiträume von jeweils sechs Monaten auswählten, die wir genauer prüfen wollten. Die Zeiträume wurden dabei so gewählt, dass u.a. ein Zeitraum der Anfangszeit der ATD, ein weiterer Zeitraum im zeitlichen Zusammenhang mit dem Urteil des BVerfG sowie ein Zeitraum jüngeren Datums erfasst war.

Im März 2015 erhielten wir eine weitere CD mit den Protokolldaten für den eingegrenzten Zeitraum. Die CD war mit VS-nur für den Dienstgebrauch (nfD) – die niedrigste Einstufung nach der Verschlusssachenanweisung – eingestuft. Dies bedeutete für uns, dass wir die Prüfung in unserer Dienststelle durchführen konnten. Sie enthielt nur noch 16.600 Seiten. Auf ca. 14.500 Seiten der Protokolle waren – abgesehen von einem Aktualisierungsdatum – keine inhaltlichen Änderungen erkennbar. Vielmehr waren alter und neuer Wert identisch.

Unsere daraufhin mit Blick auf die Aussagekraft der Protokolle an das LKA gerichtete Anfrage, warum auf den 14.500 Seiten keine inhaltlichen Änderungen erkennbar waren, konnte uns zunächst nicht beantwortet werden. Vielmehr wurde unsere Anfrage an das BKA zur Beantwortung weitergeleitet. Wir erhielten hierauf die Information, dass die Protokolle ohne inhaltliche Änderungen durch die Quelldatei – das ist die Datei, in die die Daten eingegeben und in bestimmten Zeiträumen in die ATD überspielt werden– erzeugt würden. Programmseitig sei vorgesehen, dass jegliche Änderungen in der Quelldatei – auch ohne ATD Relevanz – protokolliert würden.

Trotz der hohen Anzahl der Protokolldaten setzten wir die Prüfung fort, indem wir beispielsweise überprüften, ob die Vorgaben des BVerfG umgesetzt werden oder aber gelöschte Personen (z.B. Kontaktpersonen) erneut angelegt wurden (z.B. als politisch motivierte Gewalttäter). Solche Abgleiche sind insbesondere geeignet, mögliche datenschutzrechtliche Verstöße zu erkennen. Als Indiz für mögliche datenschutzrechtliche Verstöße könnte z.B. die Feststellung der Häufigkeit der Zugriffe auf bestimmte Personen herangezogen werden. Die Abgleiche eignen sich auch, um Ungereimtheiten, wie z.B. nicht nachvollziehbare Änderungen, zu finden, um dann die konkrete Akte selbst zu überprüfen.

Im Fortgang der Prüfung stellten wir weitere nicht nachvollziehbare Protokollierungen fest.

In mehreren Telefonaten und Gesprächen vor Ort haben wir dem LKA mitgeteilt, dass die Protokolldaten in einer kaum auswertbaren Form erstellt werden. Dies ist insoweit nicht nachvollziehbar, weil nach Auffassung des BVerfG für eine effektive Datenschutzkontrolle erforderlich ist, „dass Zugriffe und Änderungen des Datenbestandes vollständig protokolliert werden. Dabei muss durch technische und organisatorische Maßnahmen sichergestellt werden, dass die Daten den Datenschutzbeauftragten in praktikabel auswertbarer Weise zur Verfügung stehen und die Protokollierung hinreichende Angaben für die Zuordnung zu dem zu kontrollierenden Vorgang enthält" (BVerfG, a.a.O. Rn. 215).

Dies kann nach bisheriger Prüfung nicht festgestellt werden.

Die Rücksprache mit den Kollegen anderer Bundesländer ergab, dass auch dort ähnliche Fragestellungen aufgekommen sind. Vor diesem Hintergrund haben wir über die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) einen Termin Anfang Dezember 2015 mit dem BKA vereinbart, bei dem sich alle Datenschutzbeauftragten der Länder und die BfDI die Protokollierung haben erläutern lassen. Diesen Termin gilt es noch auszuwerten.

Im Rahmen der Aktenanalyse haben wir uns die Akten zu den gespeicherten Personen zeigen lassen. Wir hatten zuvor eine Stichprobe von sechs Personen genommen. Dabei

handelte es sich um Personen, die zuvor in der Protokolldatenauswertung aufgefallen sind, z.B. aufgrund der Häufigkeit der Zugriffe auf ihre Datensätze, aufgrund häufig vorgenommener Änderungen in ihren Datensätzen oder aber weil eine Person, die zunächst als Kontaktperson gespeichert war, nunmehr als Gefährder oder Gefährderin erfasst ist.

Die stichprobenartige Überprüfung der in die Antiterrordatei gespeicherten Datensätze hat keine Mängel ergeben. Die Einspeicherungen waren jeweils fachlich nachvollziehbar und inhaltlich gründlich dokumentiert. In einem Fall allerdings musste das LKA die inhaltliche Begründung der Speicherung nachliefern, weil aus der Aktenlage zunächst nicht hervorging, warum die Person weiterhin als ATD relevante Person in der ATD erfasst werden soll.

Ein abschließendes Gespräch mit dem LKA sowie die Erstellung des Prüfberichts steht noch aus.

Die oben beschriebene Prüfung wird im nächsten Berichtszeitraum auch beim Landesamt für Verfassungsschutz (LfV) durchgeführt werden müssen, da dieses ebenfalls gemäß § 1 Abs. 1 ATDG eine beteiligte Behörde der ATD ist. Allerdings zeichnet sich bereits jetzt schon ab, dass es unserer Behörde große Schwierigkeiten bereiten wird, die vom BVerfG auferlegte und nunmehr gesetzlich verankerte Prüfpflicht aufgrund des Personaldefizits mindestens alle zwei Jahre zu erfüllen.

Das BVerfG hat in seiner Entscheidung zur ATD ausdrücklich betont, dass angesichts der Kompensationsfunktion der aufsichtlichen Kontrolle für den schwach ausgestalteten Individualrechtsschutz deren regelmäßiger Durchführung besondere Bedeutung zukomme und solche Kontrollen in angemessenen Abständen – deren Dauer ein gewisses Höchstmaß, etwa zwei Jahre, nicht überschreiten darf – durchzuführen sei; dies sei bei der Ausstattung der Aufsichtsbehörde zu berücksichtigen (BVerfG, a.a.O., Rn. 217).

Wir werden im nächsten Berichtszeitraum über die Prüfung weiter berichten.

1.5 Verdeckte Ermittlungen im Polizeirecht

Ist eine offene Aufklärung aussichtslos und ein verdeckter Einsatz von Polizeibeamtinnen oder -beamten verhältnismäßig, kann auch eine verdeckte Ermittlerin oder ein verdeckter Ermittler eingesetzt werden. Beobachter für Lagebeurteilungen bedarf es daher nicht mehr. Zwar wird durch die verdeckte Datenerhebung durch die Polizei regelmäßig und intensiv in das Grundrecht auf informationelle Selbstbestimmung der Personen eingegriffen, denn es werden heimlich – d.h. ohne Erkennbarkeit, dass es sich um eine polizeiliche Maßnahme handelt – personenbezogene Daten erhoben. Neben einer ausdrücklichen Rechtsgrundlage, die hinreichend bestimmt und verhältnismäßig sein muss, bedarf es auch einer hinreichend bestimmten Anordnung. Anderenfalls führt der Einsatz zur Rechtswidrigkeit insgesamt, selbst wenn der Einsatz materiell-rechtlich gerechtfertigt war.

In diesem Berichtszeitraum haben wir uns intensiv mit dem Einsatz von verdeckt ermittelnden Polizeibeamtinnen und -beamten beschäftigt. Hintergrund hierfür waren zwei Fälle, die - Anfang November 2014 und Ende August 2015 - aufgedeckt wurden.
Im ersten Fall handelt es sich um eine verdeckt ermittelnde Polizeibeamtin, die unter einer ihr auf Dauer angelegten, veränderten Identität (Legende) im Umfeld der Roten Flora im Zeitraum 01. August 2001 bis zum 31. März 2006 zur Gefahrenabwehr als sogenannte Beobachterin zur Lagebeurteilung (BfL) und zur Strafverfolgung als verdeckte Ermittlerin nach der Strafprozessordnung (StPO) eingesetzt wurde. Für den Einsatz als verdeckte Ermittlerin lagen Beschlüsse von Ermittlungsrichtern vor, so dass sich unsere Überprüfung auf die Tätigkeit als BfL fokussierte.
Im zweiten Fall wurde die verdeckt ermittelnde Polizeibeamtin ausschließlich zur Gefahrenabwehr als verdeckte Ermittlerin gemäß § 12 Polizeidatenverarbeitungsgesetz (PolDVG) in den Jahren 2009 bis 2012 eingesetzt.

Die Umstände und die Einsätze beider Polizeibeamtinnen beschäftigte unsere Behörde intensiv. In sieben Sitzungen des Innenausschusses (18.11.2014, 09.12.2014, 07.01.2015, 15.06.2015, 28.08.2015, 15.10.2015, 05.11.2015) wurden beide Fälle im Beisein unserer Behörde im Rahmen der Selbstbefassung gem. § 53 Absatz 2 der Geschäftsordnung der Hamburgischen Bürgerschaft aufgearbeitet.
Beide Fälle erforderten intensive Prüfungen, Gespräche mit der Behörde für Inneres (BIS) und der Polizei Hamburg sowie umfangreiche Auswertungen. Zudem haben wir in beiden Fällen eine datenschutzrechtliche Prüfung einiger - für die Einsätze relevanter - Unterlagen bei der in unserem Zuständigkeitsbereich liegenden Polizei Hamburg vorgenommen.

Dazu im Einzelnen:
Zu dem Einsatz der Polizeibeamtin als Beobachterin für Lagebeurteilung (BfL):

Zum Zeitpunkt des Bekanntwerdens lag der Einsatz bereits fast zehn Jahre zurück. Die Aufbewahrungsfristen für viele Unterlagen waren bereits abgelaufen und diese vernichtet. Eine Rekonstruktion des Falles erschien zu diesem Zeitpunkt kaum möglich. Daher hatte die BIS zur Sachverhaltsaufklärung und -darstellung eine Arbeitsgruppe zusammengestellt, die alle in Betracht kommenden Aktenbestände der Polizei Hamburg daraufhin überprüft hat, ob sich in diesen Unterlagen Akten befanden, die sich aufgrund ihres Kontextes, der Legendierung oder einer sonstigen Kennzeichnung auf den fraglichen Einsatz beziehen könnten. Es handelte sich hierbei insbesondere um Akten der Staatsschutzabteilung des Landeskriminalamtes und des Fachstabes des Landeskriminalamtes. Daher wurden alle Aktenbestände des Landesamtes für Verfassungsschutz überprüft, in denen die jeweiligen Beobachtungsbereiche eine Speicherung von Informationen der verdeckt operierenden Polizeibeamtin möglich erscheinen ließen. Soweit die in den Lageberichten enthaltenen Informationen für die Aufgabenwahrnehmung des Landesamtes für Verfassungsschutz erforderlich erschienen, wurden diese auch dorthin übermittelt.

Die BIS hat in der Sitzung des Innenausschusses am 09.12.2014 erste Ergebnisse seit der Einrichtung dieser Arbeitsgruppe vorgetragen:
Der Einsatz der Beamtin als BfL erfolgte nach Aussage des Senates auf der Grundlage der entsprechenden Anwendung des § 2 Abs. 3 S. 3 PolDVG konkretisiert durch die Dienstanweisung vom 26.04.2001 „Einsatz von Beobachtern für Lagebeurteilung des LKA 8. Diese Dienstanweisung wurde anlässlich des Einsatzes eines BfL (damalige Bezeichnung Verdeckte Aufklärer (VA)) aus dem Jahr 1998 mit dem damaligen Hamburgischen Datenschutzbeauftragten erarbeitet, da der Einsatz eines nicht offen ermittelnden Polizeibeamten weder spezialgesetzlich geregelt war, noch Rechtsprechung und Literatur zum damaligen Zeitpunkt vorlagen, die den Einsatz eines BfL grundrechtskonform abstecken.

Die Dienstanweisung legte dabei die Voraussetzungen für den Einsatz fest und grenzte insbesondere durch Regelungen zum Gebrauch einer Legende und durch ein grundsätzliches Verbot des Betretens von Wohnung diese Einsatzform von den Befugnissen eines verdeckten Ermittlers nach § 12 PolDVG ab. Insbesondere aber regelte sie auch, dass

- die Tätigkeit von BfL zur Gewinnung von Lagebildern über Aktivitäten in bestimmten Szenen statthaft ist, wenn in den Berichten der BfL keine auf bestimmte Personen bezogene oder beziehbare Daten enthalten sind.

Auch wenn unsere heutige Bewertung des Einsatzes von BfL von der seinerzeitigen abgestimmten Dienstanweisung abweicht (s.u.), haben wir diese unserer Prüfung zugrunde gelegt.

Die BIS hatte beim Landesamt für Verfassungsschutz (LfV) Lageberichte, die für deren Aufgabenwahrnehmung erforderlich waren und dorthin übermittelt wurden, vorgefun-

den. Nach Auffassung der BIS seien unter den Lageberichten – die der BfL zweifelsfrei zugeordnet werden konnten – lediglich zwei, die personenbezogene Daten enthielten. Dabei handele es sich um eine namentliche Benennung eines zu einer öffentlichen Veranstaltung eingeladenen Gastes in einem Szenepapier mit unbekanntem Autor und in einem anderen Fall um eine als Anmelder einer Versammlung angefragte Person. Weitere personenbezogene Daten seien jedoch nicht enthalten.

Am 06.01.2015 haben wir eine Prüfung der noch vorhandenen 70 Berichte der BfL beim LfV vorgenommen. Der Schwerpunkt der Prüfung lag bei der Frage, ob die Dienstanweisung für den Einsatz von BfL eingehalten wurde. Insbesondere ging es darum zu erfahren, ob personenbezogene oder personenbeziehbare Daten in den Berichten, die aus dem Einsatz der BfL herrühren, gespeichert wurden. Die Prüfung hat ergeben, dass entgegen der Dienstanweisung die Berichte neben den zwei benannten auch weitere personenbezogene und personenbeziehbare Daten enthalten. Das Ergebnis der Prüfung haben wir in der öffentlichen Sitzung des Innenausschusses der Hamburgischen Bürgerschaft am 07.01.2015 vorgetragen (Drs. 20/35 vom 07.01.2015, S. 25 ff.).

Rechtlich ist hierzu Folgendes anzumerken: Die gesetzliche Situation hat sich seit der Erarbeitung der Dienstanweisung nicht geändert. Angesichts der zwischenzeitlich detailliert vorgenommenen datenschutzrechtlichen Beurteilung einzelner Datenverarbeitungsprozesse entspricht die seinerzeitige Dienstanweisung nicht mehr der aktuellen rechtlichen Bewertung. Einigkeit besteht insoweit, dass der Einsatz der BfL nicht auf die bestehenden Vorschriften zu den verdeckten Ermittlerinnen und Ermittlern, § 12 PolDVG gestützt werden kann.

Im Hinblick auf die Datenverarbeitungsprozesse gibt es Änderungen in der Rechtsprechung, die zwar nicht originär die BfL-Tätigkeit betreffen, sich jedoch unmittelbar auf die Aufgabenwahrnehmung der Polizei in Abgrenzung zu den Nachrichtendiensten auswirken (vgl. zuletzt BVerfG, Urteil vom 24. April 2013 – 1 BvR 1215/07 –, BVerfGE 133, 277-377). So stellt das Bundesverfassungsgericht klar, dass die Rechtsordnung zwischen einer grundsätzlich offen arbeitenden Polizei, die auf eine operative Aufgabenwahrnehmung hin ausgerichtet und durch detaillierte Rechtsgrundlagen angeleitet ist, und den grundsätzlich verdeckt arbeitenden Nachrichtendiensten unterscheidet, die auf die Beobachtung und Aufklärung im Vorfeld zur politischen Information und Beratung beschränkt sind und sich deswegen auf weniger ausdifferenzierte Rechtsgrundlagen stützen können. Eine Geheimpolizei ist nicht vorgesehen (BVerfG a.a.O., Rn. 122).

Darüber hinaus ist der Begriff der personenbezogenen Daten von zentraler Bedeutung für den Anwendungsbereich des Hamburgischen Datenschutzgesetzes (HmbDSG). Nur wenn personenbezogene Daten verarbeitet werden, ist der Anwendungsbereich des HmbDSG überhaupt eröffnet (vgl. § 1 HmbDSG).

Gemäß § 4 Abs. 1 HmbDSG sind personenbezogene Daten Einzelangaben über persön-

liche oder sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen (zu dem Personenbezug siehe HmbDSG Gesetzestext und Erläuterungen, zu § 4, S. 53 sowie Erwägungsgrund 26 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Abl. EG 1995, L 281/31) - Datenschutz-Richtlinie). Bei der Entscheidung, ob eine Person bestimmbar ist, sind alle Mittel zu berücksichtigen, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. Da auch Möglichkeiten Dritter zur Personenbestimmung einzubeziehen sind, ist auch das Zusatzwissen Dritter von Bedeutung. An der Bestimmbarkeit fehlt es somit nur, wenn die beschaffende Stelle einschließlich der für sie handelnden Personen zu keinem Zeitpunkt in der Lage ist, die Bezugsperson zu bestimmen (Damman in Simitis, 8. Aufl., § 3 Rn. 108). Das entscheidende ist aber, dass es – ohne dass es um die Berücksichtigung eines Zusatzwissens von Dritten geht – auf die Daten verarbeitende Stelle an sich ankommt, nicht aber auf einzelne Personen. Das bedeutet, dass für die Daten verarbeitende Stelle ein Personenbezug zu bejahen ist, wenn das entsprechende Wissen bei einem Mitglied dieser Daten verarbeitenden Stelle vorhanden ist. Dann besitzt auch die Daten verarbeitende Stelle selber bereits das Wissen für den Personenbezug.

Die beim LfV geprüften Berichte der BfL enthalten demnach mehr als zwei personenbezogene/personenbeziehbare Daten, da die BfL selbst und auch die übrigen Teilnehmer einer Veranstaltung die Teilnehmenden bestimmen können. Da somit die BfL selbst und damit auch als Teil der Daten verarbeitenden Stelle den Personenbezug herstellen kann, ist der Personenbezug für die zu betrachtenden Daten verarbeitenden Stellen insgesamt gegeben, unabhängig davon, welche Person der Daten verarbeitenden Stelle konkret die Kenntnis erhalten hat. Entscheidend ist, dass die Daten verarbeitende Stelle das Wissen hat, so dass es auf etwaiges Zusatzwissen Dritter gar nicht mehr ankommt. Die Daten verarbeitende Stelle verarbeitete, insbesondere speicherte damit personenbezogene Daten.

Auch wenn man der seinerzeit vertretenen Auffassung folgt, dass Beobachtungen für Lagebeurteilungen der Polizei, bei denen keine zielgerichtete Identifizierung von Personen erfolgt, kein Erheben darstellt (Drs. 16/3995, S. 10), so stellt spätestens das Anfertigen von Lageberichten mit personenbezogenen Daten eine Datenverarbeitung in Form des Speicherns dar; die Voraussetzungen der seinerzeitigen Dienstanweisung sind damit schon deshalb nicht erfüllt. Denn der Tatbestand des Speicherns ist bereits erfüllt, wenn von der Daten verarbeitenden Stelle erhobene oder ihr sonst bekannte Informationen, in welcher Form auch immer, „nachlesbar" fixiert werden (vgl. HmbDSG Gesetzestext und Erläuterungen, zu § 4, S. 57).

Das Beobachten und die dabei erfolgende Erhebung von personenbezogenen Daten stellt ein Eingriff in das informationelle Selbstbestimmungsrecht dar. Selbst wenn man

die seinerzeitige Dienstanweisung zugrunde legt, war der Einsatz der BfL von dieser Dienstanweisung nicht gedeckt und somit rechtswidrig.

Am 30. April 2015 haben wir in einem gemeinsamen Gespräch mit verschiedenen Vertreterinnen und Vertretern der BIS und Polizei Hamburg das Ergebnis unserer Prüfung, den Begriff des „Personenbezugs" sowie das weitere Vorgehen, soweit die BIS weiterhin an dem Einsatz von BfL interessiert sein sollte, erörtert. Die nunmehr datenschutzrechtlich geltende Auffassung, dass es – in Fallgestaltungen der vorliegenden Art, in der allein eine Daten verarbeitende Stelle zu betrachten ist – bei dem „Personenbezug" einzig und allein auf die Kenntnis der Daten verarbeitenden Stelle an sich und nicht auf die Kenntnis einzelner Mitarbeiter ankommt, wurde nicht geteilt.
Am 15.06.2015 teilte der Senat der BIS in der Sitzung des Innenausschusses mit, dass die Innenrevision der BIS beauftragt werde, den gesamten Komplex „verdeckt ermittelnde Polizeibeamtinnen und –beamte" sowie die strukturellen Abläufe im Staatsschutz der Polizei Hamburg, zu analysieren und hierüber ein Bericht zu erstatten. Dieser 39-seitige Bericht wurde in der Sitzung des Innenausschusses am 28. August 2015 vorgetragen (vgl. Drs. 21/2).

Nach Auffassung der Innenrevision:
„ist der Einsatz von BfL mit dem heutigen Kenntnisstand überholt. Zulässig war der Einsatz von BfL erst dann, wenn es politisch motivierte Gewalttaten gegeben hat, die sich einem abgrenzbaren Problemfeld zuordnen lassen und auch nur dann, wenn entsprechende Informationen zur Gefahrenabwehr benötigt werden und eine offene Aufklärung aussichtslos wäre. Wenn in solchen Fällen ein verdeckter Einsatz verhältnismäßig ist, kann auch ein VE-Einsatz erfolgen. Eines gesonderten, niederschwelligen Instrumentes bedarf es d.E. nicht. Von dem Instrument des BfL sollte Abstand genommen werden". (vgl. Revisionsbericht der Innenrevision, S. 32 in der Anlage zu Drs.21/2).

In ihrem 17 Punkte umfassenden Empfehlungskatalog empfahl die Innenrevision dann schließlich, auf den Einsatz von BfL gänzlich zu verzichten.

Der Innensenator hat sich zu dem Bericht geäußert und mitgeteilt, dass er die Polizei bereits angewiesen habe, alle Empfehlungen umzusetzen.

Damit wird die Polizei Hamburg in der Zukunft auf den Einsatz von Bfl gänzlich verzichten.

Zu dem Einsatz der Polizeibeamtin als verdeckte Ermittlerin gemäß § 12 PolDVG:
Unsere Anfrage an die Polizei hat ergeben, dass die zweite enttarnte Polizeibeamtin als verdeckte Ermittlerin gem. § 12 PolDVG in dem Zeitraum von Juli 2008 bis Ende 2012 eingesetzt war. Hier konzentrieren wir uns daher auf die Prüfung der Anordnungen zum Einsatz der verdeckten Ermittlerin nach § 12 Abs. 4 i.V.m. § 9 Abs. 2 PolDVG

und das Vorliegen der Voraussetzungen. Ferner interessierte uns, ob die Polizei die Personen, gegen die sich die Maßnahme richtete, nach Abschluss der Maßnahme unterrichtet hat, wie es in § 12 Abs. 4 i.V.m. § 9 Abs. 3 PolDVG vorgesehen ist.

Die Schwierigkeiten ergeben sich bei den Anordnungen zum Einsatz von verdeckten Ermittlerlinnen und Ermittlern, wenn formal zwar die Zustimmung der Staatsanwaltschaft vorliegt, im Übrigen aber die Anordnungen zu unbestimmt oder aber fehlerhaft sind.

In formeller Hinsicht gilt es daher zu überprüfen, ob sich aus den Anordnungen folgende Punkte ergeben:

- Art, Beginn und Ende der Maßnahme; eine Verlängerung ist zulässig, soweit die Voraussetzungen für die Anordnung der Maßnahme fortbestehen,
- an der Durchführung beteiligte Personen,
- Tatsachen, die den Einsatz der Maßnahme begründen,
- Zeitpunkt der Anordnung und Name sowie Dienststellung des Anordnenden,
- Anordnung durch den Polizeipräsidenten oder seinem Vertreter im Amt.

In materieller Hinsicht hingegen ist die Erhebung von personenbezogenen Daten durch den Einsatz von verdeckten Ermittlerinnen und Ermittlern nur zulässig, wenn

- dies zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist, oder aber
- Tatsachen die Annahme rechtfertigen, dass Straftaten von erheblicher Bedeutung begangen werden sollen und der Einsatz zur Verhütung dieser Straftaten erforderlich ist; der gezielte Einsatz gegen bestimmte Personen ist nur zulässig, wenn Tatsachen die dringende Annahme rechtfertigen, dass diese Personen Straftaten von erheblicher Bedeutung begehen werden und die Aufklärung des Sachverhalts auf andere Weise aussichtslos wäre.

Wir haben uns von der Polizei Hamburg die Anordnungen für die benannten Zeiträume zeigen lassen. Ob und inwiefern die o.g. Anforderungen vorliegen, wird derzeit von uns geprüft. Sollte dies nicht der Fall sein, so wäre der Einsatz der verdeckten Ermittlerin insgesamt als rechtswidrig zu bewerten. Denn eine fehlerhafte oder zu unbestimmte Einsatzanordnung führt zu ihrer Rechtswidrigkeit und damit zur Rechtswidrigkeit des Einsatzes insgesamt, selbst wenn der Einsatz materiell-rechtlich gerechtfertigt war (VG Karlsruhe, Urteil vom 26. August 2015 – 4 K 2107/11 –, Rn. 56, juris Belz/Muss-

mann/Kahlert/Sander, Polizeigesetz für Baden-Württemberg, 8. Aufl. 2015, § 22 RN 52; VG Freiburg, Urt. v. 06.07.2005 - 1 K 439/03 - juris).
Sobald wir eine Auswertung vorgenommen haben, werden wir mit der Polizei Hamburg in Gespräche eintreten.

1.6 Öffentlichkeitsfahndung im Internet durch Sicherheitsbehörden

Eine Nutzung sozialer Netzwerke privater Betreiber zur Öffentlichkeitsfahndung ist aus datenschutzrechtlicher Sicht sehr problematisch. Durch die weltweit recherchierbare Veröffentlichung von Fahndungsdaten wird in weitaus schwerwiegenderer Weise in die Grundrechte Betroffener eingegriffen, als dies bei der Nutzung klassischer Medien der Fall ist.

Im letzten Tätigkeitsbericht haben wir ausführlich über die Nutzung sozialer Netzwerke insbesondere Facebook durch die Polizei Hamburg berichtet (vgl. 24. TB V. 5.) und auf Bedenken gegen eine Öffentlichkeitsfahndung auch in sozialen Netzwerken hingewiesen. Mit zunehmender Beliebtheit sozialer Netzwerke bei Bürgerinnen und Bürgern steigt das Interesse von Strafverfolgungsbehörden, diese sozialen Netzwerke auch zur Öffentlichkeitsfahndung zu nutzen. So gibt es in Deutschland bereits Polizeidienststellen, die mittels Facebook nach Straftäterinnen und Straftätern suchen.

Dies ist bedenklich, weil durch die weltweit recherchierbare Veröffentlichung von Fahndungsdaten in weitaus schwerwiegenderer Weise in die Grundrechte Betroffener (Tatverdächtige oder auch Zeuginnen und Zeugen) eingegriffen wird, als dies bei der Nutzung klassischer Medien der Fall ist. Der Umstand, dass die Daten mit geringem Aufwand weiter verbreitet, kopiert und auf anderen Webseiten veröffentlicht werden können, beinhaltet zusätzlich die Gefahr, dass die Daten verarbeitende Stelle die Datenverarbeitung nicht mehr kontrollieren kann. Hinzu kommt, dass eine Löschung einer veröffentlichten Ausschreibung nicht nur wesentlich erschwert wird, sondern in vielen Fällen unmöglich ist.

Die Anlage B zu den Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) geht in Ziffer 3.2 allerdings von der Zweckmäßigkeit aus, die staatlichen Fahndungsaufrufe im Internet auf speziellen Seiten - etwa der Polizei - zu bündeln, um die Aufmerksamkeit der Internetnutzer für die Öffentlichkeitsfahndung zu erlangen. Da aber auch im Internet gilt, dass die ausschreibende Behörde als datenschutzrechtlich verantwortliche Stelle ihre Verantwortung für die Verarbeitung der Daten sowohl rechtlich als auch tatsächlich wahrnehmen kann, sieht die RiStBV in Ziffer 3.2 bisher vor, dass private Internetanbieter grundsätzlich nicht für Fahndungsaufrufe eingeschaltet werden sollen.

Diese Problematik haben die Datenschutzbeauftragten des Bundes und der Länder verfolgt und schließlich in ihrer 87. Konferenz am 27./28.03.2014 hierzu in der Entschließung „Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke - Strenge Regeln erforderlich!" Vorgaben für eine Öffentlichkeitsfahndung in sozialen Netzwerken aufgestellt (*http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/87_DSKOeffentlichkeitsfahndungSozialeNetzwerke.pdf?__blob=publicationFile&v=1*).

Sofern es Strafverfolgungsbehörden gestattet werden soll, zu Zwecken der Öffentlichkeitsfahndung auf soziale Netzwerke mit deaktivierter Kommentierungsfunktion zurückzugreifen, so darf dies - ungeachtet der generellen Kritik an der Nutzung sozialer Netzwerke durch öffentliche Stellen - nur geschehen, wenn folgende Maßgaben beachtet werden:

- Die Vorschriften der Strafprozessordnung (StPO) zur Öffentlichkeitsfahndung (§ 131 Abs. 3, § 131a Abs. 3, § 131b StPO) kommen aufgrund der technikoffenen Formulierung als Rechtsgrundlage für die Öffentlichkeitsfahndung im Internet grundsätzlich in Betracht. Sie sind aber im Hinblick auf den Verhältnismäßigkeitsgrundsatz nur eingeschränkt anzuwenden. Eine entsprechende Klarstellung durch den Gesetzgeber wäre wünschenswert. Zumindest aber sind die besonderen Voraussetzungen der Fahndung im Internet, insbesondere in sozialen Netzwerken in Umsetzungsvorschriften zu konkretisieren. Änderungsbedarf besteht beispielsweise für die Anlage B der RiStBV.

- In materiell-rechtlicher Hinsicht haben die Strafverfolgungsbehörden den Verhältnismäßigkeitsgrundsatz strikt zu beachten. Die zu schaffenden Regelungen müssen den besonderen Gefahren der Öffentlichkeitsfahndung in sozialen Netzwerken gerecht werden. Insbesondere muss sichergestellt werden, dass eine solche Fahndung nur bei im Einzelfall schwerwiegenden Straftaten überhaupt in Betracht gezogen werden kann.

- In verfahrensrechtlicher Hinsicht müssen die Umsetzungsregelungen die Staatsanwaltschaft verpflichten, bereits im Antrag auf richterliche Anordnung der Maßnahme die Art, den Umfang und die Dauer der Öffentlichkeitsfahndung konkret anzugeben. Dies umfasst insbesondere die ausdrückliche Angabe, ob und warum die Anordnung auch die Öffentlichkeitsfahndung in sozialen Netzwerken umfassen soll.

- Es ist sicherzustellen, dass
  - die zur Öffentlichkeitsfahndung verwendeten personenbezogenen Daten von den Strafverfolgungsbehörden ausschließlich auf im eigenen Verantwortungsbereich stehenden Servern gespeichert und verarbeitet werden, nicht hingegen auf Servern der privaten Anbieter,

- die Weitergabe und der automatisierte Abruf der personenbezogenen Daten aus dem Internet durch Web-Crawler und ähnliche Dienste so weit als technisch möglich verhindert werden und

- die Kommunikation zwischen den Strafverfolgungsbehörden und den Nutzern nur außerhalb der sozialen Netzwerke erfolgt.

Eine konkrete Bestrebung, die Öffentlichkeitsfahndung auch in sozialen Netzwerken näher zu regeln, ist ein großes Anliegen der Strafverfolgungsbehörden. Daher hat sich auch der Strafrechtsausschuss der Konferenz der Justizministerinnen und Justizminister sowie Justizsenatorinnen und Justizsenatoren (JuMiKo) mit der Öffentlichkeitsfahndung in Facebook und anderen sozialen Netzwerken befasst. Als Ergebnis seiner Beratungen hat der Ausschuss Empfehlungen zu Änderungen der Ziffer 3.2 der Anlage B zur RiStBV, der einer Öffentlichkeitsfahndung in sozialen Netzwerken bislang entgegenstand, formuliert. Die o.g. Entschließung wurde dabei zur Kenntnis genommen, aber wesentliche Aspekte nicht berücksichtigt.
Die Behörde für Justiz und Gleichstellung hat uns im August 2014 die beabsichtigte Neufassung der Ziffer 3.2, die als Allgemeine Verfügung (AV) umgesetzt werden soll, zur Stellungnahme vorgelegt. Wir haben auch im Hinblick auf die zuvor benannte Entschließung unsere Bedenken geäußert und nachdrücklich auf die Gefahren der Öffentlichkeitsfahndung hingewiesen.
Gleichwohl hat uns kurz vor Redaktionsschluss die Information erreicht, dass zwischenzeitlich die JuMiKo beschlossen habe, den Entwurf umzusetzen. Sollten die Strafverfolgungsbehörden von dieser Maßnahme nunmehr Gebrauch machen, gilt es jetzt die Entwicklung sorgsam zu beobachten.

1.7 Öffentlichkeitsarbeit über Social Media (Twitter und Facebook)

Die Polizei setzt zunehmend für ihre Öffentlichkeits- und Vollzugstätigkeit soziale Medien ein. Wir sind darüber informiert und begleiten diese Aktivitäten kritisch.

Wie bereits im letzten Tätigkeitsbericht (24. TB Ziff. V. 5) dargestellt, wird die Nutzung sozialer Medien durch die Polizei zur Öffentlichkeitsarbeit durch uns inhaltlich begleitet. Wir wurden im aktuellen Berichtszeitraum durch das Öffentlichkeitsreferat der Polizei über die Ausweitung der Aktivitäten in diesem Bereich regelmäßig informiert und haben, soweit erforderlich, dazu Stellung genommen.

Die Polizei hat die Nutzung der Facebook-Fanpage inhaltlich ausgedehnt und setzt diese sowohl zur allgemeinen Öffentlichkeitsarbeit als auch zur Sachfahndung ein. Zudem wird der Kurznachrichtendienst Twitter genutzt. Neben dem Ziel der Verbreitung der

eigenen Pressemitteilung soll der Dienst zur sogenannten taktischen Öffentlichkeitsarbeit Verwendung finden. Unter letzterer versteht die Polizei die öffentliche Verbreitung von Informationen zu aktuell stattfindenden Veranstaltungen oder Demonstrationen über Twitter, durch welche sie sich eine steuernde Wirkung auf die Beteiligten erhofft.

Gemeinsam mit der Polizei haben wir, wie bereits für die Nutzung der Fanpage, einige Grundbedingungen für den beanstandungsfreien Einsatz derartiger Dienste festgelegt. So werden die Profile bzw. Fanpage an sieben Tagen in der Woche jeweils 24-Stunden lang betreut, um sicherzustellen, dass keine rechtwidrige Inhalte über die Kommentarfunktionen auf den Angeboten der Polizei erscheinen. Außerdem wird das 4-Augen-Prinzip beim Veröffentlichen von Inhalten beibehalten. Dies soll die effektive Kontrolle der Einhaltung der datenschutzrechtlichen Grenzen der Veröffentlichung von personenbezogenen Daten gewährleistet. Das Melden von Gefahren oder Strafanzeigen muss weiterhin über die üblichen Kanäle, wie der Rufnummer 110, erfolgen.

Dass diese Grenzen erforderlich sind und deren Einhaltung auch kontrolliert werden muss, wurde im Rahmen einer Eingabe deutlich. Dabei ging es um die Veröffentlichung von Bildern von Angehörigen des Polizeidienstes im Internet über einen der genutzten Dienste. Die Erteilung der Einwilligung der Betroffenen in die Veröffentlichung konnte durch die Polizei nicht nachgewiesen und eine Gefährdung der Privatsphäre der Betroffenen nicht vollständig ausgeschlossen werden. Zudem benötigte die Polizei in diesem Fall sehr lange, um die Beschwerde zu bearbeiten und letztendlich die Bilder aus dem Internet zu entfernen.

Wir haben zwar darauf verzichtet dieses förmlich zu beanstanden. Jedoch wurde durch uns eindringlich darauf hingewiesen, dass die Persönlichkeitsrechte auch und gerade der Polizeivollzugskräfte bei der Verwendung sozialer Medien beachtet werden müssen und gefordert, dass Beschwerden gegen die Veröffentlichung von Bildern und anderer personenbezogener Daten zügig bearbeitet und eventuelle Verstöße entsprechend abgestellt werden. Erneut wurde durch uns darauf verwiesen, dass die Veröffentlichung von Bildern im Internet durch die Polizei nur auf einer gesetzlichen Grundlage und anderenfalls - was der Regelfall ist – nur mit der Einwilligung der Betroffenen zulässig ist.

1.8 Einrichtung und Betrieb eines Rechen- und Dienstleistungszentrums zur Telekommunikationsüberwachung der Polizeien im Verbund der norddeutschen Küstenländer

Die frühzeitige und kontinuierliche Einbindung der Datenschutzbeauftragten in Planungen neuer Anwendungen zur Nutzung der IuK-Technik ist nicht nur wünschenswert, sondern datenschutzgesetzlich zwingend notwendig.

Auf der Grundlage eines Beschlusses der Konferenz der Innenminister und -senatoren der norddeutschen Küstenländer (Nord-IMK) im September 2010 informierte uns die Polizei Hamburg im November 2011, dass die Bundesländer Hamburg, Schleswig-Holstein, Niedersachsen, Bremen und Mecklenburg-Vorpommern beabsichtigten, ein bereits seit 2008 diskutiertes regionales Rechen- und Dienstleistungszentrum zur Telekommunikationsüberwachung einzurichten (RDZ -TKÜ Nord).

Geplant war, das RDZ-TKÜ Nord in zwei Phasen schrittweise umzusetzen. Während in einer ersten Phase der Aufbau einer technischen Kooperation der Länder zur Schaffung von erforderlichen Kompensationsmöglichkeiten beim Ausfall der ländereigenen TKÜ-Anlagen und eines sofortigen Ausgleiches bei Lastspitzen eines Landes im Bereich der IP-basierten TKÜ erfolgen sollte, war in der zweiten Phase die Erstellung eines Umsetzungskonzeptes zur vollständigen Zentralisierung der TKÜ in einem RDZ-TKÜ Nord an den Standorten Hamburg und Hannover zu einem redundant ausgelegten TKÜ System vorgesehen.

Die erste Phase hat zwischenzeitlich begonnen. Die beteiligten Bundesländer haben mit den Ländern Hamburg und Niedersachsen im April 2012 Auftragsdatenverarbeitungsverträge (ADV-Vertrag) abgeschlossen, die die Rahmenbedingungen für eine tatsächliche Übernahme einer Telekommunikationsüberwachung regeln („Datenverarbeitungsauftrag für die technische Kooperation bei der Telekommunikationsüberwachung der Polizeien im Verbund der norddeutschen Küstenländer"). Die für das gesamte Projekt eingerichtete länderübergreifende Projektgruppe „RDZ-TKÜ", deren Leitung im Landeskriminalamt (LKA) Niedersachsen liegt, hat uns bis dahin über den Sachstand des Projektes einschließlich der Ziele und Verfahrensschritte sowie der technisch-organisatorischen Planungen unterrichtet. Da es sich um eine Kooperation zwischen den norddeutschen Küstenländern für das IT-Verfahren der TKÜ handelt, haben die Datenschutzaufsichtsbehörden der beteiligten fünf Bundesländer vereinbart, die projektbegleitenden Beratungen gemeinsam und abgestimmt durchzuführen.

In mehreren Prüfschritten und Besprechungen wurden mit den Projektverantwortlichen die Fragen der datenschutzrechtlichen Zulässigkeit und Ausgestaltung des Vertrages sowie die technisch-organisatorischen Anforderungen zur Umsetzung der fachlichen und technischen Konzeption und des Betriebskonzepts erörtert.

Da der Start der ersten Phase ab der Unterzeichnung des ADV-Vertrags erfolgen sollte, haben wir gegenüber dem LKA Hamburg noch in einem Schreiben im April 2012 unsere Bedenken geäußert und Verbesserungsvorschläge unterbreitet. Der Stand der bis zu diesem Zeitpunkt durch die Datenschutzbeauftragten erfolgten gemeinsamen Prüfung und Bewertung der fachlichen und technischen Konzeptionen sowie des tatsächlichen Ist-Standes bei der Erarbeitung der betrieblichen Details ließ erkennen, dass der Projektstatus nicht den erforderlichen Reifegrad bei der Informationssicherheit und den datenschutzrechtlichen Schutzmaßnahmen im technisch-organisatorischen Bereich

erreicht hatte, der aber für einen vertretbaren Betrieb mit Echtdaten unverzichtbar ist. Wir haben daher für den weiteren Fortgang des Projektes empfohlen, solange auf die Erteilung von Einzelaufträgen an das LKA Hamburg und damit auf die dortige Datenverarbeitung im Auftrag zu verzichten, bis die genannten Mängel behoben und die datenschutzrechtlichen Bedenken ausgeräumt sind.

Trotz dieser Bedenken wurde der ADV-Vertag am 26.04.2012 von den LKA Leitern der beteiligten Bundesländer unterzeichnet. Nach ihrer Auffassung seien die datenschutzrechtlichen und IT-sicherheitsrelevanten Maßnahmen grundsätzlich dazu geeignet, um mit dem Wirkbetrieb der technischen Kooperation beginnen zu können.

Im Januar 2013 erhielten wir erste Informationen zum Planungsstand der zweiten Phase – die Zentralisierung der TKÜ-Anlage ab dem Jahr 2016, in dem alle TKÜ-Maßnahmen der beteiligten Bundesländer Hamburg, Schleswig-Holstein, Niedersachsen, Bremen und Mecklenburg-Vorpommern zentralisiert durchgeführt werden sollen. Bereits beschlossen war zu diesem Zeitpunkt durch die Nord IMK, dass das Rechenzentrum nur noch an dem Standort Hannover, redundant ausgelegt, betrieben werden soll und für die Errichtung eines gemeinsamen Zentrums ein Staatsvertrag zu schließen wäre, der mit der Ratifizierung durch die Landesgesetzgeber eine gesetzliche Grundlage für die Zentralisierung schaffen soll. Die haushaltsrelevanten Unterlagen sollten bis Mitte 2013 erstellt werden, damit auf dieser Grundlage eine Wirtschaftlichkeitsbetrachtung erfolgen könne. Ein Umsetzungskonzept für die Zentralisierung und der dazugehörige Staatsvertrag waren bis Ende 2013 vorgesehen.

Im April 2014 erhielten wir dann vom Schwerpunktthemenverantwortlichen für den Bereich Datenschutz der Projektgruppe „RDZ-TKÜ" die Information, das LKA Hamburg habe die Beteiligung an dem Projekt gekündigt. Eine gesonderte Unterrichtung unserer Behörde durch das LKA Hamburg hat es jedoch nicht gegeben.

Ebenso wenig wie uns das LKA Hamburg den Ausstieg aus dem Projekt angezeigt hat, hat es auch den Wiedereinstig in das Projekt angezeigt. Vielmehr erfuhren wir erst aus der Drucksache 21/93, dass Hamburg seine Beteiligung zwischenzeitlich wieder aufgenommen habe. Die Nachfrage beim LKA hat hierzu ergeben, dass nach diversen Erörterungen und Klärungen Hamburg seine Beteiligung formal Anfang 2015 wieder aufgenommen habe. Selbst wenn das LKA Hamburg die Projektgruppe und damit den Schwerpunktthemenverantwortlichen für den Bereich Datenschutz informiert hat, hätte das LKA Hamburg unsere Behörde gemäß § 23 Abs. 4 HmbDSG sowie Ziff. 1 der Richtlinie zur Beteiligung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) vom 14.02.2011 (Beteiligungs-RL) rechtzeitig unterrichten müssen.

Bereits in der Projektphase 1 hatte sich die Kooperation zwischen den Datenschutzbeauftragten und der Projektgruppe bewährt und wurde bei einem gemeinsamen Termin

Ende Juni 2015 fortgesetzt, bei dem der aktuelle Stand des Projekts sowie das weitere Vorgehen erörtert wurde. Mecklenburg-Vorpommern hatte zu diesem Zeitpunkt als erstes Bundesland ein entsprechendes Gesetzgebungsverfahren zum Abschluss eines Staatsvertrages über die Einrichtung und den Betrieb des gemeinsamen RDZ-TKÜ Nord initiiert, so dass uns bereits ein erster Entwurf des Staatsvertrages über die Einrichtung und den Betrieb des RDZ -TKÜ Nord als auch das Umsetzungskonzept sowie ein Entwurf der Schutzbedarfsfeststellung vorlagen.

Da beabsichtigt ist, im März 2016 das förmliche Verhandlungsverfahrens zum Abschluss eines Staatsvertrages über die Einrichtung und den Betrieb des gemeinsamen RDZ-TKÜ Nord aufzunehmen, haben wir uns mit den Datenschutzbeauftragten der beteiligten Bundesländer darauf geeinigt, eine gemeinsame Position zum Staatsvertrag abzustimmen und gleichlautende Stellungnahmen im Gesetzgebungsverfahren einzubringen.

Das endgültige Datenschutzkonzept liegt noch nicht vor. Daher kann noch nicht beurteilt werden, ob die Inhalte tatsächlich ausreichend sind. Fest steht zu diesem Zeitpunkt lediglich, dass ein hoher Standard für den Datenschutz und die Datensicherheit vorgesehen ist. Das ist zu begrüßen.

Aus datenschutzrechtlicher Sicht ist die Einbindung des RDZ -TKÜ Nord an das LKA Niedersachsen allerdings mit größeren Herausforderungen verbunden. Daher muss sichergestellt werden, dass nicht nur technisch, sondern auch organisatorisch eine strikte Trennung zwischen dem LKA Niedersachen und dem gemeinsamen RDZ -TKÜ Nord erfolgt. Zentrales Anliegen der Datenschutzbeauftragten ist daher neben ihrer kontinuierlichen Einbindung in Entscheidungen über das RDZ -TKÜ Nord mit Auswirkungen auf Datenschutz und Datensicherheit, dass das RDZ -TKÜ Nord unmittelbar der Kontrolle durch die Datenschutzbeauftragten der beteiligten Länder unterliegt, soweit es für diese Länder Maßnahmen durchführt.
Wir werden das Thema weiterhin auf der Tagesordnung haben und auf eine datenschutzkonforme Praxis drängen.

1.9 Regeln zur Identifizierung von abwesenden Petenten bei Auskunftsersuchen

Erteilen die Sicherheitsbehörden eine Auskunft über gespeicherte personenbezogene Daten, müssen auch sie sicherstellen, dass nur die berechtigten Personen die Auskunft erhalten.

Anfang Oktober 2014 legte uns die Behörde für Inneres und Sport (BIS) einen Entwurf einer Handlungsanweisung vor, der Regeln zur Identifizierung von Petenten - unter anderem die Vorlage einer Ausweiskopie - bei Auskunftsersuchen vorsah. Hintergrund

hierfür war, dass immer mehr Auskunftsersuchen per E-Mail, Brief oder aber Fax eingingen und für eine Identifizierung der Personen bisher kein geregelter Ablauf vorgesehen war. Insbesondere die per Fax und E-Mail eingehenden Auskunftsersuchen stellten die datenverarbeitenden Stellen in der BIS vor eine große Herausforderung, weil Unterschriften entweder nicht lesbar, kaum lesbar oder nicht als Unterschrift erkennbar waren. Datenschutzrechtliche Bedenken bestehen bei dieser Form der Auskunftsersuchen an sich nicht, denn weder die Form der Antragstellung noch die Art und Weise der Identifizierung der Antragsteller ist in den für Sicherheitsbehörden geltenden Gesetzen (PolDVG, HmbVerfSchG, HmbDSG) geregelt.

Allerdings stellen gerade diese Form des Auskunftsersuchens die datenverarbeitenden Stellen in der BIS vor die Herausforderung zu entscheiden, ob die Person, die den Antrag gestellt hat, auch die Person ist, auf die sich die Auskunft beziehen soll. Denn in der Praxis muss die Auskunft erteilende Stelle sicherstellen, dass sie Auskunftserteilungen an unberechtigte Dritte, die sich lediglich unter Ausnutzung des Namens des Betroffenen an die Polizei gewandt haben, ausschließt.

Die Vorlage des Personalausweises, Reisepasses oder des Aufenthaltstitels als Mittel zur Identifizierung gegenüber einer Behörde ist zwar ein Schutz vor missbräuchlichem Auskunftsersuchen von Dritten, setzt aber voraus, dass die Betroffenen persönlich bei der datenverarbeitenden Stelle erscheinen müssen. Um den Auskunftsersuchen nachzukommen, ist als Alternative die Vorlage einer einfachen Ausweiskopie denkbar. Zu beachten ist jedoch, dass das Vervielfältigen von Pässen und Personalausweisen durch Fotokopieren nur unter bestimmten Voraussetzungen möglich ist. Hierüber haben wir bereits ausführlich im letzten Tätigkeitsbericht (TB) berichtet und verweisen daher an dieser Stelle auf unseren 24. TB III.20.2.

Unsere Sichtweise haben wir gegenüber dem behördlichen Datenschutzbeauftragten der BIS dargelegt. Nach einem konstruktiven Dialog haben wir gemeinsam Regeln zur Identifizierung entwickelt. Wird nunmehr eine Kopie des Personalausweises angefordert, so darf diese ausschließlich zu Identifizierungszwecken verwendet werden und ist vom Empfänger unverzüglich zu vernichten, sobald der mit der Kopie verfolgte Zweck der Identifizierung erreicht ist. Das Vorliegen der Ausweiskopie ist ggf. vor der Vernichtung zu vermerken. Ein Einscannen, das zu einer automatisiert auswertbaren Datei führt, hat zu unterbleiben.

Durch die Erstellung der Regeln wird die unterschiedliche Vorgehensweise bei der Identifizierung von Petenten – die bei anderen Landes- und Bundesbehörden von der Vorlage von Ausweisen bis hin zur Vorlage von beglaubigten Ausweiskopien reichen und unter Umständen für die Betroffenen in einer solchen Weise erschwerend sein kann, dass dies als Beeinträchtigung gesehen wird - vermieden. Gleichzeitig bieten die Regeln ein Mindestmaß an Sicherheit hinsichtlich der Identität.

1.10 Nutzung von erkennungsdienstlichen Bildern aus dem Polizeilichen Auskunftssystem (POLAS) für Verkehrsordnungswidrigkeitenverfahren

Die Nutzung von Lichtbildern aus dem Polizeilichen Auskunftssystem (POLAS) für die Ermittlung von Betroffenen in Bußgeldverfahren, bei denen ein Beweisfoto vorliegt, ist unter besonderer Beachtung der Verhältnismäßigkeit zulässig, wenn die Errichtungsanordnung diesen Zweck festgelegt hat.

Im Februar 2015 ist die Polizei Hamburg mit der Bitte an uns herangetreten, zu prüfen, ob und ggfs. inwieweit sie Lichtbilder aus dem Polizeilichen Auskunftssystem (POLAS) zur Identitätsfeststellung in Verkehrsordnungswidrigkeitenverfahren nutzen kann. Bisher hatte sie von dieser Möglichkeit keinen Gebrauch gemacht. Vielmehr hat sie zur Feststellung der Identität zulässige Ermittlungen im Umfeld des Betroffenen getätigt oder aber Lichtbilder aus dem Personalausweis- oder Passregister gem. § 25 Abs. 2 Personalausweisgesetz (PAuswG) sowie § 22 Abs. 2 Paßgesetz (PaßG) automatisiert abgerufen.

Zur Erforschung der Ordnungswidrigkeit kann die Beiziehung eines Lichtbilds des Betroffenen mit dem in POLAS hinterlegten Lichtbild grundsätzlich erforderlich sein, wenn durch den Vergleich eines anlässlich des Verkehrsverstoßes gefertigten Lichtbilds des Fahrers die Identität des Betroffenen festgestellt werden kann.

Dies haben wir der Polizei gegenüber dargelegt und darauf hingewiesen, dass dieser Zweck gem. § 26 Abs. 1 Nr. 2 Polizeidatenverarbeitungsgesetz (PolDVG) in der Errichtungsanordnung festgelegt sein muss. Die Polizei Hamburg hat unserer Stellungnahme folgend die Errichtungsanordnung ergänzt.

Die Errichtungsanordnung sieht nun vor, dass für die Ermittlung von Betroffenen in Bußgeldverfahren, bei denen ein Beweisfoto vorliegt, unter besonderer Beachtung der Verhältnismäßigkeit die Datei POLAS genutzt werden kann. Eine Einschränkung findet sich in der Errichtungsanordnung dahingehend, dass nur ein Abgleich mit dem Lichtbildbestand vorgenommen werden kann. Weitergehende Informationen aus POLAS hingegen dürfen nicht verwendet werden.

Der Versuch der Datenerhebung beim Betroffenen, d.h. bei demjenigen, in dessen Rechte durch einen späteren Lichtbildabgleich eingegriffen wird, ist in den meisten Fällen nicht zielführend. Der Abgleich eines Lichtbilds aus dem eigenen Datenbestand der Polizei mit dem eines anlässlich des Verkehrsverstoßes gefertigten Lichtbilds des Fahrers stellt ein wesentlich geringen Eingriff im Vergleich zu anderen zulässigen Er-

mittlungen bei dritten Stellen dar. So würden bei Nachfragen im Umfeld des Betroffenen (wie z.B. Bildbefragung von Angehörigen, Nachbarn oder Arbeitskollegen) oder aber bei einem automatisierten Abruf aus dem Personalausweis- oder Passregister personenbezogene Daten des Betroffenen bzw. die Information, dass die Polizei seinetwegen ermittelt, ohne Kenntnis des Betroffenen sogar an Stellen außerhalb der Polizei übermittelt. Durch die hier getroffene Vorgehensweise wird das informationelle Selbstbestimmungsrecht des Betroffenen somit dadurch gestärkt, dass zunächst interne Ermittlungsmöglichkeiten ausgeschöpft werden.

1.11 Polizeilicher Informations- und Analyseverbund (PIAV)

Mit dem Polizeilichen Informations- und Analyseverbund wird neben INPOL ein weiteres, eigenständiges Verbundsystem geschaffen. Da Verbundsysteme stets einen sehr großen Datenbestand enthalten, sind sie in der Entwicklungs- und Nutzungsphase kontinuierlich zu begleiten.

Anfang 2013 hat uns die Polizei Hamburg die geplante Einführung eines Polizeilichen Informations- und Analyseverbundes (PIAV) zwischen dem Bund und den Ländern angezeigt und in einer ersten Informationsveranstaltung den aktuellen Stand berichtet.
Die Einführung von PIAV soll den bisherigen Kriminalpolizeilichen Meldedienst (KPM) und die Sonderdienste (SMD) schrittweise ablösen. Die Ist-Aufnahme dieser beiden Meldedienste hatte u.a. ergeben, dass aufwändige Mehrfacherfassungen erfolgten, die Daten eine mangelnde Qualität aufwiesen und ein hoher länderübergreifender Kommunikationsaufwand zur Erkenntnisgewinnung betrieben werden musste.
Wie die Planung und Ausgestaltung tatsächlich aussehen sollte, war zu diesem Zeitpunkt noch nicht abschließend geklärt. Bekannt war lediglich, was PIAV können soll:

- Erkennen von Tat-Tat- und Tat-Täter-Zusammenhängen
- Identifizierung länderübergreifend oder deliktsübergreifend handelnder Straftäter/Täterorganisationen/Straftatenserien
- Frühzeitiges Erkennen von Kriminalitätsphänomenen sowie von zeitlichen oder geographischen Kriminalitätsbrennpunkten
- Führzeitiges Erkennen von kriminalitätsfördernden Faktoren
- Erstellung von Kriminalitätslageberichten und Kriminalitätslagebildern für eine effektive Beratung der polizeilichen und politischen Führungs- und Entscheidungsebene

- Schnelle Anpassung des länderübergreifenden Informationsaustausches und der gemeinsamen Analyse neuer Kriminalitätsphänomene.

Ein Lastenheft PIAV-Operativ Zentral sowie ein Entwurf einer Errichtungsanordnung für PIAV Zentral (Stand 2012) lag zu diesem Zeitpunkt bereits vor, so dass wir uns einen ersten vertieften Eindruck über das Verbundsystem verschaffen konnten.
Das Bundeskriminalamt (BKA) hat als Zentralstelle für den elektronischen Datenverbund zwischen Bund und Ländern gemäß § 11 Absatz 6 Satz 5 BKAG die technischen und organisatorischen Maßnahmen im polizeilichen Informationssystem zu treffen. Die maßgebliche Verantwortung für die Beachtung datenschutzrechtlicher Aspekte in den Phasen der Planung und Umsetzung und während des laufenden Betriebs liegt daher auch beim BKA. Die Überwachung der Einhaltung datenschutzrechtlicher Bestimmung hingegen liegt bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) als aufsichtführende Stelle.

Da aber die Teilnehmer des Informationsverbundes die im System ausgetauschten Daten eigenverantwortlich und automatisiert anliefern, wird demzufolge auch die datenschutzrechtliche Verantwortung für die Speicherungen größtenteils auf die Teilnehmer und somit für den hamburger Bereich auf die Polizei Hamburg entfallen. Für diesen Teilbereich liegt die datenschutzrechtliche Aufsicht dann bei den Datenschutzbeauftragen der Länder.

Vorgesehen ist, dass PIAV stufenweise aufgebaut wird. Als erste operative Pilotanwendung in PIAV wird derzeit der Bereich „Waffen- und Sprengstoff" entwickelt, der Mitte 2016 in Betrieb gehen soll. Für die nächsten Jahre sollen dann nachfolgende Deliktsbereiche in PIAV einfließen:

2017 – BtM-, Gewaltdelikte, gemeingefährliche Straftaten
2018 – Eigentumsdelikte, Sexualdelikte, Cybercrime
2019 – Schleusung, Menschenhandel, Dokumente
2020 – Wirtschaftskriminalität, Falschgeld, Korruption
2021 – politisch motivierte Kriminalität
2022 – Organisierte Kriminalität

Bereits jetzt zeichnet sich ab, dass PIAV intensiv datenschutzrechtlich betreut werden muss. Daher haben wir die Polizei Hamburg noch einmal nachdrücklich darum gebeten, uns bei allen datenschutzrechtlichen Frage einzubeziehen und uns insbesondere Unterlagen zeitnah nach Erstellung zu übersenden, damit wir eine umfangreiche datenschutzrechtliche Prüfung vornehmen können.

Im April 2015 hat uns die Polizei Hamburg erste Entwürfe der Verfahrensbeschreibung, eine Liste der zu speichernden Daten sowie des Netzplans vorgelegt. Ende September 2015 erreichte uns dann die die Schutzbedarfsfeststellung.

Derzeit befinden wir uns in der Prüfung dieser Dokumente. Die erste Durchsicht zeigt aber, dass noch weitere Informationen in die Dokumentation aufgenommen werden müssen. Die Risikoanalyse und das Sicherheitskonzept sowie die Errichtungsanordnung (für den Teilbereich Hamburg – PIAV Land) stehen noch aus.

Über die weitere Entwicklung werden wir im nächsten Tätigkeitsbericht berichten.

1.12 Data Center Polizei

Der Betrieb von gleichartigen IT-Verfahren in Data Centern berücksichtigt vorrangig Anforderungen der Wirtschaftlichkeit und IT-Sicherheit. Die Anforderungen an den Datenschutz müssen gleichrangig berücksichtigt werden.

Anfang Dezember 2013 haben wir bei der Polizei Hamburg angefragt, ob die norddeutschen Länder Pläne zum gemeinsamen Betrieb von IT-Verfahren hätten. Die Antwort: Der Aufwand sei zu hoch, wenn sich was täte, würden wir informiert. Eine erneute Nachfrage im Mai 2014 ergab, dass bereits im Februar 2014 ein Workshop der Polizeien zum Data Center Polizei (DCP) stattgefunden hatte. Eine offizielle Vorstellung gab es kurz darauf im Juni 2014.

Im August 2014 gaben die Landesdatenschutzbeauftragten der Länder Bremen, Schleswig-Holstein und wir eine gemeinsame Stellungnahme zum DCP an die Ministerien und Landespolizeien ab. Wesentliche Punkte darin waren:

- Es dürfen durch Zusammenlegung (und unzureichende Mandantentrennung) keine gemeinsamen Verfahren entstehen, die den Daten verarbeitenden (verantwortlichen) Stellen verschiedener Bundesländer einen Zugriff auf die personenbezogenen Daten anderer Bundesländer erlauben, soweit keine Rechtsgrundlagen dafür bestehen.

- Insgesamt ist die „Orientierungshilfe Mandantenfähigkeit“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu beachten. Danach ist der Grad der technischen Trennung der Mandanten anhand des Risikos einer mandantenübergreifenden Datenverarbeitung zu bemessen. Bei hohem Risiko kann dies auch bedeuten, dass eine Trennung innerhalb einer mandantenfähigen Applikation nicht realisiert werden kann und mandantenindividuelle Verfahren erforderlich sind.

- Soll ein länderübergreifender Datenaustausch erfolgen, so sind die jeweiligen Datenübermittlungs- und Datenerhebungsvorschriften zu beachten. Sollen automatisierte Abrufe von polizeilichen Daten aus anderen Bundesländern erfolgen oder

gemeinsame Verfahren eingerichtet werden, so sind die datenschutzrechtlichen Vorgaben zu beachten, die eine Rechtsgrundlage fordern.

- Für einen Betrieb des DCP ist eine gemeinsame Festlegung von Schutzbedarfen und zusätzlichen Sicherheitsmaßnahmen durch die Polizeien sinnvoll. Unterschiedliche Anforderungen der Polizeien durch landesspezifisch geltende (datenschutz-)rechtliche Vorgaben können dabei zu zusätzlichen Sicherheitsmaßnahmen führen, die für andere Auftraggeber nicht zwingend erforderlich sind.

- Für die Festlegung von Sicherheitsmaßnahmen, deren Fortschreibung und die Überwachung der tatsächlich umgesetzten Sicherheitsmaßnahmen ist ein Gremium der Auftraggeber zu bilden, das dauerhaft die Aufgabe eines gemeinsamen Datenschutz- und IT-Sicherheitsmanagements für das Data Center Polizei wahrnimmt.

- Es ist erforderlich, dass eine vollumfängliche Risikoanalyse vor der Transition der Verfahren der Polizei Hamburg in DCP durchgeführt wird. Dabei ist die Mandantenfähigkeit für alle betroffenen Verfahrens- und Infrastrukturkomponenten sowie genutzte Dienste nachzuweisen.

- Vor dem Hintergrund der Sicherheitsrelevanz der durch die Polizeien der Länder verarbeiteten Daten und genutzten Verfahren und deren Kumulation ist eine sorgfältige tiefgehende Vorabkontrolle zwingend. Eine Transition kann erst durchgeführt werden, wenn die Maßnahmen, die aus der Risikoanalyse folgen, umgesetzt sind.

Mitte Januar 2015 forderten wir die Polizei Hamburg zur Übersendung der Risikoanalyse auf. Nach Fristsetzungen für Mai und Juni 2015 liegen seit Mitte Oktober 2015 die Unterlagen aus der Vorabkontrolle vor. Von einer Übersendung der Papierunterlagen wurde in Anbetracht des Umfangs abgesehen.

Die Polizei Hamburg weist darauf hin, die Risiken und Maßnahmen zur Abwehr bewertet, einzelne Maßnahmen zur Verfahrenstrennung durchgeführt, ein Koordinierungsgremium eingesetzt und zu überführende Verfahren weiterhin analysiert zu haben. Maßnahmen aus der Risikoanalyse befinden sich noch in der Abstimmung zwischen den Polizeien und dem IT-Dienstleister.

Die Prüfung der Unterlagen ist noch nicht abgeschlossen.

1.13 Predictive Policing

Der Einsatz von Systemen zur Datenanalyse, die auf der Auswertung einer Vielzahl unterschiedlicher Datenquellen das Ziel haben, Prognosen über künftige Straftaten oder Gefahrensituationen durch die Polizei zu ermöglichen, weist ein erhebliches Risikopotential für das informationelle Selbstbestimmungsrecht möglicher Betroffener auf.

Polizeibehörden zeigen zunehmend Interesse an Systemen zur Datenanalyse und erste Bundesländer erproben zwischenzeitlich eine Prognosesoftware, die in der Bekämpfung der Wohnungseinbruchskriminalität die polizeiliche Arbeit unterstützen soll (sog. predictive policing). Ein Trend, den es zu beobachten gilt, denn bevor solch eine Software flächendeckend eingesetzt werden soll, haben die Datenschutzbeauftragten des Bundes und der Länder auf ihrer 89. Konferenz am 18. und 19. März 2015 in Wiesbaden in der Entschließung „Big Data zur Gefahrenabwehr und Strafverfolgung: Risiken und Nebenwirkungen beachten" hinsichtlich der Gefahren von Prognosesoftware nachdrücklich darauf hingewiesen, dass der Einsatz solcher Systeme durch die Polizei geeignet ist, elementare Grundsätze des Datenschutzes und des Rechts auf informationelle Selbstbestimmung in Frage zu stellen.

Der Versuch, mit dem Einsatz von Technik relevante Ereignisse anhand bloßer statistischer Wahrscheinlichkeiten vorherzusagen, verschiebt die polizeiliche Eingriffsschwelle weit über den Bereich einer individuellen Handlungszurechnung hinweg in ein Vorfeld, das verdachtsunabhängig und ohne eindeutige Kausalitätszusammenhänge zu Tat und Täter auskommt. Die Erstellung von Prognosen, an deren Ende Personen nur aufgrund einer statistischen Wahrscheinlichkeit unter den Verdacht geraten, Straftaten zu begehen oder zu Störern zu werden, ist unter rechtsstaatlichen Gesichtspunkten fragwürdig. Sie widerspricht der für unser Rechtssystem fundamentalen Unschuldsvermutung, ist fehleranfällig und ersetzt polizeiliche Einschätzungen durch automatisierte intransparente Maschinenlogik.

Eine Gelegenheit mit der Behörde für Inneres und Sport (BIS) über dieses Thema ins Gespräch zu kommen, hat es bisher nicht gegeben. Zwar wird in Hamburg noch keine Prognosesoftware eingesetzt und uns sind auch keine konkreten Planungen der Polizei Hamburg bekannt. Allerdings zeigt sich auch die BIS an der sogenannten „Predictive Policing" Software interessiert, wie sich aus der Schriftlichen Kleinen Anfrage (Drs. 21/529) entnehmen lässt.

Wir gehen davon aus, dass wir entsprechend § 24 Abs. 4 S. 2 Hamburgisches Datenschutzgesetz rechtzeitig über Planungen neuer Anwendungen unterrichtet werden.

2. Verfassungsschutz

2.1 Datenerfassung aus sozialen Netzwerken im Internet

Mit dem Landesamt für Verfassungsschutz (LfV) erörtern wir die Datenverarbeitung im Zusammenhang mit der Auswertung von Informationen aus sozialen Netzwerken im Internet.

Im vergangenen Sommer hat uns das Landesamt für Verfassungsschutz (LfV) darüber informiert, dass es ein Verfahren einführen wolle, mit dem eine Erfassung von allgemein zugänglichen Informationen aus einem sozialen Netzwerk erfolgen kann. Hintergrund hierfür war insbesondere, dass zwischenzeitlich Personen, bei denen die Voraussetzungen des § 9 Abs. 1 S. 1 Nr. 1 Hamburgisches Verfassungsschutzgesetz (HmbVerfSchG) zur Datenverarbeitung vorliegen (Betroffene), zunehmend ihre Aktivitäten in soziale Netzwerke verlagern und diese dazu nutzen, sich anderen mitzuteilen sowie Bilder oder Videos zu veröffentlichen. Die inhaltliche Auswertung der Aktivitäten in sozialen Netzwerken trage nach Auffassung des LfV wesentlich zur Informations- und Erkenntnisgewinnung im Aufgabenbereich des § 4 Abs. 1 HmbVerfSchG bei. Aufgenommen in das Verfahren werden derzeit nur Betroffene, die zuvor schon extremistische Inhalte i.S.d. § 4 Abs. 1 HmbVerfSchG allgemein zugänglich in sozialen Netzwerken mitgeteilt haben. Die Betroffenen werden händisch durch die Mitarbeiter bestimmt und in das Verfahren aufgenommen. Sodann werden Mitteilungen der im Verfahren definierten Betroffenen automatisiert von dem Verfahren erfasst und für die Dauer der Auswertung gesondert von den sonstigen Dateien beim LfV gespeichert. Mitteilungen mit Inhalten, die verfassungsfeindliche Bestrebungen i.S.d. § 4 Abs. 1 HmbVerfSchG enthalten, werden nach Auswertungsphase dauerhaft in den sonstigen Dateien des LfV transferiert und personenbezogen gespeichert.

In einem zweiten Schritt wurde das Verfahren für einen Teilbereich der Extremismusbeobachtung nach dem HmbVerfSchG insofern erweitert, dass auch allgemein zugängliche Mitteilungen von Personen, die in Kontakt zum Betroffenen treten und so Mitteilungen an den Betroffenen richten, zunächst unter den Voraussetzungen des § 9 Abs. 1 S. 1 Nr. 2 HmbVerfSchG erfasst werden.

Mehrere Gespräche mit dem LfV, bei dem wir uns auch das Verfahren haben zeigen lassen, sowie unsere Stellungnahme gegenüber dem LfV führten zur nachfolgenden Konkretisierung des Verfahrens:

Binnen weniger Tage nach Erfassung der jeweiligen Mitteilungen des Betroffenen muss diese auf ihre Erforderlichkeit hin überprüft werden. Nach erstmaligem Lesen der Mitteilung hat der Anwender nur die Möglichkeit, erforderliche Mitteilungen zu speichern oder nicht erforderliche Mitteilungen zu löschen. Erforderliche Mitteilun-

gen werden dauerhaft gespeichert und in den sonstigen Dateien des LfV transferiert, nicht erforderliche hingegen umgehend und unwiederbringlich gelöscht. Erfolgt keine Erforderlichkeitsprüfung binnen einer festgelegten Bearbeitungsdauer, werden die Mitteilungen des Betroffenen automatisch im Verfahren gelöscht. Gleiches gilt für Mitteilungen Dritter an den Betroffenen. Diese werden, sofern sie sich direkt auf eine Mitteilung des Betroffenen beziehen, für eine konkret bestimmte Dauer vom Verfahren erfasst. Zudem erstellt das Verfahren eine Statistik zu den erfassten Daten, auf deren Basis eine Evaluation erfolgen kann.

Das LfV hat diese Vorgaben im Verfahren umgehend umgesetzt. Zwingende Voraussetzung für die Aufnahme von Personen in beide Verfahren als Betroffene ist zudem eine bestehende Speicherung der personenbezogenen Daten im Nachrichtendienstlichen Informationssystem (NADIS). Damit wird sichergestellt, dass allein Personen Betroffene der Maßnahme werden können, zu denen die Speichervoraussetzungen bereits vorliegen. Eine willkürliche Aufnahme der Personen in das Verfahren kann somit ausgeschlossen werden.

Allerdings ist bei der Erfassung der Mitteilungen Dritter problematisch, dass die Möglichkeit besteht, dass auch Personen, die noch nicht 14 Jahre alt sind, Mitteilungen an die Betroffenen richten und aus der Mitteilung heraus nicht deutlich wird, dass der Dritte unter 14 Jahre alt ist. Unabhängig davon, ob das LfV positive Kenntnis von der Minderjährigkeit hat oder nicht, sieht der Wortlaut des § 10 Abs. 1 HmbVerfSchG vor, dass Daten Minderjähriger, die noch nicht 14 Jahre alt sind, nicht in amtseigenen Dateien gespeichert werden dürfen. Daher haben wir beim LfV eine gesetzliche Änderung angeregt.

2.2 Eingaben zu Speicherungen beim Landesamt für Verfassungsschutz

Das Landesamt für Verfassungsschutz darf personenbezogene Daten an andere Behörden übermitteln, wenn dies zum Schutz vor verfassungsschutzrelevanten Bestrebungen oder Tätigkeiten erforderlich ist.

Auch in diesem Berichtszeitraum haben sich wieder Bürgerinnen und Bürger an uns gewandt, weil sie wissen wollten, ob und welche personenbezogenen Daten über sie beim Landesamt für Verfassungsschutz (LfV) gespeichert sind. Auffällig viele Anfragen erreichten uns kurz nachdem eine verdeckt ermittelnde Polizeibeamtin enttarnt wurde und nach Informationen der Behörde für Inneres (BIS) Berichte aus dem Einsatz an das LfV übermittelt wurden (vgl. IV 1.5). Weil es in vielen Fällen aber keine konkreten Anhaltspunkte gab, um direkt an das LfV heranzutreten, haben wir die Bürgerinnen und Bürger zunächst gebeten, dass sie selbst von ihrem Auskunftsrecht gegenüber dem

LfV Gebrauch machen können. Viele wussten nicht, wie sie von ihrem Auskunftsrecht Gebrauch machen können, an wen das Auskunftsersuchen gerichtet sein und wie es inhaltlich formuliert sein muss. Vor diesem Hintergrund haben wir das Informationsblatt „Auskunft im Bereich Sicherheit und Strafverfolgung" mit Musterbriefen an das LfV, die Polizei Hamburg und die Staatsanwaltschaft erstellt und den Bürgerinnen und Bürgern zukommen lassen. Das Informationsblatt kann bei Bedarf jederzeit in unserer Behörde angefordert werden.

Es haben uns aber auch Anfragen erreicht, die uns zu einer Überprüfung der Speicherung veranlasst haben. Bei unserer Bewertung haben wir gegenüber den Betroffenen immer wieder deutlich gemacht, dass es grundsätzlich nicht unsere Aufgabe ist, uns mit einer eigenen verbindlichen Bewertung von Erkenntnissen an die Stelle des LfV zu setzen. Die fachliche Bewertung bleibt den Daten verarbeitenden Stellen vorbehalten; allerdings können wir unsere Meinung äußern, wenn Zweifel daran bestehen, dass die Daten die Voraussetzungen der Speicherungen erfüllen. Dabei ist auch entscheidend, dass keine sachfremden Erwägungen einbezogen werden oder Willkür bei der Speicherung erkennbar ist. Damit beschränkt sich unsere Überprüfung auf eine sogenannte Plausibilitätskontrolle. Wir überprüfen daher in der Regel, ob die Speicherung annehmbar, einleuchtend und nachvollziehbar ist oder nicht.

So gingen wir auch bei dem nachfolgenden Fall vor, bei dem wir die Datenverarbeitung beim LfV im Zusammenhang mit einer erlaubnispflichtigen Tätigkeit überprüften. Der Petent hatte sich bei uns gemeldet, weil einem seiner Familienangehörigen eine erlaubnispflichtige Tätigkeit nicht erteilt wurde. Begründet wurde dies u.a. mit einem Bezug zur jihadistischen/salafistischen Szene und der damit nicht vorhandenen Eignung für die erlaubnispflichtige Tätigkeit. Bei der Erlaubnisablehnung wurde auch der Name des Petenten mitgeteilt. Der Petent bat uns daher um Überprüfung der Speicherung beim LfV sowie der Übermittlung dieser Daten.

Die Sachverhaltsaufklärung hat ergeben, dass das LfV der Aufsichtsbehörde personenbezogene Daten des Petenten – die Zugehörigkeit zur jihadistischen/salafistischen Szene – übermittelt hatte. Im Rahmen der Erlaubnisprüfung wiederum gelangten diese Informationen an die Genehmigungsbehörde mit der Folge, dass die Erlaubnis nicht erteilt wurde. Der Ablehnungsbescheid enthielt auch die personenbezogenen Daten des Petenten, obwohl er die Erlaubnis nicht beantragt hatte.

Unsere Prüfung ergab, dass die Datenverarbeitung insgesamt rechtmäßig war. Dies betraf nicht nur das LfV, sondern auch die übrigen Daten verarbeitenden Stellen.

Die Prüfung beim LfV ergab, dass die Daten des Petenten nach § 9 Abs. 1 i.V.m. § 4 Abs. 1 Hamburgisches Verfassungsschutzgesetz (HmbVerfSchG) gespeichert werden dürfen. Das LfV durfte diese Daten auch an die Aufsichtsbehörde übermitteln. Dies folgt aus § 14 Abs. 1 HmbVerfSchG, wonach das LfV Informationen einschließlich

personenbezogener Daten an inländische öffentliche Stellen übermitteln darf, wenn diese zum Schutz vor Bestrebungen oder Tätigkeiten nach § 4 Abs. 1 HmbVerfSchG zwingend erforderlich sind. So lag es auch in diesem Fall, denn hier waren Bestrebungen gegen die freiheitliche demokratische Grundordnung zu befürchten, die gerade auch für die erlaubnispflichtige Tätigkeit von Bedeutung waren. Dies haben wir dem Petenten mitgeteilt.

3. Ausländerwesen

3.1 Kompetenzfeststellung von Asylantragstellern: Programm Work & Integration for Refugees (W.I.R.)

Sollen Flüchtlinge zum Zwecke einer möglichst schnellen Integration in den Arbeitsmarkt und im Hinblick auf Ausbildung und Studium gefördert werden, bedarf es für die hiermit im Zusammenhang stehende Verarbeitung personenbezogener Daten mangels entsprechender gesetzlicher Grundlagen einer den datenschutzrechtlichen Anforderungen entsprechenden Einwilligungserklärung; wichtig ist in diesem konkreten Zusammenhang, dass die Unterlagen auch übersetzt vorliegen, damit die Betroffenen die Aufklärung und die Einwilligungserklärung auch tatsächlich zur Kenntnis nehmen können.

Seit September 2015 besteht für Flüchtlinge die Möglichkeit, am Programm W.I.R. teilzunehmen. Ziel dieses Programmes ist es, die Flüchtlinge möglichst schnell in den Arbeitsmarkt integrieren zu können. Mit Informations-, Beratungs- und ggf. Förder- und Vermittlungsangeboten sollen die Betroffenen so früh wie möglich auf den Einstieg in Arbeit oder Ausbildung bzw. Studium im Falle eines positiven Ausgangs Ihres Asylverfahrens vorbereitet werden. Hierzu kooperieren in dem Programm W.I.R. verschiedene Partner, unter anderem die Behörde für Arbeit, Soziales, Familie und Integration (BASFI), die Agentur für Arbeit Hamburg, Jobcenter team.arbeit.hamburg und weitere öffentliche und nicht-öffentliche Stellen, um eine systematische Erfassung der jeweiligen Lebenslage sowie die Feststellung der beruflichen Kompetenzen zu erreichen. Nach einer ersten Erhebung grundlegender Informationen schließt sich eine Besprechung an, in dem es um die jeweilige konkrete Situation der Betroffenen, eventuelle Einschränkungen und auch besondere Qualifizierungsbedarfe wie z.B. Sprachförderung geht.

Das Projekt hatte bereits erkannt, dass es mangels gesetzlicher Grundlage für die Erhebung und Verarbeitung der Daten, insbesondere den gegenseitigen Austausch der Daten unter den Beteiligten, einer Einwilligung der Betroffenen bedarf. Kurz vor dem Start des Programmes wurden wir Anfang September 2015 über das Projekt informiert; insbesondere ging es hierbei auch um eine sehr zeitnahe Abstimmung über den Inhalt der Einwilligungserklärung.

Voraussetzung für die Wirksamkeit einer Einwilligungserklärung in datenschutzrechtlicher Hinsicht ist u.a., dass die Betroffenen zunächst umfassend über die vorgesehene Datenverarbeitung aufgeklärt werden und dass die Einwilligung freiwillig erteilt wird. Die Freiwilligkeit wurde vom Projekt von Anfang an betont; so fand sich schon im ersten Einwilligungsentwurf der Hinweis, dass die Teilnahme oder auch Nichtteilnahme am Projekt in keinem Zusammenhang mit dem anhängigen Asylverfahren steht und weder auf dessen Ausgang noch auf die Frage des Verbleibs oder Nichtverbleibs in Deutschland Einfluss nimmt.

Darüber hinaus haben wir insbesondere im Hinblick auf eine umfassende Aufklärung mit dem Projekt gemeinsam Verbesserungen an den diesbezüglichen Unterlagen vorgenommen; dies betraf insbesondere die Erläuterung des Verfahrens und die in Betracht kommenden Datenverarbeitungen. Wichtig war insoweit, dass der Text der Einwilligungserklärung auch so gefasst wurde, dass die Datenverarbeitungen von der Einwilligung nur umfasst sind, soweit es für die Erfüllung der Aufgaben der jeweiligen beteiligten Partner erforderlich ist. Auch hinsichtlich der Freiwilligkeit haben wir z.B. den Aspekt der Widerrufbarkeit und deren Folgen für die bis dahin angefallenen Daten stärker in den Aufklärungstext aufnehmen lassen. Damit die Betroffenen die Aufklärung und die Einwilligungserklärung auch verstehen können, übersetzt das Projekt diese Unterlagen in verschiedene Sprachen. Dadurch soll gewährleistet werden, dass die mehrheitlich fremdsprachigen Betroffenen die Unterlagen auch inhaltlich tatsächlich zur Kenntnis nehmen können.

4. Justiz

4.1 Änderung der Bundesnotarordnung

Als Organe der Rechtspflege fallen Notare eindeutig unter den Anwendungsbereich des Hamburgischen Datenschutzgesetzes und unterliegen damit der Kontrolle des Hamburgischen Datenschutzbeauftragten.

Die Bund-Länder-Arbeitsgruppe „Aufbewahrung von Notariatsunterlagen“ hat unter Beteiligung der Bundesnotarkammer Vorschläge zur Errichtung eines Elektronischen Urkundenarchivs erarbeitet. Der von der Bund-Länder-Arbeitsgruppe erarbeitete „Entwurf eines Gesetzes zur Neuordnung der Aufbewahrung von Notariatsunterlagen und Errichtung eines Elektronischen Urkundenarchivs bei der Bundesnotarkammer“ wurde uns im März 2015 durch die Behörde für Justiz und Gleichstellung im Rahmen einer Praxisbeteiligung zur Stellungnahme vorgelegt.

Der Gesetzentwurf sieht unter anderem Änderungen in den §§ 92, 93 Bundesnotarordnung (BNotO) vor, die zur Folge haben, dass die Aufsicht in jeder Hinsicht – also auch in Belangen des Datenschutzes – allein der Landesjustizverwaltung zusteht.

Gegenüber der Behörde für Justiz und Gleichstellung haben wir ausdrücklich betont, dass es nicht nachvollziehbar, sogar datenschutzrechtlich völlig inakzeptabel ist, dass Notare nicht mehr der Aufsicht der Landesdatenschutzbeauftragten unterstehen sollen. Die in der Gesetzesbegründung genannten Gründe, der Kontrollzuständigkeit der Landesdatenschutzbeauftragten stünde die notarielle „Verschwiegenheitspflicht" entgegen und eine parallele und damit doppelte Kontrolle des Datenschutzes durch Dienstaufsicht und Landesdatenschutzbeauftragten sei unnötig, überzeugen nicht.
Notare sind gemäß § 1 BNotO unabhängige Träger eines öffentlichen Amtes, die für die Beurkundung von Rechtsvorgängen und andere Aufgaben auf dem Gebiet der vorsorgenden Rechtspflege in den Ländern bestellt werden. Die Notare sind öffentliche Stellen der Freien und Hansestadt Hamburg im Sinne von § 2 Abs. 1 Hamburgisches Datenschutzgesetz (HmbDSG). Sie sind nicht gemäß § 23 Abs. 1 S. 2 HmbDSG von der Kontrollzuständigkeit ausgenommen, so dass Notare der Kontrollbefugnis hinsichtlich der Einhaltung der Vorschriften des HmbDSG und anderer Vorschriften über den Datenschutz unterfallen. § 23 Abs. 5 S. 1 HmbDSG statuiert eine allgemeine Verpflichtung, den HmbBfDI bei der Erfüllung seiner Aufgaben zu unterstützen. Hierzu wird dem HmbBfDI bzw. dessen Mitarbeitern, die ihn bei der Erfüllung seiner Aufgaben unterstützen, das Recht eingeräumt, Auskunft zu Fragen sowie die Einsicht in alle Unterlagen und Akten zu erhalten, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Dabei bestimmt § 23 Abs. 5 S. 3 HmbDSG ausdrücklich, dass gesetzliche Geheimhaltungsvorschriften diesem umfassenden Auskunfts- und Einsichtsverlangen nicht entgegengehalten werden können. Würde man schließlich der Argumentation in der Gesetzesbegründung folgen, wären auch andere Berufsgeheimnisträger gänzlich von der Kontrolle der Landesdatenschutzbeauftragten ausgenommen, wie z.B. Ärzte, Psychologen, staatlich anerkannte Sozialarbeiter oder staatlich anerkannte Sozialpädagogen, Krankenversicherungen u.s.w. (weitere Beispiele in § 203 StGB). Dies würde jedoch eine umfassende einheitliche Kontrolle und damit die Realisierung des Schutzes des informationellen Selbstbestimmungsrechts unmöglich machen.

Unabhängig davon unterliegen öffentliche Stellen stets der „doppelten Kontrolle", da sie grundsätzlich der Dienst- und Fachaufsicht unterliegen und unabhängig davon der Kontrollbefugnis des Landesdatenschutzbeauftragten. Warum eine andere Regelung für Notare gelten sollte, bleibt daher völlig unklar.

Es bleibt daher abzuwarten, ob die von uns erhobenen Bedenken in dem Gesetzentwurf Berücksichtigung finden.

4.2 Datenschutz in Rechtsanwaltskanzleien

Die Anwendung des Bundesdatenschutzgesetzes auf Rechtsanwältinnen und Rechtsanwälte als Daten verarbeitende Stellen wird durch die Regelung des anwaltlichen Berufsrechts grundsätzlich nicht verdrängt, sondern lediglich ergänzt. Zudem enthält die Bundesrechtsanwaltsordnung keine deckungsgleichen Normen zum Bundesdatenschutzgesetz und verdrängt dieses schon deshalb nicht.

Im Rahmen unserer aufsichtsrechtlichen Tätigkeit haben wir uns an verschiedene Rechtsanwältinnen und Rechtsanwälten gewandt. Zunehmend hatten sich Bürgerinnen und Bürger bei uns beschwert, weil Rechtsanwältinnen und Rechtsanwälte Auskünfte über die zu ihrer Person gespeicherten Daten nicht erteilt, unzureichend erteilt oder aber die Auskunftsersuchen der Bürgerinnen und Bürger schlicht ignoriert haben. Unsere an die Rechtsanwältinnen und Rechtsanwälte gerichteten Anfragen blieben in den allermeisten Fällen ebenfalls erfolglos. In zahlreichen Schriftwechseln brachten die Rechtsanwältinnen und Rechtsanwälte deutlich zum Ausdruck, dass das Bundesdatenschutzgesetz (BDSG) auf Rechtsanwältinnen und Rechtsanwälten keine Anwendung finde, weil Regelungen der Bundesrechtsanwaltsordnung (BRAO) und Berufsordnung für Rechtsanwältinnen und Rechtsanwälte (BORA) als bereichsspezifische Normen gegenüber den Datenschutzregelungen vorrangig seien. In den allermeisten Fällen wurde uns die Auskunft schlicht mit der anwaltlichen Schweigepflicht versagt.

Wir haben diese Entwicklung zum Anlass genommen und haben im Frühjahr 2015 die Hanseatische Rechtsanwaltskammer Hamburg (RAK Hamburg) um ein Gespräch gebeten. Zudem besteht seit geraumer Zeit auch zwischen den Rechtsanwaltskammern und den Datenschutzaufsichtsbehörden Unklarheit darüber, ob sich die Zuständigkeit der staatlichen Aufsichtsbehörden gemäß § 38 BDSG auf die Anwaltschaft erstreckt oder aber die berufsrechtlichen Regelungen abschließend sind und damit die Zuständigkeit und Aufsicht bei den Rechtsanwaltskammern verbleibt. Bisher konnte keine Einigung erzielt werden. Auch fehlt es an klarstellenden Regeln oder entsprechender Rechtsprechung.

Nicht eindeutig gerichtlich geklärt ist schließlich auch die Frage, inwieweit Rechtsanwältinnen und Rechtsanwälte vor dem Hintergrund der anwaltlichen Schweigepflicht dazu verpflichtet sind, den datenschutzrechtlichen Aufsichtsbehörden Auskunft im Sinne des § 38 Abs. 3 BDSG zu erteilen bzw. ob die Standesaufsicht durch die Rechtsanwaltskammern die Datenschutzaufsicht sogar gänzlich verdrängt.

Gegenüber der RAK Hamburg haben wir dargelegt, dass die Anwendung des BDSG durch die Regelung des anwaltlichen Berufsrechts grundsätzlich nicht verdrängt wird, sondern lediglich ergänzt. Zudem enthält die BRAO keine deckungsgleichen Normen

zum BDSG und verdrängt diese schon deshalb nicht. Dies wird insbesondere in folgenden drei Themenbereichen deutlich:

- Verstöße gegen technische und organisatorische Maßnahmen bei der Verarbeitung von personenbezogenen Daten (§ 9 BDSG),
- unternehmerische Tätigkeit bei Rechtsanwälten sowie
- Beschäftigtendatenschutz.

Für diese Themenbereiche finden sich weder in der BRAO noch in der BORA Regelungen.

Schließlich unterscheidet sich auch der Normzweck der BRAO vom Datenschutzrecht, denn während die berufsrechtliche Verschwiegenheitspflicht sich auf alle Geheimnisse zwischen Anwalt und Mandant bezieht und damit allein den Schutz des Vertrauensverhältnisses zwischen Anwalt und Mandant berücksichtigt, reicht das Datenschutzrecht weiter, weil es auch den Schutz von Gegnern des Mandanten oder sonstigen Dritten umfasst (so auch herrschende Meinung, vgl. Dix in Simitis, 8. Aufl. 2014, § 1, Rn. 170 m.w.N.). Damit verbleibt die datenschutzrechtliche Aufsicht über Rechtsanwältinnen und Rechtsanwälte bei den zuständigen Aufsichtsbehörden.

Zu den o.g. Themenbereichen haben wir im Einzelnen dargelegt:

- Verstoß gegen technische und organisatorische Maßnahmen bei der Verarbeitung von personenbezogenen Daten (§ 9 BDSG)

Sowohl die BRAO als auch die BORA enthalten für die Einhaltung von technischen und organisatorischen Maßnahmen bei der Verarbeitung personenbezogener Daten (vgl. § 9 BDSG) keine Normen und verdrängen das Bundesdatenschutzgesetz deshalb nicht. Daher werden wir Eingaben, die diese Fälle betreffen, bearbeiten.

Bisher handelt es sich insbesondere um Fälle der unverschlüsselten E-Mail Kommunikation. Gem. § 9 BDSG haben nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG, insbesondere die in der Anlage zu § 9 Satz 1 BDSG genannten Anforderungen, zu gewährleisten. Dabei bestimmt die Anlage zu § 9 Satz 1 Nr. 4 BDSG ausdrücklich:

> *„Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbe-*

zogenen Daten oder Datenkategorien geeignet sind,
[…]
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung […] nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können […].
Eine Maßnahme nach Satz 2 Nummer […] 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren."

Die Einhaltung der technischen und organisatorischen Maßnahmen wird grundsätzlich für nicht abdingbar gehalten. Betroffene können auch nicht darin einwilligen, dass ihre Daten ohne einen ausreichenden Schutz nach dem Stand der Technik verarbeitet werden. Das gilt auch für Rechtsanwälte.

- Unternehmerische Tätigkeit bei Rechtsanwältinnen und Rechtsanwälten

Auch für die Fälle, in denen Rechtsanwältinnen und Rechtsanwälte eindeutig unternehmerisch tätig sind, obliegt die datenschutzrechtliche Aufsicht den Datenschutzaufsichtsbehörden.

In der Vergangenheit hat es gerade im Bereich der Inkassodienstleistungen durch Rechtsanwälte eine Vielzahl von Beschwerden gegeben.

Ob durch den neu eingefügten § 43d BRAO, der nunmehr die anwaltlichen Darlegungs- und Informationspflichten speziell bei Inkassodienstleistungen gegenüber Privatpersonen regelt und somit eine anwaltliche Berufspflicht darstellt, ein Rücklauf der Beschwerdezahlen bei Nichterteilung der Auskunft im Zusammenhang mit Inkassodienstleistungen bei uns eintreten wird, bleibt abzuwarten. Zwar sind die Angaben aus § 43d BRAO und § 34 BDSG nicht deckungsgleich, dennoch gibt es hier Überschneidungen.

Da aber die Überwachung der anwaltlichen Berufspflichten den die Berufsaufsicht führenden Rechtsanwaltskammern und den Anwaltsgerichten obliegt, wäre bei einem Verstoß gegen § 43d BRAO die RAK Hamburg zuständig.

- Beschäftigtendatenschutz

Nach unserer Auffassung gibt es keine berufsrechtlichen Regelungen zum Beschäftigtendatenschutz (dies betrifft ausschließlich Arbeitnehmerdaten), so dass auch Beschwerden in diesem Bereich der ausschließlichen Zuständigkeit der Datenschutzaufsichtsbehörden unterliegen.

Wir werden in den o.g. Fällen sowie in den Fällen, in den sich Bürgerinnen und Bürger an uns wenden, weil sie einen Anspruch aus § 34 Abs. 1 BDSG gegenüber einer Rechtsanwältin oder einem Rechtsanwalt geltend machen, weiterhin unseren Prüfauftrag wahrnehmen.

Unsere Auffassung haben wir schließlich Ende Juli 2015 der RAK Hamburg schriftlich mitgeteilt und gebeten, die vorstehende Auffassung künftig zu beachten.

Die RAK Hamburg teilt unsere Meinung nicht.

Sollte eine einvernehmliche Lösung mit den beteiligten Stellen nicht möglich sein, dürfte an einer gerichtlichen Klärung kein Weg vorbeiführen.

4.3 Protokollierung lesender Zugriffe auf BASIS-Web

Mangels Zugriffsprotokoll ist im Nachhinein nicht nachvollziehbar, wer welche Gefangenendaten für welche Zwecke zur Kenntnis genommen hat. Eine lückenlose Protokollierung trägt zur Sicherstellung des informationellen Selbstbestimmungsrechts bei.

Im Sommer 2015 haben wir uns an das Amt für Justizvollzug und Recht der Justizbehörde - Abteilung Justizvollzug - gewandt, weil ein Petent die fehlende Protokollierungsmöglichkeit bei lesenden Zugriffen auf die im Buchhaltungs- und Abrechnungssystem im Strafvollzug (BASIS-Web) gespeicherten personenbezogenen Daten moniert hat.
BASIS-Web ist ein länderübergreifendes Projekt, dem gegenwärtig 13 deutsche Bundesländer und Luxemburg angehören. Das Land Nordrhein-Westfalen koordiniert federführend die Weiterentwicklung. In seiner aktuellen Version ist BASIS-Web eine umfassende Softwarelösung zur Datenverarbeitung und -verwaltung in Justizvollzugsanstalten. Die Fachanwendung unterstützt die Arbeitsvorgänge aller wichtigen Verwaltungsbereiche, strukturiert und vereinfacht Arbeitsabläufe. In BASIS-Web werden sämtliche Haftarten und -formen abgewickelt. Es dient u.a. der Aufnahme und Entlassung von Häftlingen, der Verwaltung von Gefangenengeldern, der Abwicklung und Dokumentation medizinischer Versorgung, dem Gefangeneneinkauf und der Arbeitsverwaltung. In Hamburg wird BASIS-Web seit 2006 eingesetzt.

Aus der uns vorliegenden Risikoanalyse ergibt sich, dass in BASIS-Web zumindest auch Daten mit Schutzbedarf „hoch“ verarbeitet werden. Daher haben wir gegenüber der Justizbehörde gefordert, dass auch lesende Zugriffe protokolliert werden müssen. Dies folgt insbesondere aus § 8 Hamburgisches Datenschutzgesetz (HmbDSG). Da das Hamburgische Strafvollzugsgesetz (HmbStVollzG) zu den technischen und organisatorischen Maßnahmen allenfalls rudimentäre Regelungen enthält, verweist es ergänzend auf § 8 Hamburgisches Datenschutzgesetz (HmbDSG).

§ 8 Abs. 2 Nr.5 HmbDSG schreibt für personenbezogene Daten, die automatisiert verarbeitet werden vor, dass technische und organisatorische Maßnahmen zu treffen sind, die geeignet sind zu gewährleisten, dass festgestellt werden kann, wer wann welche

personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit). Revisionsfähigkeit verlangt die Nachvollziehbarkeit der Datenverarbeitung. Hierzu gehört auch die Dokumentation der Verarbeitungsverfahren, soweit sie erforderlich ist, um festzustellen, in welcher Weise personenbezogene Daten verarbeitet werden. Revisionsfähigkeit wird durch die Maßnahme der Protokollierung umgesetzt. Üblicherweise müssen die Tätigkeiten der Authentifizierung und Autorisierung, der Dateneingabe und -veränderung, der Dateneinsicht (lesende Zugriffe), der Datenübermittlung und der Datenlöschung protokolliert werden (vgl. hierzu ausführlich die Orientierungshilfe „Protokollierung" des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder von 2009 , abzurufen unter:

https://www.datenschutz-hamburg.de/uploads/media/Orientierungshilfe_Protokollierung.pdf).

Wie für alle Sicherungsziele gilt auch für die Revisionsfähigkeit die Bestimmung des § 8 Abs. 1 Satz 2 HmbDSG. Danach sind technische und organisatorische Maßnahmen nur erforderlich, wenn ihr Aufwand in einem angemessenen Verhältnis zur Schutzwürdigkeit der Daten steht. Die Auswahl der zu treffenden Maßnahmen ist dabei aber durch eine Abwägung zwischen Schutzbedarf auf der einen und Aufwand auf der anderen Seite zu treffen.

Dies haben wir der Justizbehörde mitgeteilt. Allerdings stellte sich nach mehreren Gesprächen mit der Justizbehörde heraus, dass die Einstufung der Daten in BASIS-Web im Hinblick auf die Daten des Verfahrensteils des Ärztlichen Dienstes erfolgte, dieser aber von Hamburg bisher nicht genutzt wird. Im Zeitpunkt der Erstellung der Risikoanalyse war dieser Umstand jedoch noch nicht bekannt.

Damit festgestellt werden kann, welche technischen und organisatorischen Maßnahmen tatsächlich erforderlich sind, haben wir die Justizbehörde aufgefordert, bis Ende 2015 eine erneute Schutzbedarfsfeststellung vorzunehmen. Sollte sich herausstellen, dass die Daten lediglich einen Schutzbedarf von „normal" haben, wäre eine Protokollierung von lesenden Zugriffen nicht zwingend erforderlich. Sobald uns die Risikoanalyse vorliegt, werden wir bei Bedarf in weitere Gespräche mit der Justizbehörde eintreten.

5. Meldewesen

5.1 Hamburgisches Ausführungsgesetz zum Bundesmeldegesetz / Meldedatenübermittlungsverordnung / Spiegelmelderegister

Durch unsere Beteiligung und Intervention bei dem Gesetzgebungsverfahren zum Hamburgischen Ausführungsgesetz zum Bundesmeldegesetz (HmbAGBMG) und dem Erlass der Meldedatenübermittlungsverordnung (MDÜV) sowie der Verfahrenskonzeption des Spiegelmelderegisters konnten wir u.a. durch Verfahrensvorgaben und inhaltliche Überprüfungen erreichen, dass das informationelle Selbstbestimmungsrecht aller im Melderegister gespeicherten Bürgerinnen und Bürger im Rahmen des Bundesmeldegesetzes (BMG) möglichst gut sichergestellt wird. Ferner wurden die Anforderungen an ein mandantenfähiges Verfahren im IT-Konzept des Verfahrens festgeschrieben.

Wie bereits berichtet, wurde das Gesetzgebungsverfahren für das BMG von den Datenschutzbeauftragten des Bundes und der Länder intensiv begleitet. Nicht allen Forderungen der Datenschutzbeauftragten ist der Gesetzgeber nachgekommen, so dass das BMG aus datenschutzrechtlicher Sicht erhebliche Defizite aufweist (siehe hierzu 22.TB, III 17; 23. TB, III 17.1 und 24. TB, III 19.1).

Das am 01.11.2015 in Kraft getretene BMG ersetzt das bis dahin geltende Rahmen- und Landesrecht. Die für die Länder im BMG enthaltene Regelungsbefugnis hat die Freie und Hansestadt Hamburg durch Erlass des HmbAGBMG und einer neuen MDÜV wahrgenommen. Dadurch sollte zum einen das Hamburgische Melderecht der nach Inkrafttreten des BMG geltenden Rechtslage angepasst und zum anderen die Rechtsgrundlage für den Aufbau und Betrieb eines Spiegelregisters geschaffen werden. Mit dem Spiegelregister wollen die Hamburgischen Meldebehörden die Anforderungen des § 39 Abs. 3 BGM, wonach vor allem für die in § 34 Abs.4 S. 1 BMG genannten Sicherheitsbehörden ein Datenabruf zu jeder Zeit (also 24 h) sicherzustellen ist, umsetzen.

Wir wurden sowohl im Rahmen des Gesetz- und Verordnungsgebungsverfahrens als auch bei der Verfahrenskonzeption des Spiegelregisters beteiligt.

Hamburgisches Ausführungsgesetz zum BMG

Im Rahmen des Beteiligungsverfahrens zum vorgelegten Gesetzentwurf haben wir uns u.a. für die folgenden Punkte eingesetzt:

- Die datenschutzrechtliche Verantwortung für das Spiegelregister und dessen Inhalt, Aufgabe und Betrieb ist normenklar zu regeln.

- Zum Schutz der Rechte der Betroffenen sind Änderungen im originären zentralen Melderegisterbestand, wie die Eintragung einer Auskunftssperre unmittelbar im Spiegelregister umzusetzen.

- In das Ausführungsgesetz sind nicht nur die Einzelheiten des Aufbaus, Inhaltes und Betriebes des Spiegelregisters aufzunehmen, sondern es muss eine Verordnungsermächtigung beinhalten, auf deren Grundlage insbesondere auch die datenschutzgerechte technische und organisatorische Ausgestaltung der einzurichtenden Abruf- und Übermittlungsverfahren unter Beachtung der Grundsätze der Erforderlichkeit und Datensparsamkeit zu regeln ist.

- Die Regelung in § 4 Abs. 1 S. 4 des bisher geltenden Hamburgischen Meldegesetzes (HmbMG), wonach nur die zentrale Meldebehörde Zugriff auf sensible Daten wie Wahlberechtigung und Wählbarkeit sowie waffen- und sprengstoffrechtliche Erlaubnisse erhält, ist beizubehalten.

- Es ist vorzusehen, dass öffentlich-rechtliche Religionsgesellschaften, bevor Meldedaten an sie übermittelt werden dürfen, durch Vorlage eines Sicherheitskonzeptes gegenüber der für das Meldewesen zuständigen Behörde nachweisen müssen, dass sie ausreichende technische und organisatorische Maßnahmen zum Datenschutz getroffen haben.

Unsere Forderungen und Anregungen wurden im Gesetzgebungsverfahren aufgenommen und umgesetzt.

Hamburgische Meldedatenübermittlungsverordnung

Im Nachgang erfolgte auch die Anpassung der MDÜV. Bereits im Vorfeld des Verordnungsgebungsverfahrens wurden wir bei dem Entwurf des neuen Verordnungstextes beteiligt. Auch wenn das Ziel grundsätzlich die Anpassung des bisherigen Verordnungstextes an die neuen gesetzlichen Grundlagen war, sahen wir im Hinblick zum einen auf die bisherigen Regelungen und zum anderen auf neue Regelungen einige Änderungsbedarfe, damit das informationelle Selbstbestimmungsrecht der Betroffenen hinreichend gewahrt bleibt.

Verschiedenen Stellen sollte u.a. auch die Staatsangehörigkeit im Wege von regelmäßigen Datenübermittlungen oder von Abrufen übermittelt werden. Zum Teil konnten wir nachvollziehen, dass dieses Datum für die Aufgaben erforderlich ist; soweit uns die Erforderlichkeit nicht schlüssig erschien, haben wir um entsprechende Erläuterungen gebeten. Aufgrund der Rückmeldungen konnte die Übermittlung dieses Datums an einige Stellen aus dem Verordnungsentwurf gestrichen werden.

Ferner sah der Verordnungsentwurf vor, dass Polizeibehörden und dem Landesamt für

Verfassungsschutz im Wege des Datenabrufes das Datum „rechtliche Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft" übermittelt werden darf. Dies würde den Katalog abrufbarer Daten nach dem BMG erweitern. Aus unserer Sicht ist die Religionszugehörigkeit eine Information, welche als besonders sensibles personenbezogenes Datum zu qualifizieren ist und im Melderegister ausschließlich zum Zwecke der Kirchensteuererhebung gespeichert ist, nicht aber zu Zwecken der Informationsbeschaffung der genannten Behörden. Mit Blick auf die Kirchensteuererhebung sind im Melderegister somit auch nur die folgenden Religionen gespeichert: katholisch (alt- und röm.-), evangelisch (reformiert und lutherisch) sowie jüdisch. Daher äußerten wir Bedenken, ob nach den Grundsätzen der Erforderlichkeit und der Zweckbindung die Religionszugehörigkeit im Wege des Datenabrufes für die genannten Behörden abrufbar sein darf. Mangels hinreichender Begründungsmöglichkeit nahm zunächst die Polizei Abstand davon, die Religionszugehörigkeit im automatisierten Verfahren abrufen zu können. Nachdem das Landesamt für Verfassungsschutz zunächst wegen einer bundesweit angestrebten einheitlichen Regelung an seiner Forderung festgehalten hatte, wurde letztlich auch diese mangels Umsetzung in anderen Bundesländern zurückgezogen.

Aufgenommen wurde auf unsere Veranlassung hin auch die bereits früher existente Regelung zur Informationspflicht betroffener Bürgerinnen und Bürger in den Fällen, in denen es zu unzulässigen Datenverarbeitungen gekommen ist. Eine solche Regelung, die sich auch im Bundesdatenschutzgesetz (§ 42a BDSG) und im Sozialgesetzbuch (§ 83a SGB X) findet, dient nicht nur der Transparenz, sondern vor allem auch der Wahrnehmung und Realisierung des informationellen Selbstbestimmungsrechtes durch die Betroffenen. Nur wenn sie von einer unzulässigen Verarbeitung ihrer personenbezogenen Daten Kenntnis haben, können sie weitere Maßnahmen bis hin zu Schadensersatzforderungen ergreifen.

Des Weiteren sah § 1 Abs. 4 des Entwurfstextes vor, dass zur Sicherung der Datenintegrität bei regelmäßigen Datenübermittlungen die Übermittlung von Komplettdatenabzügen an die zuständige Behörde zulässig sei. Hintergrund war die Erfahrung, dass die Daten im Zentralen Schülerregister von den Daten im Melderegister abwichen, obwohl aufgrund einer regelmäßigen Übermittlung die Daten identisch sein müssten. Dies lag an technischen Fehlern; der Datenbestand im Zentralen Schülerregister musste daher durch einen umfänglichen Abgleich wieder auf den aktuellen Stand gebracht werden.

Im Hinblick auf die vorgesehene Entwurfsfassung wiesen wir jedoch darauf hin, dass hierin keine hinreichend bestimmte, normenklare und verhältnismäßige Regelung für einen Grundrechtseingriff zu sehen ist, vor allem weil ein Datenabgleich ohne jedwede Einschränkung zulässig sein sollte. Zu bedenken ist insoweit, dass nach der Freigabe-Richtlinie jede Software und jedes Datenverarbeitungsverfahren vor der Freigabe in einem Funktionstest und in einem Abnahmetest ausreichend daraufhin

zu prüfen ist, ob sie den fachlichen Anforderungen entspricht und in der geplanten Betriebsumgebung fehlerfrei abläuft. Erfolgt die Freigabe nur nach erfolgreich bestandenen Tests, dürfte es grundsätzlich zu keinen abweichenden Datenbeständen der vorliegenden Art kommen. Auch wenn es inhaltlich nur um diejenigen Daten geht, die der empfangenden Behörde ohnehin bekannt sein sollen, hielten wir eine Beschränkung der Regelung dahin gehend für notwendig, dass entweder Abweichungen festgestellt wurden bzw. dass die Möglichkeit des Abgleichs zur Wahrung der Richtigkeit des jeweiligen Datenbestandes nur in zeitlich eingeschränktem Turnus gegeben ist. Unserer Stellungnahme entsprechend wurde der Verordnungstexts angepasst und zusätzlich aufgenommen, dass unsere Behörde über einen solchen Datenabgleich zu informieren ist. So ist sichergestellt, dass wir von einem Datenabgleich Kenntnis erlangen, um die Voraussetzungen hierfür überprüfen zu können.

Spiegelmelderegister

Die Bundesländer Hamburg, Sachsen-Anhalt und Schleswig-Holstein haben eine gemeinsame IT-Infrastruktur aufgebaut, mit der die Anforderungen der §§ 38 ff. sowie 49 ff. BMG in Form bundesweiter elektronischer Abrufe von Meldedaten ab 01.11.2015 durch ein Spiegeldatenbanksystem umgesetzt werden. Dieses Spiegeldatenbanksystem existiert neben den jeweiligen Meldedatenverfahren in den Ländern. Änderungen von Meldedaten im originären Melderegister erfolgen in Hamburg durch die Meldebehörden in den Kundenzentren ausschließlich im Basisverfahren OK.EWO und werden in das Spiegeldatenbanksystem übertragen. Die Übertragung erfolgt auf Basis einer zwischen den Ländern Hamburg, Sachsen-Anhalt und Schleswig-Holstein vereinbarten Befüllungsvorschrift, welche die Datenübertragung im Detail regelt. Mit dieser Befüllungsvorschrift soll sichergestellt werden, dass im Zentralen Meldebestand (ZMB) nur Daten gespeichert werden, die für die Beantwortung von automatisierten Abrufen erforderlich sind.

Unsere Herangehensweise bei länderübergreifenden Projekten ist geprägt von einer möglichst engen Abstimmung mit den anderen beteiligten Landesdatenschutzbeauftragten, um zu einheitlichen datenschutzrechtlichen Anforderungen und einer einheitlichen Bewertung des Verfahrens zu kommen. Im Zuge der Erörterung mit der Fachlichen Leitstelle N/ITB in Hamburg konnten verschiedene datenschutzrechtliche Verbesserungen verankert werden:

Bei länderübergreifenden Projekten ist als ein zentraler Punkt in der Vorabkontrolle zu klären, durch welche technischen und organisatorischen Maßnahmen gewährleistet wird, dass die Daten der beteiligten Länder strikt voneinander getrennt sind. So muss u.a. gewährleistet sein, dass die Sachbearbeitung immer nur für die Daten eines Mandanten zugriffsberechtigt ist und keinen direkten Zugriff auf die Daten eines anderen Mandanten hat. Die Anforderungen an eine sogenannte Mandantentrennung haben die Datenschutzbeauftragten des Bundes und der Länder in einer Orientierungshilfe beschrieben. Im Projekt „Zentraler Meldebestand“ sind dabei zum einen die Melde-

daten der drei Länder durch entsprechende technische und organisatorische Maßnahmen zu trennen. In Hamburg ist aufgrund des bestehenden zentralen Melderegisters und der Allzuständigkeit der örtlichen Meldebehörden in den Bezirksämtern keine weitere Untertrennung der Meldedaten erforderlich. Im Zuge der Gespräche mit dem Projekt wurde jedoch deutlich, dass auch die Protokollierung der automatisierten Abrufe der hamburgischen Sicherheitsbehörden wie Polizei, Staatsanwaltschaft etc., die nach § 40 Abs. 3 BMG von der jeweiligen abrufenden Stelle vorzunehmen ist, in der gemeinsamen Infrastruktur Zentraler Meldebestand gespeichert werden soll. Für diese Protokolldaten ist jedoch die jeweils abrufende Sicherheitsbehörde die Daten verarbeitende Stelle und nicht die Meldebehörde. Daher müssen diese Protokolldatensätze unterschiedlichen Mandanten zugeordnet werden. Das Projekt hat auf der Grundlage der Orientierungshilfe ein Konzept zur technischen und organisatorischen Mandantentrennung vorgelegt, in dem zu treffende Maßnahmen festgeschrieben wurden.

Das Projekt kommt in seiner Schutzbedarfsfeststellung zu dem Ergebnis, dass der Schutzbedarf mit „hoch" zu bewerten ist. Wir vertreten demgegenüber die Auffassung, dass von einem „sehr hohen" Schutzbedarf auszugehen ist, da in diesem Verfahren auch die umfangreichen Meldedaten der Personen enthalten sind, für die nach § 51 BMG eine Auskunftssperre besteht. Von der Meldebehörde wird auf Antrag oder von Amts wegen eine solche Auskunftssperre im Melderegister eingetragen, wenn Tatsachen vorliegen, die die Annahme rechtfertigen, dass der betroffenen oder einer anderen Person durch eine Melderegisterauskunft eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen erwachsen kann. Eine Auskunftssperre wird nur eingetragen, wenn eine besondere Gefährdung auf den jeweiligen Einzelfall bezogen begründet wurde. Die Betroffenen müssen Tatsachen dargetan haben, die nach allgemeiner Lebenserfahrung geeignet sind, die befürchteten Beeinträchtigungen auszulösen. Allein schon in der Tatsache, dass eine Auskunftssperre eingerichtet ist, sehen wir bereits eine erste, entsprechend zu schützende Erkenntnis; umso mehr gilt dies für die dahinterstehenden weiteren personenbezogenen Daten. Gerade im Hinblick auf Vertraulichkeit und Verfügbarkeit gehen wir – angesichts der gesetzlichen Voraussetzungen für die Einrichtung einer Auskunftssperre – von schwerwiegenden Folgen aus, sollten diese Schutzziele verletzt werden und dadurch die eigentlich gesperrten Meldedaten Unbefugten bekannt werden. In unseren Hinweisen zur Erstellung von Risikoanalysen und Vorabkontrollen, die über unser Internet-Angebot abrufbar sind, sind als Beispiele für IT-Systeme mit sehr hohem Schutzbedarf neben medizinischen Daten lebenserhaltender Systeme solche Verfahren genannt, in denen die Identitätsdaten von verdeckten Ermittlern verarbeitet werden. Die Gefährdung etwa bei Verlust der Vertraulichkeit ist vergleichbar zu den Personen mit Auskunftssperre.

Zur Umsetzung der rechtlichen Vorgaben aus der MDÜV, die differenziert für jede abrufende Stelle den maximalen Umfang der abrufbaren Daten festschreibt und den Grundsätzen der Erforderlichkeit und Datensparsamkeit, wurde im IT-Verfahren ein

Checkbox-Verfahren eingerichtet. Der abrufenden Stelle wird eine Auflistung der für sie abrufbaren Daten angeboten. Der Sachbearbeiter muss entscheiden, welche dieser Daten im vorliegenden Einzelfall erforderlich sind und diese durch Anklicken auswählen. In der Default-Einstellung der Checkbox sind keine Daten ausgewählt.

In der Suchanfrage müssen die Abrufberechtigten zwingend das Feld Aktenzeichen füllen. Hier haben wir gefordert, dass es eine automatisierte Prüfung geben muss, die eine Mindestlänge der Eingabe sicherstellt und Trivialeingaben verhindert (vgl. IV 5.2). Diese Anforderung wurde von der Daten verarbeitenden Stelle anerkannt und soll in der nächsten Version in der ersten Jahreshälfte 2016 produktivgesetzt werden.

Bei der bisherigen Lösung von Online-Abrufen aus dem Melderegister wurde bei Abrufen eine Auskunftssperre unmittelbar nach der Eintragung des Sperrvermerks in das Melderegister berücksichtigt. Bei der geplanten Trennung von Meldeverfahren und Spiegelregister haben wir die Anforderung gestellt, dass die Einführung des Spiegelregisters nicht zu einer Verschlechterung der Situation führen darf. Die zunächst angedachte Lösung, hier lediglich einen täglichen Datenaustausch vorzusehen, hielten wir für völlig inakzeptabel. Eine moderne IT-Technik müsste in der Lage sein, eine unmittelbare Übertragung sicherzustellen, wie sie im § 5 Abs. 2 HmbAGBMG festgeschrieben ist. Auch wenn bei dem neuen Verfahren zunächst nur eine Aktivierung des Sperrvermerks innerhalb einer Stunde realisiert wird, sollten die technischen Möglichkeiten zukünftig genutzt werden, um eine gesetzeskonforme Lösung zu realisieren.

Die Prüfung des IT-Verfahrens haben wir uns für den nächsten Berichtszeitraum vorgenommen.

5.2 Prüfung des Abrufverfahrens aus dem Melderegister für Jobcenter

Es wurden gravierende Mängel an dem beim Bezirksamt Harburg – Amt für Zentrale Meldeangelegenheiten – eingerichteten automatisierten Abrufverfahren festgestellt.

Von der Polizei hatten wir eine Anzeige wegen eines unberechtigten Datenabrufs aus dem Melderegister durch einen Mitarbeiter des Jobcenters Harburg erhalten. Die Zuständigkeit für die datenschutzrechtliche Kontrolle über die Jobcenter als gemeinsamer Einrichtung nach SGB II obliegt nicht dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, sondern der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Daher haben wir den Vorgang dorthin zur Überprüfung der Rechtmäßigkeit der Datenerhebung durch das Jobcenter Harburg abgegeben. Gleichzeitig haben wir den Vorfall unsererseits zum Anlass genommen, beim

Bezirksamt Harburg – Amt für Zentrale Meldeangelegenheiten – das Verfahren des Datenabrufs aus dem Melderegister für Jobcenter zu überprüfen.

Rechtsgrundlagen für das Abrufverfahren zum Zeitpunkt des Abrufs waren § 31 Abs. 4 Hamburgisches Meldegesetz (HmbMG) und §§ 34 ff. Meldedatenübermittlungsverordnung (MDÜV). Danach können, sofern die Freischaltungsvoraussetzungen nach § 35 MDÜV vorliegen, durch nichthamburgische Behörden bei einem Grundabruf u.a. Daten wie Familiennamen, Vornamen, gegenwärtige Anschrift und Tag und Ort der Geburt abgerufen werden. Bei einem erweiterten Datenabruf können darüber hinaus Angaben wie etwa frühere Namen, Familienstand, Staatsangehörigkeit oder gesetzlicher Vertreter abgerufen werden. Für einen Datenabruf ist die betroffene Person durch die Angabe des Familiennamens und eines Vornamens sowie mindestens zwei der nachfolgenden Daten zu bezeichnen: Geburtsdatum, Geschlecht, eine frühere oder gegenwärtige hamburgische Anschrift. Die Übermittlung von Daten hat zu unterbleiben, wenn z.B. die Verwendung der Abruf-Merkmale dazu führt, dass die Daten nicht nur auf eine Person zutreffen oder eine Auskunftssperre nach § 34 Abs. 5 und 7 HmbMG besteht.

Die Abrufe sind unabhängig vom Ergebnis der Anfrage zu protokollieren und – je nach Art der Abfrage – zwischen 1 und 6 Monaten für Kontrollmaßnahmen im Rahmen der Dienst- und Fachaufsicht aufzubewahren. Die abrufenden Stellen sind verpflichtet, durch geeignete technische und organisatorische Maßnahmen zu gewährleisten, dass ein Abruf nur durch berechtigte Bedienstete im Rahmen ihrer Aufgaben erfolgt. Zu diesem Zweck wird in den Protokolldaten auch das Abfrage-Aktenzeichen protokolliert. Auch die Protokolldaten können zum Zwecke der Datenschutzkontrolle durch festgelegte autorisierte Berechtigte abgerufen werden.

Die abrufende Stelle hat für die ordnungsgemäße Durchführung des Abrufverfahrens eine verantwortliche Person zu benennen und der Meldebehörde u.a. festgestellte unberechtigte Abrufe anzuzeigen. Die Meldebehörde hat die Freischaltung des Abrufverfahrens unverzüglich aufzuheben, wenn die Freischaltungsvoraussetzungen nicht mehr vorliegen, also z.B. eine hinreichende Datenschutzkontrolle nicht sichergestellt ist oder wiederholt unberechtigt abgerufen wurde. Auf die insoweit bestehende Datenschutzkontrollpflicht haben wir die Meldebehörde im Rahmen unserer Prüfung hingewiesen, woraufhin von Seiten der Meldebehörde eine Überprüfung des Vorliegens der Freischaltungsvoraussetzungen bei dem Jobcenter Harburg eingeleitet wurde.

Bei der Überprüfung des Abrufverfahrens haben wir gravierende Mängel festgestellt. Dazu gehören:

- Es wurde nicht dokumentiert, ob und wenn ja welche Tests im Zuge der Freigabe des Abrufverfahrens durchgeführt wurden. Ein Testplan konnte nicht vorgelegt werden.

- In der vorgelegten Risikoanalyse wird von der Daten verarbeitenden Stelle festgestellt, dass für die automatisiert übermittelten Inhaltsdaten kein erhöhter Schutzbedarf bestehe. Diese Einschätzung wird von uns nicht geteilt. Im Falle einer Auskunftssperre sind die angefragten Daten, also z.B. Name und Anschrift einer Person, als besonders schützenswert zu bewerten. Diese Wertung wurde für jeden Abrufenden aus der Übertragung des Antwortschlüssels „15" (Keine Auskunft aufgrund einer Auskunftssperre) ebenso offensichtlich wie die Erkenntnis, dass bei dieser Meldebehörde Anschriftsdaten zu dieser Person überhaupt vorliegen; beides bietet Ansätze für einen möglichen Missbrauch. Ein automatisierter Abruf von Daten, bei denen ein erhöhter Schutzbedarf besteht, erfordert ein sicheres Authentisierungsverfahren. Ein solches ist nicht gewährleistet, wenn dieses ausschließlich auf der Nutzung von Benutzerkennung und Passwort basiert.

- Das Feld „Aktenzeichen" ist nicht als Pflichtfeld gekennzeichnet. Bei der Prüfung der Protokolldatensätze wurde festgestellt, dass in diesem Feld sehr häufig Trivialwerte wie „XX" oder „XXXXX" enthalten waren. Damit kann das Ziel der Protokollierung, die Prüfung der Erforderlichkeit eines konkreten Abrufes zur Erfüllung der Aufgaben der abrufberechtigten Person, nicht erreicht werden.

- Die MDÜV legt explizit fest, dass die „abgerufenen Daten" zu protokollieren sind. Daraus ergibt sich, dass bezüglich der Antwortdaten nur die tatsächlich übermittelten Daten zu protokollieren sind. Auch wenn der Antwortschlüssel „15" (Keine Auskunft aufgrund einer Auskunftssperre) übermittelt wurde, sind jedoch in dem dazugehörigen Protokolldatensatz „TrefferGebDatum", „TrefferGeschlecht", „TrefferAnschrift" enthalten. Auch diese Protokolldatensätze konnten durch die abrufberechtigten Stellen zu Zwecken einer dort durchzuführenden Kontrolle abgerufen werden, so dass diese Angaben dann im Wege des Datenabrufs übermittelt würden, obwohl bei Vorliegen einer Auskunftssperre ein automatisierter Datenabruf gerade nicht zulässig ist.

- Eine Verfahrensbeschreibung nach § 9 Hamburgisches Datenschutzgesetz wurde nicht erstellt.

Die Daten verarbeitende Stelle hat nach unserer Aufforderung die Möglichkeit des automatisierten Abrufs der Protokolldatensätzen unverzüglich unterbunden. Aufgrund der kurz bevorstehenden Ablösung des Abrufverfahrens aus dem Melderegister durch ein neues IT-Verfahren (s. IV 5.1) wurden die weiteren Mängel nicht mehr im bestehenden Verfahren behoben. Die aufgedeckten Schwachstellen wurden jedoch genutzt, um die Anforderungen an das neue Verfahren zu schärfen, um mit der Inbetriebnahme des neuen Abrufverfahrens zum 01.11.2015 diese Mängel des Abrufverfahrens aus dem Melderegister zu beseitigen. Dies werden wir im kommenden Berichtszeitraum überprüfen.

6. Personenstandswesen

6.1 Generalregisterverfahren

Ob für das historisch gewachsene Verfahren Generalregister, wie von uns gefordert, eine rechtskonforme Lösung gefunden wurde, konnten wir aufgrund noch nicht vorhandener Verordnungsregelungen sowie fehlender datenschutzrechtlicher Unterlagen noch nicht abschließend beurteilen. Da das neue Verfahren gleichwohl produktiv gesetzt wurde, haben wir eine zügige Umsetzung der ausstehenden Maßnahmen unter Benennung eines konkreten Zeitrahmens, bis wann die Arbeiten abgeschlossen sein werden, angemahnt.

Wie bereits berichtet (23. TB, III 17.3; 24. TB, III 18.2) wurden wir im Rahmen einer Ad-hoc-Prüfung bei der Standesamtlichen Registerstelle auf das Verfahren Generalregister aufmerksam. Das Generalregister war eine historisch gewachsene, spezifisch hamburgische Einrichtung. Aufgrund der damaligen Vielzahl von Standesämtern in Hamburg hatte man die Einrichtung eines zentralen Suchverzeichnisses für zweckmäßig erachtet, da so aufwendige Umlaufverfahren zur Ermittlung des für den Personenstandsfall zuständigen Standesamtes entbehrlich wurden. Im Laufe der Zeit wurde das papierne Suchverzeichnis in ein elektronisches Verfahren überführt. Das vorgefundene Verfahren, wies wie bereits berichtet, erhebliche rechtliche und technische Mängel auf. U.a. konnte für das Verfahren keine Verfahrensbeschreibung und Risikoanalyse vorgelegt werden, die Datenübertragungswege von den Standesämtern zur Registerstelle waren unzureichend abgesichert und es fehlte zudem an einer tragfähigen rechtlichen Grundlage. Wir hatten daher den Kreis der Verantwortlichen bestehend aus den Standesämtern, der Registerstelle, der fachlichen Leitstelle N/ITB und der Behörde für Inneres und Sport (BIS) als aufsichtsführende Fachbehörde aufgefordert, unter Beachtung der nach Inkrafttreten des neuen Personenstandsgesetzes 2009 und der Einführung des elektronischen Personenstandsregisters (ePR) 2012 geänderten Rechtslage gemeinsam eine rechtskonforme Lösung für das Verfahren zu erarbeiten. Hierzu wurde das Projekt „Zukünftiges Verfahren Generalregister" eingesetzt.

Wir haben das Projekt bezüglich der uns vorgestellten verschiedenen Lösungsansätze beraten und dabei auf noch zu klärende Fragen und notwendige rechtliche und technische Maßnahmen hingewiesen.

Im Mai 2015 wurde uns das Handbuch für das zukünftige Verfahren Generalregister mit der Bitte um eine datenschutzrechtliche Einschätzung übersandt. Darin wurde das Konzept des schließlich vom Projekt gewählten Lösungsansatzes dargestellt. Dieser beinhaltete, dass das neue Generalregisterverfahren als funktionelle Erweiterung des Zentralregisters im AutiSta-Client umgesetzt werden soll. Die berechtigten Nutzer

und Nutzerinnen erhalten danach Einsicht in die von den Standesämtern geführten AutiSta-Suchverzeichnisse für die papiernen Personenstandsbücher sowie in die Registereinträge des ePR aller hamburgischen Standesämter. Dies ermöglicht den Anwendern und Anwenderinnen das für den Personenstandsfall zuständige Standesamt zu ermitteln. Der bisher separate zentrale Datenbestand „Generalregister" bei der Registerstelle sollte entfallen.

In unserer Stellungnahme haben wir dem Projekt mitgeteilt, dass gegen die im Handbuch dargestellte Konzeption keine grundlegenden datenschutzrechtlichen Bedenken bestehen. Wir haben aber auch deutlich darauf hingewiesen, dass allein auf der Basis des übersandten Handbuches eine abschließende datenschutzrechtliche Beurteilung des geplanten neuen Generalregisterverfahrens nicht möglich ist. Eine solche kann nur unter Einbeziehung des organisatorischen und rechtlichen Rahmens, in welchen das Verfahren eingebettet werden soll, erfolgen. Dieser Rahmen war in den uns übersandten Unterlagen jedoch noch nicht hinreichend dargestellt. Es lagen noch keine aktuelle angepasste Verfahrensbeschreibung und Risikoanalyse und kein Entwurf des Verordnungstextes vor. Daher waren Fragegestellungen, wie etwa

- welchem Personenkreis Benutzerrechte für welche Aufgaben durch wen eingeräumt werden können,
- wo die datenschutzrechtliche Verantwortung liegt,
- wie die Protokollierung der Zugriffe erfolgt
- und durch welche Maßnahmen die Berücksichtigung von Sperrvermerken, welche aus den Suchverzeichnissen nicht ersichtlich sind, gewährleistet werden soll,

noch offen.

Überrascht hat uns daher die Mitteilung der fachlichen Leitstelle N/ITB, dass das Verfahren im November 2015 produktiv gesetzt wurde, man an der Verfahrensbeschreibung und Risikoanalyse arbeite und eine Verordnung wegen der hohen Belastung der BIS durch Aufgaben im Flüchtlingsbereich noch ausstehe.

Wir haben N/ITB darauf hingewiesen, dass auch unter Berücksichtigung der Tatsache, dass durch das neue Verfahren die datenschutzrechtlichen Defizite des Altverfahrens behoben werden sollten, für ein rechtskonformes Vorgehen die vorgeschriebene Reihenfolge, d.h. Schaffung einer Rechtsgrundlage, Erstellung und Abstimmung von Risikoanalyse und Verfahrensbeschreibung einzuhalten sind. Wir haben eine zügige Umsetzung der ausstehenden Maßnahmen unter Benennung eines konkreten Zeitrahmens, bis wann die Arbeiten abgeschlossen sein werden, angemahnt.

6.2 Automation im Standesamt (AutiSta)

Unseren Bedenken hinsichtlich der Einrichtung eines fiktiven Standesamtes in der Produktionsumgebung für Testzwecke wurde gefolgt. Ein in der Produktivumgebung von AutiSta und elektronischem Personenstandsregister eingerichteter Testmandant wurde inzwischen wieder aus der Produktivumgebung entfernt.

Die Arbeitsprozesse in den Hamburger Standesämtern werden durch das Fachverfahren AutiSta des Verlages für Standesamtswesen unterstützt. Vor der Einführung des elektronischen Personenstandsregisters beschränkte sich das Verfahren auf die Unterstützung bei der Vorbereitung und Durchführung von Beurkundungen sowie begleitende Prozesse wie Verwaltungsaufgaben und die Führung elektronischer Namensverzeichnisse. Mit der Einführung des elektronischen Personenstandsregisters (ePR) hat das Fachverfahren zusätzlich die Aufgabe bekommen, das elektronische Personenstandsregister mit Daten zu beliefern und dessen Daten weiter zu bearbeiten.

Entsprechend der Verfahrensänderungen waren die datenschutzrechtlichen Verfahrensunterlagen anzupassen. Bei deren Durchsicht stellten wir u.a. Ungereimtheiten hinsichtlich der Anzahl der ausgewiesenen Standesamtsmandanten fest. Wie sich herausstellte, war für den Test der abschließenden Verfügung eines Personenstandsfalles mit Signaturkarte in der AutiSta und ePR-Produktivumgebung ein Testmandant eingerichtet worden. Für dieses Testverfahren lag keine Sicherheitskonzeption vor, ebenso wenig war eine Risikobewertung des Verfahrens erfolgt. Gegen dieses Vorgehen, die Aufhebung der Trennung von Test- und Produktionssystem, haben wir Bedenken geäußert. Die Durchführung von Tests darf keine Auswirkungen auf den Produktionsbetrieb und die Produktionsdatenbestände (amtliche Register) haben. Daher sollten Tests grundsätzlich in einer isolierten Testumgebung ohne Verbindung zu einem Verfahren im Produktivsystem erfolgen (s. hierzu die Freigaberichtlinie der FHH, die Orientierungshilfe „Daten, Datenschutz und Datensicherheit in Projekten: Projekt- und Produktivbetrieb“ des AK Technik der Datenschutzbeauftragten des Bundes und der Länder und den BSI Grundschutz-Maßnahmenkatalog).

Unsere Bedenken wurden aufgegriffen. Das Teststandesamt wurde nach unserer Stellungnahme zeitnah aus der AutiSta-Produktivumgebung entfernt. Schwieriger gestaltete sich die Löschung des Testmandanten aus dem ePR. Inzwischen hat uns jedoch auch hier die Löschungsbestätigung erreicht.

7. Statistik

7.1 Registergestützte Volkszählung Zensus 2011 – Löschung der Hilfsmerkmale

Der Zensus 2011 mit seinem registergestützten Stichprobenverfahren und den Löschungsvorschriften für die Hilfsmerkmale steht nun auf dem Prüfstand des Bundesverfassungsgerichtes.

Über den Zensus 2011 haben wir in der Vergangenheit bereits berichtet (vgl. 21. TB, 5.2, 23. TB, III 19.1, 24. TB III 17.1). Von der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wurde ein Eckpunktepapier mit datenschutzrechtlichen Forderungen für einen künftigen Zensus 2021 veröffentlicht *http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/EckpunktepapierZensus2021.html?nn=408908.* Dieses beruht auf den Ergebnissen der von der Bund-Länder-Arbeitsgruppe der Datenschutzbeauftragten zum Zensus 2011 diskutierten Fragestellungen und Erfahrungen.

Wie zuletzt berichtet, lag nach Abschluss der Erhebungsphase und Bekanntgabe der aus dem Zensus 2011 ermittelten amtlichen Bevölkerungszahlen am 31. Mai 2013 das Augenmerk aus datenschutzrechtlicher Sicht vor allem auf der Einhaltung der gesetzlichen Löschfristen für die Hilfsmerkmale. Hilfsmerkmale sind Angaben, die einen direkten Personenbezug zu den Betroffenen herstellen und der technischen Durchführung der Statistik dienen, wie beispielsweise Name und Anschrift einer Person. Diese sind zum frühestmöglichen Zeitpunkt von den eigentlichen statistischen Daten, den sogenannten Erhebungsmerkmalen, zu trennen. Während die Erhebungsmerkmale dauerhaft gespeichert werden, sind die Hilfsmerkmale nach § 19 ZensG2011 zu löschen, sobald bei den statistischen Ämtern die Überprüfung der Erhebungs- und Hilfsmerkmale auf ihre Schlüssigkeit und Vollständigkeit abgeschlossen ist. Spätestens jedoch vier Jahre nach dem Berichtszeitpunkt (09.05.2011), also mithin zum 09.05.2015. Zentrale Frage war, welche Hilfsmerkmale für die Durchführung und Kontrolle der Erhebungen nicht mehr erforderlich sind und damit frühzeitig bzw. welche Hilfsmerkmale noch benötigt werden und erst zur gesetzlichen Höchstfrist gelöscht werden können. Vom Statistischen Amt für Hamburg und Schleswig-Holstein (Statistikamt Nord) hatten wir ein Löschkonzept angefordert, anhand dessen der jeweils aktuelle Stand der Löschungen festgestellt werden kann. Wir haben uns regelmäßig über den Stand der Löschung der Hilfsmerkmale unterrichten lassen und diesen auch in mehreren Besprechungen mit dem Statistikamt Nord erörtert.

Aufgrund der Aufgabenzuweisung durch das Zensusgesetz 2011 (ZensG2011) wurden Hilfsmerkmale von Bürgerinnen und Bürgern aus Hamburg und Schleswig-Holstein nicht nur beim Statistikamt Nord, sondern auch bei den Statistikämtern verarbeitet, denen durch § 12 ZensG2011 besondere zentrale Datenverarbeitungen wie die Haus-

haltsgenerierung, die Haushaltsstichprobe, das Anschriften- und Gebäuderegister oder der Referenzdatenbestand zugewiesen sind (Poolstatistikämter).

Gegen die durch die Statistikämter festgestellten amtlichen Einwohnerzahlen haben in ganz Deutschland viele Gemeinden Widerspruch eingelegt bzw. Klage erhoben. Die Gemeinden zweifeln das Verfahren und die Rechtmäßigkeit der Feststellung der Einwohnerzahlen an. Neben Hamburg wurde von 150 schleswig-holsteinischen Gemeinden Widerspruch eingelegt. Zum Teil wurden von den Gemeinden beim Statistikamt Nord Datenhaltungsanträge bezüglich der dort vorliegenden Datenbestände mit Hilfsmerkmalen gestellt. Das Statistikamt Nord teilte uns mit, dass einige der dort als auch in den Poolstatistikämtern noch vorliegenden Hilfsmerkmale erst zur gesetzlichen Höchstfrist gelöscht werden würden, weil diese zur Überprüfung im Rahmen des Widerspruchsverfahrens noch benötigt werden könnten. Auf Nachfrage erklärte uns das Statistikamt, dass dies bei Gemeinden, die keinen Widerspruch eingelegt oder diesen später zurückgenommen haben, nicht zutrifft, so dass bezüglich dieser Gemeinden die Löschung der Hilfsmerkmale noch vor Ablauf der Höchstfrist erfolgen konnte.

Im April 2015 teilte uns das Statistikamt Nord mit, dass man dort mit Blick auf den kurz bevorstehenden spätesten Löschtermin und den von der Stadt Hamburg im Rahmen des Widerspruchverfahrens gestellten außergerichtlichen Datenhaltungsantrag prüfe, ob es zulässig sei, die nach § 3 ZensG2011 zur Durchführung des Zensus vom Melderegister zu den jeweiligen Stichtagen übermittelten Melderegisterdaten an die Stadt Hamburg zu übermitteln; hierzu wurden wir um eine rechtliche Einschätzung gebeten. In unserer Stellungnahme haben wir dem Statistikamt ausführlich dargelegt, dass eine solche Datenübermittlung unzulässig ist, weil es an einer Rechtsgrundlage fehlt, dies zudem eine Umgehung der Löschungsverpflichtung aus § 19 ZensG2011 wäre und darüber hinaus einen Verstoß gegen die statistische Geheimhaltung und das vom Bundesverfassungsgericht im Volkszählungsurteil aufgestellte Rückspielverbot von Daten aus der statistischen Erhebung an die Verwaltung darstellen würde.

Mit dem Näherrücken der gesetzlichen Höchstfrist für die Löschung am 09.05.2015 wurden bundesweit die Verwaltungsgerichte mit der Frage befasst, ob eine weitere Datenhaltung der Datenbestände mit Hilfsmerkmalen zur Durchführung der Widerspruchs- und Klageverfahren erforderlich und zulässig ist. Während einige Verwaltungsgerichte dies u.a. wegen des ausdrücklichen Löschungsgebotes des § 19 ZensG2011 ablehnten, wurde durch andere Gerichte mit sehr unterschiedlichen Begründungen eine Datenhaltung im Wege des einstweiligen Rechtsschutzes oder als prozessleitende Maßnahme angeordnet. Eine Rolle spielte dabei auch die Frage, ob es gänzlich ausgeschlossen ist oder ob prozessuale Möglichkeiten bestehen, die dem Statistikgeheimnis unterliegenden Zensusdaten zum Gegenstand eines Verwaltungsprozesses zu machen.

Das Statistikamt Nord hat uns darüber unterrichtet, dass es der gesetzlichen Ver-

pflichtung zur Löschung aus § 19 ZensG2011 nachgekommen ist. Die im Statistikamt Nord noch vorhandenen Hilfsmerkmale der Betroffenen aus Hamburg seien gelöscht worden, da das Verwaltungsgericht den Eilantrag der Stadt Hamburg gegen die Datenlöschungen zurückgewiesen hat. Mit Ausnahme der Stadt Flensburg, hier hat das OVG Schleswig auf die Beschwerde der Stadt Flensburg gegen den ablehnenden Beschluss des VG Schleswig hin die weitere Datenhaltung angeordnet, seien auch die Hilfsmerkmale aus den noch widerspruchführenden Gemeinden Schleswig-Holsteins gelöscht worden.

In den sogenannten Poolstatistikämtern liegen die Hilfsmerkmale aufgrund verwaltungsgerichtlicher Datenhaltungsanordnungen zum Teil noch vor.

Mit einer Eilentscheidung am 26.08.2015 (BVerfG, B.v. 26.08.2015, 2 BvF 1/15) setzte das Bundesverfassungsgericht (BVerfG) auf einen Normenkontrollantrag des Berliner Senats hin die Löschungsvorschrift des § 19 ZensG2011 bis zur Entscheidung in der Hauptsache, längstens jedoch für die Dauer von 6 Monaten, außer Vollzug. Im Rahmen seiner Folgenabwägung hinsichtlich des Rechts der Betroffenen auf informationelle Selbstbestimmung und einer möglichen Rechtsschutzvereitelung der betroffenen Gemeinden bezüglich der Überprüfung der Rechtmäßigkeit der festgestellten Einwohnerzahlen ist das BVerfG zu dem Ergebnis gelangt, dass ein einstweiliger Löschungsstopp geboten ist. Ausdrücklich offen gelassen hat das BVerfG die Frage, ob sich die von den Verwaltungsgerichten verfügten Löschungsuntersagungen noch im Rahmen einer zulässigen verfassungskonformen Auslegung bewegten oder ob die Gerichte die Frage der Vereinbarkeit von § 19 ZensG2011 mit dem Grundgesetz dem BVerfG nach Art. 100 Abs. 1 GG hätten vorlegen müssen.

Die Entscheidung des BVerfG über die Verfassungsgemäßheit des ZensG2011 und damit über die Rechtmäßigkeit des Zensus 2011, der anders als frühere Volkszählungen als registergestütztes Stichprobenverfahren durchgeführt wurde, bleibt jetzt abzuwarten.

7.2 Landesinformationssystem (LIS)

Das Statistische Amt für Hamburg und Schleswig-Holstein hat auf unsere Bedenken hinsichtlich der besonderen Form der Bereitstellung statistischer Daten auf Datenträgern, welche den Empfängerinnen und Empfängern die selbständige Auswertung der zugrundeliegenden Daten ermöglicht, reagiert und wird das bisher vorgesehene Konzept so nicht mehr umsetzen.

In den letzten Tätigkeitsberichten (23. TB, III 19.2; 24.TB, III 17.2) hatten wir ausführlich über die Einführung des Landesinformationssystems (LIS) beim Statistischen Amt für Hamburg und Schleswig-Holstein (Statistikamt Nord) berichtet. Die LIS-Kernan-

wendung dient der internen, zentralen Datenhaltung und Auswertung von Daten aus Anwendungen der amtlichen Statistik. Der Öffentlichkeit werden explizit freigegebene, aggregierte Daten in einer von der LIS-Kernanwendung getrennten LIS-Onlinedatenbank zum Abruf bereitgestellt. Die Bereitstellung statistischer Einzeldatensätze für andere Behörden über ein LIS-Extranet hatte das Statistikamt Nord aufgrund unserer Bedenken und rechtlichen Hinweise zurückgestellt. Auch in weiteren Erörterungen der Verfahrenskonzeption konnten unsere datenschutzrechtlichen Bedenken hinsichtlich der statistischen Geheimhaltung und Abschottung nicht ausgeräumt werden.

Im aktuellen Berichtszeitraum wurden wir auf eine weitere vom Statistikamt Nord vorgesehene Form der Datenbereitstellung aufmerksam. Für die Beantwortung von externen Anfragen sollen hierbei Daten zusammengestellt werden, welche die Anfragenden auf CD erhalten und mit LIS-Funktionalitäten selbst statistisch auswerten können. Die Auswertungsergebnisse werden hierbei grundsätzlich erst zum Zeitpunkt der Abfrage aus den zugrundeliegenden CD-Daten generiert.

Diese Art der Datenbereitstellung setzt voraus, dass die Daten aus der geschützten LIS-Kernanwendung exportiert und herausgegeben werden dürfen. Grundsätzlich ist das Statistikamt Nord nur befugt, statistische Ergebnisse unter Wahrung der statistischen Geheimhaltung herauszugeben. Nur ausnahmsweise dürfen nach § 16 Abs. 4 Bundesstatistikgesetz (BStatG) für dort festgelegte Zwecke und Empfänger Tabellen mit statistischen Ergebnissen übermittelt werden, bei denen Tabellenfelder nur einen einzigen Fall ausweisen. Seitens des Statistikamtes war daher bereits vorgesehen, dass Zeitscheiben, Dimensionen und Ausprägungen im Vorfeld des Datenexports vom verantwortlichen Fachbereich festgelegt werden und der Export der so ausgewählten Daten mit Hilfe des LIS-Auswertungsmoduls erfolgt.

In diesem Verfahren ist die Datenbereitstellung nicht auf herkömmliche, bereits erstellte Tabellen mit statistischen Ergebnissen beschränkt. Entsprechende Ergebnisse sollen vielmehr durch die Datenempfängerinnen und -empfängern durch Abfragen generierbar sein. Dabei unterliegen die Daten mit ihrem Export nicht mehr dem Zugriffsschutz der LIS-Kern-Anwendung. Mit ihrer Herausgabe entziehen sie sich vielmehr jedweder weiteren Nutzungskontrolle durch das Statistikamt. Daraus ergab sich die zentrale Fragestellung, ob die Daten vor der Datenspeicherung und der Herausgabe durch das Statistikamt hinreichend aggregiert werden bzw. ob und wie wirksam ausgeschlossen werden kann, dass auf der LIS-CD Einzeldatensätze enthalten sind. Dies haben wir neben weiteren Fragestellungen hinsichtlich der technisch-organisatorischen Ausgestaltung des Verfahrens problematisiert und ausgiebig mit dem Statistikamt Nord erörtert. Auf Nachfrage teilte uns das Statistische Amt nunmehr mit, dass das bisherige Konzept der LIS-CD nicht mehr umgesetzt wird. Wir werden uns über etwaige Konzeptionsänderungen informieren lassen und der Sache weiter nachgehen.

8. Bezirke

8.1 Online-Übertragungen aus Sitzungen der Bezirksversammlungen

Öffentliche Fragestunden im Rahmen bezirklicher Gremienarbeit dienen der demokratischen Kontrolle der Abgeordneten durch ihre Wähler und der Transparenz der politischen Entscheidungen in Angelegenheiten der örtlichen Gemeinschaft. Gleichwohl muss das informationelle Selbstbestimmungsrecht der an Sitzungen teilnehmenden Bürgerinnen und Bürger unabhängig davon beachtet werden, ob sie der Sitzung nur beiwohnen oder sich aktiv im Rahmen der Fragestunde beteiligen wollen.

Immer wieder wird der Vorschlag unterbreitet und zum Teil auch umgesetzt, Sitzungen von Bezirksversammlungen und ihren Ausschüssen per Livestream zu übertragen und hierdurch bzw. auch durch eine anschließende Verfügbarkeit im Internet einer Öffentlichkeit zugänglich zu machen, die über den Rahmen der jeweiligen konkreten Veranstaltung hinausgeht. Bereits im letzten Tätigkeitsbericht hatten wir hierzu ausführlich berichtet (vgl. 24. TB, III 16.2).

Seinerzeit stand die bzw. der einzelne Abgeordnete im Fokus; nunmehr geht es um die Frage, inwieweit die an der Sitzung teilnehmenden Bürgerinnen und Bürger in ihren Rechten auf informationelle Selbstbestimmung beeinträchtigt sind. Insbesondere bei einer öffentlichen Fragestunde als einem demokratischen Kontrollinstrument kann es zu Kollisionen mit dem Datenschutz kommen:

Während seinerzeit die Bezirksverwaltung selbst das Livestreaming anstrebte, wurde uns nun mitgeteilt, dass im Bezirksamt Altona Sitzungen der Bezirksversammlung und ihrer Ausschüsse durch einen Online-Dienst ins Internet eingestellt würden. Dieser wird durch den Vorsitzenden der Bezirksversammlung bzw. des Ausschusses auf der Grundlage der geltenden Geschäftsordnung zugelassen. Hiermit verbunden war die Übertragung auch der öffentlichen Fragestunden und Anhörungen ins Internet.

Der uns dargestellte Ablauf der öffentlichen Fragestunde sah dabei vor, dass diejenigen Bürgerinnen und Bürger, die von ihrem Fragerecht Gebrauch machen wollen, vom Vorsitzenden aufgefordert werden, zunächst ihren Namen und den Bezug zum jeweiligen Thema, teilweise auch die berufliche Tätigkeit, deutlich zu benennen. Insoweit stellt sich neben der Besorgnis, dass eine Aufzeichnung der Sitzung auf viele Menschen eher abschreckende Wirkung entfaltet und so der Realisierung ihrer demokratischen Kontrollrechte entgegenstehen kann, datenschutzrechtlich die Frage, inwieweit diese Informationsbeschaffung durch die Bezirksversammlung und die durch sie geforderte Informationspreisgabe überhaupt erforderlich bzw. durch Gesetz oder

aufgrund von Gesetzen gerechtfertigt sein kann.

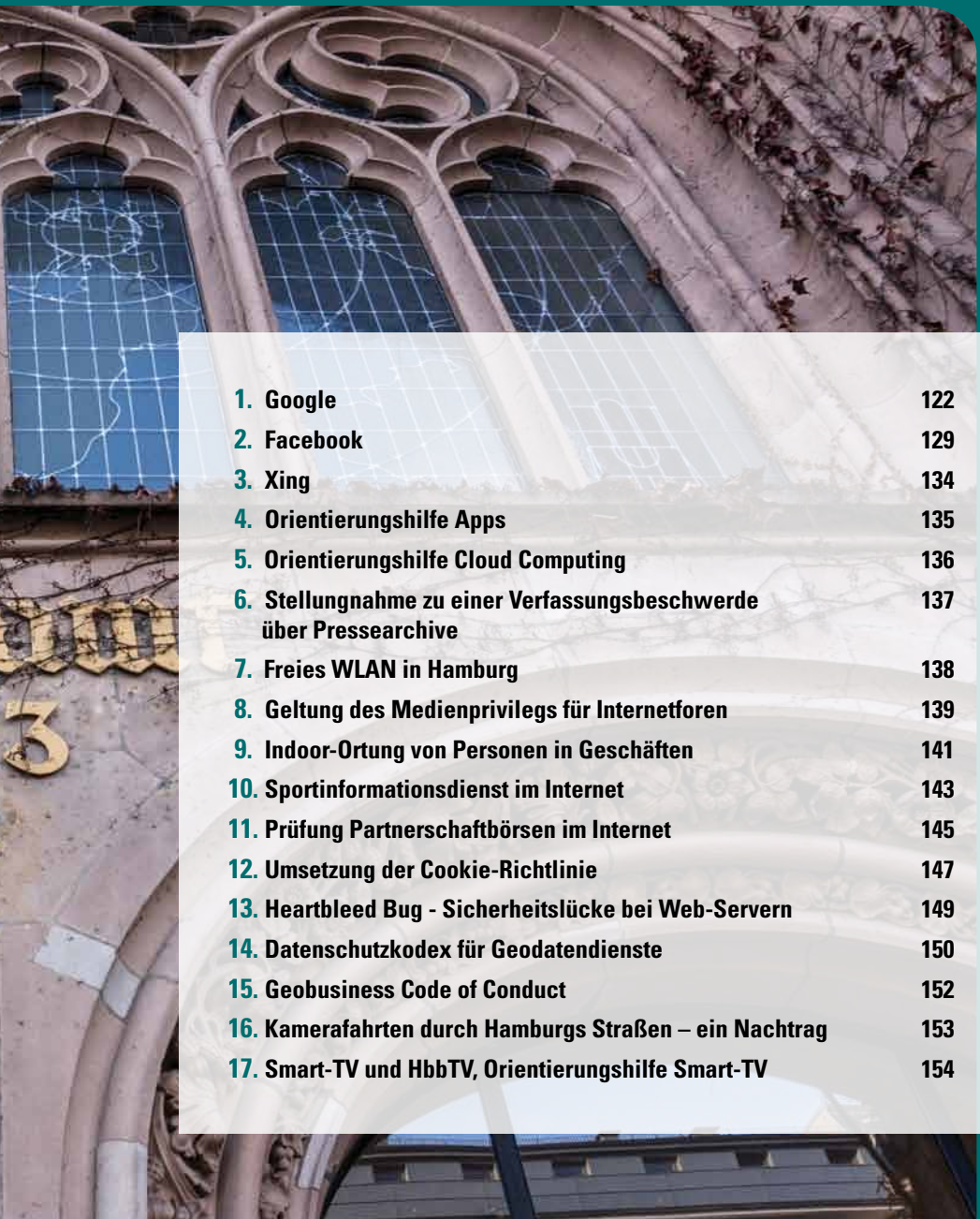
Immerhin haben Bürgerinnen und Bürger grundsätzlich das Recht, sich im öffentlichen Raum unbeobachtet bewegen zu können. Hier sehen wir bei derzeitiger Gesetzeslage keine Grundlage dafür, dass Bürgerinnen und Bürger nur unter einer über den Rahmen der jeweiligen konkreten Veranstaltung hinausgehenden öffentlichen Preisgabe ihrer Identität ihre demokratischen Rechte wahrnehmen dürfen. Eine allgemeine Regelung in der Geschäftsordnung kann daher nicht zu einer verfassungskonformen Einschränkung des Grundrechtes auf informationelle Selbstbestimmung führen, so dass eine solche Praxis rechtswidrig ist.

Wir stehen einer Online-Übertragung aus Sitzungen der Bezirksversammlung und ihrer Ausschüsse nicht per se ablehnend gegenüber; sie kann die Transparenz staatlichen Handelns deutlich fördern. Dennoch darf dies nicht über die Grundrechte der Betroffenen gestellt werden. Wir haben daher die betreffende Bezirksversammlung aufgefordert, von der Aufforderung zur Preisgabe personenbezogener Daten abzusehen und z.B. die Kameraführung auf das Rednerpult zu beschränken.

Wie bereits in anderen Ländern erfolgt und in unserem letzten Tätigkeitsbericht dargestellt, halten wir eine bereichsspezifische gesetzliche Regelung im Bezirksverwaltungsgesetz für dringend geboten, die die Aufzeichnung ganzer Sitzungen der Bezirksversammlungen und ihrer Ausschüsse sowie deren Übertragung ins Internet ausdrücklich regelt. Solange gesetzliche Grundlagen noch nicht geschaffen sind, kommt die Erhebung und vor allem die Übertragung personenbezogener Daten der teilnehmenden Bürgerinnen und Bürger nach wie vor ausschließlich auf der Grundlage deren informierter Einwilligung in Betracht. Hierfür reicht allerdings der bloße Hinweis durch den Vorsitzenden als Grundlage einer konkludenten Einwilligung angesichts der mit der weltweiten Übertragung verbundenen Eingriffstiefe nicht aus. Eine ausdrückliche Zustimmung wäre erforderlich.

Wir gehen davon aus, dass die Bezirksversammlungen den rechtlichen Vorgaben des Datenschutzes künftig entsprechen werden. Gern bieten wir hierzu unsere Hilfe an.

TELEMEDIEN V.



1. Google 122
2. Facebook 129
3. Xing 134
4. Orientierungshilfe Apps 135
5. Orientierungshilfe Cloud Computing 136
6. Stellungnahme zu einer Verfassungsbeschwerde über Pressearchive 137
7. Freies WLAN in Hamburg 138
8. Geltung des Medienprivilegs für Internetforen 139
9. Indoor-Ortung von Personen in Geschäften 141
10. Sportinformationsdienst im Internet 143
11. Prüfung Partnerschaftbörsen im Internet 145
12. Umsetzung der Cookie-Richtlinie 147
13. Heartbleed Bug - Sicherheitslücke bei Web-Servern 149
14. Datenschutzkodex für Geodatendienste 150
15. Geobusiness Code of Conduct 152
16. Kamerafahrten durch Hamburgs Straßen – ein Nachtrag 153
17. Smart-TV und HbbTV, Orientierungshilfe Smart-TV 154

1. Google

1.1 Suchmaschine/Bearbeitung von Eingaben zu abgelehnten Google-Löschanträgen

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit bearbeitet in Deutschland Eingaben in Fällen, in denen es die Google Inc. abgelehnt hat, Suchergebnisse zu entfernen, die bei der Eingabe des Namens einer Person in die Internetsuchmaschine des Unternehmens angezeigt werden.

Dieser Prüfungstätigkeit liegt das Urteil des Europäischen Gerichtshofes (EuGH) vom 13.05.2014 (C-131/12) zugrunde. Der EuGH hat entschieden, dass

- die Tätigkeit einer Suchmaschine – sofern personenbezogene Daten betroffen sind – eine Verarbeitung personenbezogener Daten im Sinne der europäischen Datenschutzrichtlinie 95/46/EG ist und der Betreiber der Suchmaschine als für diese Verarbeitung Verantwortlicher anzusehen ist;

- europäisches Datenschutzrecht bzw. das jeweilige Datenschutzrecht der europäischen Mitgliedsstaaten auf die Datenverarbeitung anwendbar ist, wenn ein außereuropäischer Betreiber einer Suchmaschine in einem Mitgliedsstaat eine Zweigniederlassung oder Tochtergesellschaft für die Förderung des Verkaufs der Werbeflächen der Suchmaschine und diesen Verkauf selbst gründet, deren Tätigkeit auf die Einwohner dieses Staates ausgerichtet ist;

- bei der Anwendung der einschlägigen datenschutzrechtlichen Bestimmungen zu prüfen ist, ob die betroffene Person ein Recht darauf hat, dass die Informationen über sie zum gegenwärtigen Zeitpunkt nicht mehr durch Suchergebnisse bei Eingabe ihres Namens in die Suchmaschine angezeigt werden;

- ein Suchmaschinenbetreiber bei Vorliegen der Voraussetzungen dazu verpflichtet ist, Suchergebnisse zu entfernen, auch wenn der Name oder die Informationen auf den Internetseiten nicht vorher oder gleichzeitig gelöscht werden, und gegebenenfalls auch dann, wenn ihre Veröffentlichung auf den Internetseiten als solche rechtmäßig ist.

Diese Entscheidung des EuGH wird allgemein als Begründung für das sogenannte „Recht auf Vergessenwerden" verstanden. Ein solches „Recht auf Vergessenwerden" gibt es jedoch nicht. Inhaltlich ist diese Bezeichnung auch unrichtig, da im Falle der Entfernung eines Suchergebnisses zu dem Namen einer Person der Inhalt auf der Internetseite, von der die Informationen stammen, bzw. in der Quelle nicht entfernt wird.

Da aber das Auffinden von Inhalten im Internet durch die Nutzer praktisch stets durch

Suchmaschinen stattfindet, kommt den Suchergebnissen zu dem Namen einer Person – insbesondere unter Berücksichtigung von deren Profilbildung (vgl. EuGH, Urteil vom 13.05.2014, C-131/12, Rn. 37) – eine überragende Bedeutung zu. Die Suchmaschine der Google Inc. hat außerdem in den Jahren 2014 / 2015 in Deutschland einen Marktanteil von mehr als 90 Prozent.

In Deutschland ist der HmbBfDI für Google zuständig, denn die in Kalifornien ansässige Google Inc. unterhält in Europa u. a. mit der Google Germany GmbH ein Vertriebsbüro in Hamburg zur Förderung des Verkaufs der Werbeflächen der Suchmaschine, dessen Tätigkeit auf in Deutschland ansässige Kunden ausgerichtet ist, und der HmbBfDI kontrolliert als Aufsichtsbehörde über die nicht-öffentlichen Stellen in Hamburg gem. § 38 des Bundesdatenschutzgesetzes (BDSG) die Ausführung der Vorschriften über den Datenschutz im Bereich der Privatwirtschaft.

Bereits am 29. Mai 2014 hat die Google Inc. ein Online-Verfahren für die Bearbeitung von Ersuchen zur Löschung von Suchergebnissen nach europäischem Datenschutzrecht eingeführt. Unter der URL *https://support.google.com/legal/contact/lr_eudpa?product=websearch* können die Ersuchen gestellt werden. Es entspricht dem europäischen und deutschen Datenschutzrecht, dass zunächst die für die Datenverarbeitung verantwortliche Stelle prüft, ob ihre Tätigkeit datenschutzrechtlich zulässig ist.

Bis Anfang Dezember 2015 gab es in Deutschland 60.510 Ersuchen (Europa: 350.435) mit insgesamt 221.640 Suchergebnissen (Europa: 1.239.955), von denen 48,2% durch Google entfernt und 51,8% nicht entfernt wurden (Europa: 42,1% entfernt und 57,9% nicht entfernt). Der Google-Transparenzbericht ist unter der URL *https://www.google.com/transparencyreport/removals/europeprivacy/?hl=de* einsehbar.

Wir sind fortlaufend in Kontakt mit den europäischen Datenschutzbehörden und der Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten (Artikel 29-Datenschutzgruppe). Die Artikel 29-Datenschutzgruppe hat am 26. November 2014 Bearbeitungshinweise veröffentlicht, die unter der URL *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf* öffentlich zugänglich sind.

Ein „Experten-Beirat" der Google Inc., der von September bis November 2014 sieben Mal in verschiedenen europäischen Ländern tagte, holte Beiträge aus Politik, Wirtschaft, Medien, Wissenschaft, dem Technologiesektor, von Datenschutzverbänden und anderen Organisationen ein (*https://www.google.com/intl/de/advisorycouncil/*). Wir haben bei der Tagung in Berlin am 14. Oktober 2014 mitgewirkt. Am 6. Januar 2015 wurde ein Bericht veröffentlicht, der ebenfalls Bearbeitungshinweise enthält und unter der URL *https://drive.google.com/a/google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view?pli=1* abrufbar ist.

Die Prüfung, ob ein Suchergebnis zu dem Namen einer (lebenden, natürlichen) Person zu entfernen ist, ist eine jeweils im Einzelfall vorzunehmende Abwägung zwischen dem öffentlichen Informationsinteresse und dem Recht auf informationelle Selbstbestimmung des Betroffenen. Bei der Abwägung wird geprüft, ob eine Person wegen ihrer besonderen persönlichen Situation ein gegenüber dem einzubeziehenden öffentlichen Informationsinteresse und auch der zu berücksichtigenden Meinungsäußerungsfreiheit und der Pressefreiheit überwiegendes schutzwürdiges Interesse hat.

Insbesondere ist zu berücksichtigen, ob es sich um die Privat- oder Sozialsphäre, das Berufsleben, die Teilnahme am geschäftlichen Verkehr, an der Meinungsbildung oder am politischen Leben handelt, ob eine Person aktiv in die Öffentlichkeit getreten ist, in welchen Medien die Informationen zugänglich gemacht wurden, ob es sich um Themen von öffentlichem Interesse, Meinungsäußerungen oder – davon meist nicht zu trennenden – Tatsachenbehauptungen handelt, welche Rolle eine Person hat, ob es sich um eine Auseinandersetzung in der Sache handelt. Ferner sind der bisherige Zeitablauf seit Veröffentlichung der Informationen, die Relevanz der Informationen zum Zeitpunkt der Prüfung – bezogen auf die Person und / oder allgemein – die bisherige und aktuelle Lebenssituation und, ob auch Wertungen anderer gesetzlicher Regelungen berücksichtigt werden können, zu beachten.

Die unterschiedlichen Fallkonstellationen der Eingaben beim HmbBfDI betreffen häufig Gegenstände von Presse- bzw. Medienberichterstattung (lokal oder überregional), aber auch Berichte und Diskussionen auf Internetseiten, in Blogs und Foren, (bisherige) geschäftliche und freiberufliche Tätigkeiten, politische Aktivitäten, Meinungsäußerungen, den politischen Meinungskampf, strafrechtliche Sachverhalte bzw. Berichte darüber.

Wir sind zu der Bearbeitung der Fälle und der Vorgehensweise des Verfahrens regelmäßig in Kontakt mit der Google Inc. als verantwortlicher Stelle. In Fällen, in denen wir eine Entfernung von Suchergebnissen für möglich halten, wird die Google Inc. angehört, die nach erneuter Prüfung Suchergebnisse entfernt oder die Ablehnung einer Entfernung ausführlich in rechtlicher und tatsächlicher Hinsicht begründet. Wir haben die Google Inc. in diversen Fällen zur Entfernung von Suchergebnissen aufgefordert und angehört. Eine verwaltungsrechtliche Anordnung zur Entfernung von Suchergebnissen wurde bislang nicht erlassen. In diversen Fällen haben die Prüfungen auch ergeben, dass die Voraussetzungen zur Entfernung von Suchergebnissen nicht vorliegen. In Großbritannien hat die Datenschutzbehörde in einem Fall eine Anordnung erlassen, in der die Entfernung eines Suchergebnisses durch die Google Inc. abgelehnt wurde, der einen Pressebericht betrifft, in dem über die vorige Entfernung eines Suchergebnisses berichtet wurde und der Betroffene dadurch den zwischenzeitlich erreichten Schutz wieder verlor. Die französische Datenschutzbehörde hat die Google Inc. ihrerseits aufgefordert, auch Suchergebnisse aus außereuropäischen Domains der Google Suchmaschine zu entfernen, da ansonsten Suchergebnisse von Europa aus mit einer

Suche über außereuropäische Google-Domains gefunden werden könnten. Beide Verfahren sind rechtshängig.

Es ist wegen der bisherigen kontinuierlichen Vielzahl der Eingaben seit Juli 2014 davon auszugehen, dass die Prüfungen der von der Google Inc. abgelehnten Ersuchen zur Entfernung von Suchergebnissen eine dauerhafte, umfangreiche Aufgabe des HmbBfDI ist. In der Zeit von Mitte Juli 2014 bis Anfang Dezember 2015 haben wir 425 Eingaben mit 2.026 Suchergebnissen im Jahr 2014 und 1.301 Suchergebnissen im Jahr 2015 erhalten. Mitte Mai 2015 wurde festgestellt, dass der HmbBfDI im Vergleich der europäischen Datenschutzbehörden die meisten Eingaben erhalten hat.

Da in jedem Fall eine Einzelprüfung und Abwägungsentscheidung – oft für eine Vielzahl von Suchergebnissen – vorzunehmen ist und nur begrenzte personelle Kapazitäten zur Verfügung stehen, muss bei den Eingaben mit erheblichen Wartezeiten gerechnet werden. Dies ist bedauerlich, aber vom HmbBfDI nicht zu vertreten. Nur durch eine vorübergehend finanzierte zusätzliche Stelle ist die Bearbeitung der Eingaben überhaupt möglich. Das Beispiel der Google-Suchmaschine zeigt sehr deutlich, dass eine angemessene personelle Ausstattung der Datenschutzaufsicht die Voraussetzung für eine wirksame Kontrolle und den Schutz des informationellen Selbstbestimmungsrechts der Betroffenen ist.

1.2 Google Privatsphärebestimmungen

Das seit nunmehr drei Jahren laufende Prüfverfahren der europäischen Task-Force zur Datenschutzerklärung von Google und zur Bildung von Nutzungsprofilen zeigt erste Ergebnisse. Ein Schlussstrich unter das Verfahren auf nationaler Ebene kann allerdings noch nicht gezogen werden.

Im 24. Tätigkeitsbericht hatten wir angekündigt, die Datenverarbeitung durch Google gemeinsam mit den Aufsichtsbehörden der Länder Frankreich, Großbritannien, Italien, Niederlande und Spanien zu prüfen (24. TB V 6.1.). Unserer damals geäußerten Auffassung entsprechend konzentrierten wir uns im Verlauf des Verfahrens darauf, sicherzustellen, dass das dienstübergreifende Zusammenführen von Nutzungs- und Bestandsdaten unterbleibt oder auf eine rechtliche Grundlage gestellt wird. Mit der Zusammenführung werden umfassende und inhaltlich äußerst aussagekräftige Nutzungs- und Interessensprofile über Nutzerinnen und Nutzer durch Google erstellt. Hierfür bedarf es einer gesetzlichen Grundlage oder einer entsprechenden Einwilligung der Nutzerinnen und Nutzer. Denn Google räumt sich in der Datenschutzerklärung das Recht ein, die gesetzlich vorgeschriebene Trennung der bei der Nutzung von verschie-

denen Diensten entstehenden personenbezogenen Informationen zu überwinden und sämtliche Daten miteinander zu verschneiden. Dadurch ist Google in der Lage, detaillierte Profile der einzelnen Nutzerinnen und Nutzer zu erstellen, die Auskünfte über die Interessen, Vorlieben, Kommunikationsbeziehungen und das Nutzungsverhalten der Betroffenen geben.
In der von der Artikel-29-Datenschutzgruppe eingesetzten Task-Force erfolgt die Koordination der jeweiligen nationalen Aktivitäten der beteiligten Aufsichtsbehörden. Dabei entstand ein arbeitsteiliges Vorgehen zwischen den Aufsichtsbehörden. Inhaltliche Positionen werden gemeinsam auf europäischer Ebene abgestimmt und dann in den jeweiligen nationalen Verfahren umgesetzt. So adressieren die französische und spanische Aufsichtsbehörde schwerpunktmäßig das Thema Transparenz und die Formulierung der Datenschutzerklärung. Wir hingegen konzentrieren uns auf die Thematik der Rechtmäßigkeit der Profilbildung.

Im September 2014 erließen wir eine Verwaltungsanordnung gegen Google. In dieser wurde das in den USA ansässige Unternehmen verpflichtet, die Nutzungs-, Bestands- und Inhaltsdaten von angemeldeten und nicht angemeldeten Nutzerinnen und Nutzern nur in dem durch das Telemediengesetz und das Bundesdatenschutzgesetz zulässigen Umfang zu Profilen zusammenzuführen oder für über die gesetzlich vorgesehenen Möglichkeiten hinaus entsprechende Einwilligungen der Betroffenen einzuholen. Google erhob gegen diese Anordnung Widerspruch, den wir unter geringfügigen Änderungen des Ausgangsbescheides im April 2015 mit einem entsprechenden Widerspruchbescheid zurückwiesen. Dagegen erhob Google Anfechtungsklage vor dem Verwaltungsgericht Hamburg. Es ist bisher nicht abzusehen, wann das Gericht sich mit der Klage inhaltlich befassen wird. Denn bislang fehlt die Klagebegründung des Unternehmens.

Parallel zu den verwaltungsrechtlichen und -gerichtlichen Verfahren hat Google auf die datenschutzrechtlichen Bedenken der Aufsichtsbehörden reagiert und bereits mit der Umsetzung verschiedener Maßnahmen begonnen. Dazu gehört zum einen die Überarbeitung der Datenschutzerklärung. Aufgrund der technischen Komplexität der Verarbeitung von Daten durch Google musste eine Lösung gefunden werden, mittels derer die Betroffenen inhaltlich vollständig und umfassend informiert werden, deren textlicher Umfang andererseits in einem verträglichen Rahmen und aus Nutzersicht handhabbar bleibt. Die Task-Force hat sich mit Google auf ein sogenanntes Schichtmodell (Layered Approach) geeinigt. Auf der ersten „Schicht" befindet sich der übliche, jedoch etwas komprimierte Text der Datenschutzerklärung, der die Nutzer im Allgemeinen über Umfang und Zweck der Erhebung personenbezogener Daten in einer klaren und verständlichen Sprache informiert. Einzelne, vor allem technische und weniger bekannte Begriffe, sind zudem im Text markiert und entsprechende weiterführende Informationen und Erläuterungen können auf der zweiten Schicht mit einer Mausbewegung als Texteinblendungen „aktiviert" werden. Die dritte „Schicht" besteht aus weiterführenden Links zu detaillierteren Erläuterungen einzelner Themen.

Im Hinblick auf die Erstellung von Profilen der Nutzerinnen und Nutzer verlangt Google seit Oktober 2015 von allen angemeldeten und nicht angemeldeten Nutzerinnen und Nutzern eine Einwilligung in die Verarbeitung der Daten, insbesondere für die dienstübergreifende Zusammenführung der Daten aus den verschiedenen Diensten. Dabei informiert Google zudem über verschiedene, teilweise neu geschaffene Einstellmöglichkeiten, mit denen Nutzerinnen und Nutzer auf den Umfang der Datenverarbeitung einwirken können (z.B. die Speicherung bzw. Löschung der Historie der Suchanfragen oder angesehener Videos bei Youtube).

Solche Kontrollmöglichkeiten haben wir von Anbeginn als entscheidende Voraussetzung dafür bewertet, dass eine rechtswirksame Einwilligung überhaupt erteilt werden kann. Denn dadurch wird eine Situation vermieden, die den Nutzerinnnen und Nutzern nur die Wahl zwischen der Meidung von Google-Diensten oder deren Nutzung unter Akzeptanz einer weitreichenden Profilbildung lässt. Ob die von Google derzeit implementierte Lösung unsere Anordnung rechtswirksam umsetzt, kann erst entschieden werden, wenn alle darin enthaltenen Pflichten durch Google erfüllt wurden. Dazu zählt auch eine geeignete Dokumentation der technischen Implementation der Einwilligungslösung und der zugehörigen Einstellmöglichkeiten. Erst mit dieser wird der HmbBfDI in der Lage sein, die Übereinstimmung des durch Google gewählten Verfahrens mit der Anordnung abschließend prüfen zu können.

1.3 Google Apps in der Cloud

Google bietet seine ansonsten kostenlosen Dienste auch gewerblichen, kommerziellen und anderen nichtprivaten Anwendern als Office-Lösung an. Unternehmen und andere Organisationen müssen dabei einige datenschutzrechtliche Vorgaben beachten.

Mit „Google Apps for Work" bietet Google Unternehmen und anderen Organisationen Teile seiner Dienste als Cloud-Lösung zum professionellen Einsatz an. Wir werden immer wieder zur datenschutzrechtlichen Zulässigkeit dieses Angebots gefragt. Eine abschließende Antwort darauf zu geben, fällt auch wegen der neueren Rechtsprechung des EuGH zum internationalen Datenverkehr (siehe X 1) nicht leicht.

Die Office-Anwendungen von Google lassen sich als Software-as-a-Service bezeichnen, für deren Verwendung lediglich eine Internetverbindung und ein Browser benötigt werden. Diese minimalen technischen Voraussetzungen und umfangreiche Funktionalitäten, wie z.B. kollaboratives Arbeiten machen es für Unternehmen offenbar attraktiv, diese Dienste zu betrieblichen Zwecken einzusetzen.

Bei der Verwendung dieser Dienste verarbeiten die jeweils verantwortlichen Stellen ggfs. nicht nur personenbezogene Daten zur Erfüllung des eigenen Geschäftszwecks

(z.B. Kundenmanagement). Auch die Nutzungs- und Bestandsdaten der Beschäftigten werden dann im Rahmen einer entsprechenden Auftragsdatenverarbeitung technisch durch Google verarbeitet.

Ausgangspunkt ist die datenschutzrechtliche Feststellung, dass Google als Auftragsdatenverarbeiter i.S.d. §§ 3 Abs. 7, 11 BDSG für die jeweilige Stelle tätig wird. Mit anderen Worten, das Unternehmen, welches Google Apps professionell einsetzt, ist gegenüber den eigenen Beschäftigten und sonstigen Betroffenen datenschutzrechtlich auch für den Umgang mit diesen Daten durch Google verantwortlich.

Problematisch in dieser Konstellation sind zwei Themen. Einerseits existiert die datenschutzrechtliche Privilegierung der Auftragsdatenverarbeitung bei Auftragnehmern mit Sitz außerhalb der Europäischen Union nicht. Denn § 3 Abs. 7 BDSG definiert als Auftragnehmer ausschließlich Stellen mit Sitz innerhalb der Europäischen Union. Das wiederum führt dazu, dass Anwender von Google Apps for Work in einem ersten Schritt eine Rechtsgrundlage für die damit rechtlich als Übermittlung einzustufende Weitergabe der Daten an Google vorweisen müssen. Im Einzelfall ist zu prüfen, ob hier auf die allgemeinen Aussagen für den internationalen Datenverkehr zurückgegriffen werden kann.

In einem zweiten, letztlich entscheidenderen Schritt muss der Verwender dieser Dienstleistungen gemäß §§ 4 b und c BDSG sicherstellen, dass Google bei dem Umgang mit den Daten ein angemessenes Datenschutzniveau gewährleistet. Dazu bietet Google einen Vertrag auf Grundlage der sogenannten Standardvertragsklauseln an, der durch die Verwender abzuschließen ist. Ob allerdings diese Lösung nach dem Urteil des EuGH zum „Safe-Harbor-Abkommen" Bestand haben kann, ist fraglich und wird derzeit durch die europäischen und nationalen Aufsichtsbehörden geprüft (vgl. X 1).

Neben der kommerziellen Lösung für Unternehmen existiert auch das Angebot „Google Apps for Education", das sich in Deutschland an Gymnasien oder höhere Bildungseinrichtungen richtet und von diesen konstenfrei genutzt werden kann. Die vorstehend genannten Aspekte sind hier in besonderem Maße zu beachten, nicht zuletzt vor dem Hintergrund, dass im schulischen Kontext häufig auch besondere Arten personenbezogener Daten verarbeitet werden. Zudem sind für öffentliche Schulen bzw. Hochschulen die jeweiligen Landesdatenschutzgesetze und bereichsspezifisches Datenschutzrecht einschlägig.

2. Facebook

Die Prüfung der Datenverarbeitung des sozialen Netzwerks Facebook und die Bearbeitung von individuellen Nutzerbeschwerden beanspruchten, wie in den vergangenen Berichtszeiträumen auch, erhebliche personelle Ressourcen des dafür zuständigen Referates. Die Prüfung Facebooks wird vor allem dadurch erschwert, dass Facebook die Zuständigkeit unserer Dienstelle nicht akzeptiert und die Beachtung deutschen Datenschutzrechts ablehnt.

2.1 Neue Datenrichtlinie von Facebook und anwendbares Recht

Ende 2014 informierte uns das Unternehmen, dass es die bis dahin geltenden „Datenverwendungsrichtlinien" durch eine neue Datenrichtlinie zu Beginn des Jahres 2015 ändern wolle. Bei einer ersten inhaltlichen Prüfung stellten wir fest, dass sich das Unternehmen vor allem bezüglich der Übermittlung von Daten der Nutzerinnen und Nutzer weitreichende Befugnisse einräumte. An der datenschutzrechtlichen Zulässigkeit dieses Vorgehens haben wir, gemeinsam mit anderen europäischen Aufsichtsbehörden, erhebliche Zweifel.

Daher baten wir Facebook, das Inkrafttreten der Nutzungsbedingungen zu verschieben und das Ergebnis der von uns und anderen europäischen Aufsichtsbehörden eingeleiteten aufsichtsbehördlichen Prüfung abzuwarten. Facebook lehnte dies ab und berief sich auf entsprechende Gespräche mit der irischen Aufsichtsbehörde. Letztere hatte die Änderungen als unbedenklich bewertet.

Dennoch eröffneten wir im Frühjahr 2015 ein aufsichtsbehördliches Prüfverfahren gegen die irische und deutsche Tochter der Facebook Inc. Die an die Facebook Ireland Ltd. versandte Aufforderung zur Stellungnahme wurde erst nach einer mehrmonatigen Diskussion zwischen uns, der irischen Aufsichtsbehörde und Facebook Ireland Ltd. gegenüber den irischen Kollegen beantwortet und uns dann von dieser zugesandt. Der Grund dieses Vorgehens liegt im Standpunkt des Unternehmens, dass die Facebook Ireland Ltd. zum einen die allein für die Verarbeitung personenbezogener Daten deutscher Nutzerinnen und Nutzer datenschutzrechtlich verantwortliche Stelle sei und zum anderen die Facebook Germany GmbH lediglich als Auftragsdatenverarbeiterin sowie als Vertriebs- und Marketingstelle für die Facebook Ireland Ltd. auf dem deutschen Markt tätig werde. Daraus leitet das Unternehmen ab, dass ausschließlich irisches Datenschutzrecht auf die Verarbeitung der Daten deutscher Nutzerinnen und Nutzer Anwendung fände und die Einhaltung dieser Vorgaben nur durch die irische Aufsichtsbehörde kontrolliert werden dürfe. Das Unternehmen beruft sich dabei u.a. auf die Rechtsprechung schleswig-holsteinischer Verwaltungsgerichte.

Wir hingegen vertreten, gestützt auf die aktuellere Rechtsprechung des EuGH zu Google aus dem Jahr 2014 (C-131/12 Google Spain) und aus dem Jahr 2015 (C-230/14 Weltimmo), die Auffassung, dass für Facebook und dessen Niederlassungen in den einzelnen EU-Mitgliedstaaten das Marktortprinzip Anwendung findet. Facebook ist danach verpflichtet, das nationale Datenschutzrecht der Staaten anzuwenden, in denen Niederlassungen des Unternehmens ihren Sitz haben – jedenfalls dann, wenn die Niederlassung im jeweiligen nationalen Markt für den Konzern wirtschaftlich aktiv wird und zur Erfüllung eigener Geschäftszwecke der verantwortlichen Stelle personenbezogene Daten der in diesem Mitgliedsstaat lebenden Menschen erhebt, verarbeitet oder nutzt. Ein belgisches Gericht hat im November 2015 die Zuständigkeit der belgischen Datenschutzaufsicht bereits unter Bezugnahme auf die Public-Relations-Tätigkeiten der Facebook-Niederlassung in Brüssel erklärt.

Die Facebook Germany GmbH erwirtschaftet Werbeinnahmen auf dem deutschen Markt und ist über diese Tätigkeit an dem wirtschaftlichen Erfolg des sozialen Netzwerks beteiligt. Das deutsche Datenschutzrecht findet daher Anwendung.

Trotz der Nichtanerkennung der Zuständigkeit der prüfenden Aufsichtsbehörden in Belgien, Deutschland, Frankreich, Niederlande und Spanien legte Facebook dar, dass die Datenrichtlinie verständlicher gestaltet und formuliert werden sollte. Wir begrüßen dieses Ziel ausdrücklich und haben positiv zur Kenntnis genommen, dass die Datenrichtlinie nunmehr intuitiver genutzt werden kann und leichter zu verstehen ist.

Das Unternehmen hat im gleichen Zug erklärt, den Umfang der zu Werbezwecken verwendeten Daten auszudehnen. Dies gilt vor allem für Informationen über die von Betroffenen genutzten Websites und Apps. Allerdings können diese sogenannten „interessenbasierte Online-Werbeanzeigen" durch die Nutzer deaktiviert werden, was jedoch nicht die Auslieferung von Werbung unterbindet, sondern nur verhindert, dass das Nutzerverhalten zur Grundlage für die Auslieferung der Werbung gemacht wird.
Zudem strebt Facebook über den Dienst „Place Tips" an, Informationen über die von den Nutzern besuchten Orte zu erheben. Facebook bietet dafür unter anderem eigene „Beacons" an, auf Bluetooth basierende Sender, die eine Kommunikation mit der Facebook-App auf dem Smartphone herstellen.

Aus Datenschutzsicht ambivalent ist außerdem die durch Facebook eingeführte „Ad Preference" oder im Deutschen bezeichnete „Einstellungen für Werbeanzeigen" – Funktion. Mit dieser können Nutzerinnen und Nutzer ihre bisherigen durch Facebook generierten Präferenzen erkennen und steuern und dadurch inhaltlich auf die Auslieferung von Werbung Einfluss nehmen. Während dies einerseits ein Element der Steuerung des eigenen Profils ist, verbessert sich andererseits dadurch auch der Aussagegehalt über die Vorlieben und Neigungen der jeweiligen Nutzerin oder des jeweiligen Nutzers. Es liegt damit in der Entscheidung eines jeden selbst, in welchem Umfang diese Funktion zum Einsatz kommen soll.

Die Datenrichtlinie prüfen wir gemeinsam mit den Aufsichtsbehörden aus Frankreich, Spanien, Belgien und den Niederlanden im Rahmen einer auf europäischer Ebene koordinierten „Contact Group". In dieser Kontaktgruppe koordinieren wir unsere jeweiligen nationalen aufsichtsbehördlichen Prüfungen und besprechen die strategischen Vorgehensweisen.

2.2. Pseudonyme Nutzung

Neben den bereits beschriebenen prinzipiellen Themen bezüglich der Beachtung datenschutzrechtlicher Vorgaben bei der Verarbeitung personenbezogener Daten durch Facebook hatten wir uns im Berichtszeitraum unter anderem mit zahlreichen Eingaben zur sogenannten „Klarnamenpflicht" des Netzwerkbetreibers zu beschäftigen. In Ziffer 4 der facebookeigenen „Erklärung der Rechte und Pflichten" wird dies wie folgt formuliert:

„Facebook-Nutzer geben ihre wahren Namen und Daten an, und wir benötigen deine Hilfe, damit dies so bleibt." Das Unternehmen setzt diese Regel zwar nicht flächendeckend und systematisch, jedoch in Einzelfällen rigoros durch. Zu den nicht geduldeten „Fake-Accounts" zählen Profile, bei denen die Nutzerinnen und Nutzer Pseudonyme also u.a. Fanatsie- oder Spitznamen, Verkürzungen, Abkürzungen oder Modifikationen des eigenen Namens verwenden. Facebook sperrt Nutzerinnen und Nutzer, die mit derartigen Profilen aufgefallen sind und fordert sie auf, ihre „wahre" Identität nachzuweisen oder zu belegen, dass der auf Facebook verwendete Name ein im täglichen Leben regelmäßig genutzter und anerkannter Name ist. Sind die Betroffenen dazu nicht in der Lage, was in den bei uns eingegangen Beschwerden die Regel ist, lässt Facebook zwei Handlungsoptionen zu. Entweder die Nutzerin oder der Nutzer verwenden das Profil unter ihrem amtlichen Namen oder das Profil wird durch Facebook entfernt.

Zur Feststellung der Identität der Nutzerinnen und Nutzer bietet Facebook im Wesentlichen zwei Möglichkeiten. Entweder die Betroffenen senden Bildscans von zwei nicht-amtlichen Ausweisen oder Belegen ein, die auf den gleichen Namen lauten und von denen eines ein Bild der betroffenen Person enthält. Oder die Nutzerinnen und Nutzer werden aufgefordert, eine digitale Kopie ihres amtlichen Ausweises, namentlich Personalausweises oder Passes, an Facebook zu übermitteln. Nicht erforderliche Angaben dürfen dabei geschwärzt werden.
Wir sehen im Klarnamenprinzip einen Verstoß gegen das Telemediengesetz und in der Speicherung der digitalen Kopien des Personalausweises oder Passes einen Verstoß gegen das Personalausweisgesetz bzw. Passgesetz. Das Telemediengesetz enthält die Verpflichtung von Internetdienstanbietern, die Nutzung dieser Dienste anonym oder pseudonym zuzulassen, soweit dies technisch realisierbar und dem Anbieter zumutbar ist, § 13 Abs. TMG. Das Personalausweisgesetz und im Wesentlichen gleichlautend das Passgesetz untersagen die Speicherung digitaler Ausweis- und Passkopien, § 20 Abs. 2 PAuswG; § 18 Abs. 3 PaßG.

Unsere Rechtsauffassung haben wir in der Vergangenheit immer wieder dem Unternehmen mitgeteilt und es aufgefordert, die pseudonyme Nutzung zuzulassen und auf Identitätsprüfungen unter Verwendung digitaler Kopien des amtlichen Personalausweises oder Passes zu verzichten. Facebook wurde mehrfach und wiederholt mitgeteilt, dass die Klarnamenpflicht gegen deutsches Datenschutzrecht verstößt und die Speicherung der Ausweiskopien unzulässig ist. Das Unternehmen beharrte jedes Mal auf dem beschriebenen Klarnamenprinzip und beschränkte sich darauf, amtliche Identifikationsdokumente lediglich als letztes Mittel der Identitätsprüfung einzusetzen.

Im Juni 2015 erhielten wir erneut eine Eingabe einer Nutzerin, deren Profil durch Facebook wegen des Verstoßes gegen das Klarnamenprinzip gesperrt wurde. Die Nutzerin hatte als Profilnamen nicht ihren richtigen Namen verwendet, sondern das Netzwerk unter einem aus Teilen ihres Namens zusammengesetzten Pseudonyms lange Zeit aktiv und umfassend zu privaten Zwecken genutzt. Durch die Verwendung des Pseudonyms wollte sie u.a. verhindern, dass sie nicht unter ihrem bekannten Namen auf Facebook von Dritten in beruflichen Angelegenheiten kontaktiert wird.

Facebook hatte sie nach einer entsprechenden Beschwerde im Frühjahr 2015 aufgefordert, ihre Identität nachzuweisen. Entsprechend der facebookeigenen Vorgaben übersandte die Nutzerin ein Lichtbilddokument und weitere Unterlagen, die ihre Identität bestätigten. Nach Ansicht von Facebook waren diese Angaben allerdings unzureichend. Der Kundensupport des Unternehmens forderte von der Petentin die Übersendung einer digitalen Ausweis- oder Passkopie. Außerdem änderte Facebook den Namen des Profils in ihren amtlichen Namen und forderte sie auf, entweder der Änderung zuzustimmen oder das Profil entfernen zu lassen. Dies wollte die Petentin nicht bzw. sah sich in ihren Rechten verletzt und wandte sich mit einer Beschwerde an uns.

Wir haben daraufhin gegen Facebook ein Verwaltungsverfahren eröffnet und bereits im Juli 2015 eine Verwaltungsanordnung erlassen. In dieser wird das Unternehmen verpflichtet, der Petentin die Nutzung ihres Profils unter ihrem selbstgewählten Namen zuzulassen. Wir haben zudem die sofortige Vollziehung dieses Anordnungspunktes angeordnet. Der zweite Anordnungspunkt betrifft die Untersagung der Speicherung von Ausweis- und Passkopien zur Durchsetzung des Klarnamenprinzips durch Facebook.

Wir sind der Auffassung, dass es Facebook zuzumuten ist, dass die Petentin selbst entscheiden darf, ob sie in dem Netzwerk gegenüber anderen Nutzerinnen und Nutzern unter Pseudonym auftritt. Zum einen ist es, wie jede Nutzerin und jeder Nutzer weiß, Realität, dass Pseudonyme bei Facebook in großem Umfang verwendet werden. Dem wirtschaftlichen Erfolg des Netzwerks würde es gewiss nicht schaden, das Profil der Petentin unter dem gewünschten Pseudonym wieder zugänglich zu machen.

Auch den von Facebook behaupteten Effekt der Disziplinierung des Kommunikati-

onsverhaltens der Nutzerin auf dem Netzwerk können wir nicht nachvollziehen. Die Petentin ist zudem in keiner Weise durch ein störendes oder kriminelles Verhalten bei Facebook aufgefallen – was nach Aussage des Unternehmens durch die Klarnamenpflicht bekämpft werden soll. Der Versuch des Unternehmens, ihr gegenüber das Klarnamenprinzip zwangsweise durchzusetzen, beschränkt sie in ihrem verfassungsrechtlich gewährleisteten und im Telemediengesetz konkretisierten Anspruch, selbst darüber zu entscheiden, wie und unter welchem Namen sie im Internet aktiv ist.

Die Anordnung der sofortigen Vollziehung des Bescheides sollte der zügigen Herstellung von Rechtssicherheit vor allem im Interesse der Petentin dienen. Sie hat vor der Sperrung einen relevanten Teil ihrer privaten und familiären Kommunikation über dieses Netzwerk abgewickelt. Daher war es auch in ihrem Interesse, zumindest eine vorläufige Entscheidung über die weitere Nutzung herzustellen.

Gegen unsere Anordnung hat Facebook die entsprechenden Rechtsmittel vor dem Verwaltungsgericht eingelegt. Die gerichtliche Entscheidung in dieser Sache stand bis Redaktionsschluss des Tätigkeitsberichtes aus.

Auch gegen den zweiten Teil der Anordnung, der Untersagung der Speicherung digitaler Kopien des Personalausweises oder Passes hat Facebook Widerspruch eingelegt. Zwar verweist Facebook auf die alternativen Identifikationsmöglichkeiten und den Umstand, dass auch in anderen Fällen Aufsichtsbehörden das Erstellen und Speichern von Ausweiskopien zugelassen hätten. Dabei handelte es sich z.B. um die Übersendung von Kopien an Auskunfteien zur Prüfung der Identität bei datenschutzrechtlichen Auskunftsansprüchen. Wir haben einerseits darauf hingewiesen, dass es sich bei den von den Aufsichtsbehörden zugelassenen Fällen der Speicherung von Kopien entweder um die Wahrung der eigenen Interessen der Betroffenen handelt oder die Speicherung durch Gesetz legitimiert ist. Nach unserer Auffassung kann die Durchsetzung des Verstoßes gegen das Recht auf pseudonyme Nutzung nicht als Rechtfertigung für den Verstoß gegen das Speicherverbot digitaler Ausweiskopien herangezogen werden. Die von Facebook vorgenommene „Identitätsprüfung" dient einem dem Telemediengesetz widersprechenden Zweck. Sie kann somit auch nicht die Speicherung von amtlichen Ausweisdokumenten legitimieren.

2.3. WhatsApp

Immer wieder erreichen uns auch Eingaben zum Kurzmitteilungsdienst WhatsApp. Auch wenn das Unternehmen mit Sitz in den USA wirtschaftlich zum Facebook-Konzern gehört und wir sporadischen Kontakt zu dem Unternehmen hatten, sind wir für die Kontrolle der Einhaltung datenschutzrechtlicher Vorgaben durch dieses Unternehmen nicht zuständig. Bei WhatsApp handelt es sich im Schwerpunkt um einen Telekommunikationsdienst. Die Kontrolle der Einhaltung des Telekommunikationsdatenschutzes obliegt der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit mit

Sitz in Bonn. Entsprechende Eingaben und Anfragen sind an die dortige Dienststelle zu richten bzw. werden von uns dorthin abgegeben.

Wir werden jedoch die Übermittlung von Daten zwischen den Unternehmen Facebook und WhatsApp beobachten und bei unzulässigen Datentransfers entsprechende aufsichtsbehördliche Maßnahmen gegenüber Facebook ergreifen.

3. XING

Mit der Xing AG haben wir im Berichtszeitraum zahlreiche Gespräche über die Verbesserung des Datenschutzes und der Datensicherheit geführt. Häufig gaben Hinweise aus dem erfreulich datenschutzsensiblen Nutzerkreis des Dienstes den Anlass dafür.

3.1 TLS Verschlüsselung

Ein Nutzer des sozialen Netzwerkes XING machte uns darauf aufmerksam, dass das Unternehmen E-Mails an Mitglieder ohne eine TLS-Transportverschlüsselung versendet, obwohl die Gegenstelle dies unterstützt. Dies betraf sowohl Werbemails als auch individuelle Nachrichten zwischen den Mitgliedern. Zum Nachweis wurden uns entsprechende technische Dokumentationen vorgelegt.

Unserer Ansicht nach stellt die fehlende Verschlüsselung eine unzureichende Beachtung technischer und organisatorischer Maßnahmen gemäß § 9 BDSG i.V.m. Anlage zum BDSG dar. Daher haben wir die XING AG zur Stellungnahme aufgefordert.

Diese bestätigte, dass E-Mails teilweise ohne Verwendung von TLS versendet wurden. Allerdings war dies nicht flächendeckend der Fall. Nach Darstellung des Unternehmens hätten einige Mailprovider den Standard TLS nicht oder fehlerhaft implementiert. In diesen Fällen konnten die Nachrichten nicht erfolgreich transportverschlüsselt versendet werden. Um dies zu vermeiden, arbeitet XING mit einer Whitelist, in die alle Mailprovider aufgenommen wurden, die TLS korrekt implementiert hatten. Dazu zählen z.B. die der Initiative „E-Mail made in Germany" beigetretenen Anbieter. Nutzerinnen und Nutzer mit Postfächern bei derartigen Providern erhielten Nachrichten unter der Verwendung von TLS zugesandt. Nach Darstellung von XING hätte es einen zu großen Aufwand bedeutet, für sämtliche Nutzer individuell zu prüfen, ob deren Provider eine korrekte TLS-Implementierung durchgeführt haben. Daher kam es dazu, dass trotz der technischen Fähigkeit zum verschlüsselten Versand bzw. Empfang bei einigen kleineren Anbietern TLS nicht eingesetzt wurde. Aufgrund der Zusage des Unternehmens, die Whitelist regelmäßig zu aktualisieren und damit sukzessive die Anzahl verschlüsselter Nachrichten zu erhöhen, haben wir von der Ergreifung weiterer aufsichtsbehördlicher Maßnahmen zunächst abgesehen.

3.2 Onlinestatus

Durch die Eingabe einer Nutzerin wurden wir auf eine datenschutzrechtlich zweifelhafte Funktion zur Anbahnung weiterer Nutzerkontakte in dem Netzwerk hingewiesen. Nutzerinnen und Nutzer mit einem Premiumkonto konnten unter der Funktion „Weitere interessante Mitglieder, die gerade erst bei XING eingeloggt waren" sehen, welche Nutzerin oder Nutzer sich ganz aktuell eingeloggt hatte und diese dann kontaktieren.
Wir sahen darin einen Verstoß gegen die Pflicht von XING, gemäß § 7 Abs. 2 Satz 3 TMG das Fernmeldegeheimnis i.S.d. § 88 TKG bezüglich der anfallenden Nutzungsdaten zu wahren. Denn für die Veröffentlichung des Login-Status existiert keine Rechtsgrundlage.
Der Login-Status ist ein Nutzungsdatum gemäß § 15 Abs. 1 TMG. Dessen Verwendung unterliegt einer strengen Zweckbindung. Für die Erbringung des Dienstes durch XING ist diese Mitteilung nicht erforderlich. Auch die Erwähnung der entsprechenden Funktion in den AGB des Dienstanbieters konnte nicht zur Bejahung der Erforderlichkeit i.S.d. Nutzungsverhältnisses führen. Denn § 15 Abs. 1 TMG ist eng auszulegen und orientiert sich an dem konkreten Erfordernis zur (technischen) Erbringung des Dienstes. Andere gesetzliche Ermächtigungsgrundlagen waren nicht ersichtlich.

Eine explizite, den Anforderungen des § 4a BDSG bzw. § 13 Abs. 2 TMG entsprechende Einwilligung der Nutzerinnen und Nutzer lag zudem nicht vor, und ein Verweis in den AGB reicht bereits aus formalen Gründen nicht als Einwilligung aus. Die Klausel war nicht hervorgehoben und als Einwilligungserklärung nicht eindeutig zu erkennen.

Aufgrund unseres rechtlichen Hinweises entschied sich XING, die Funktion zu deaktivieren und zukünftig auf die Offenlegung des Onlinestatus gegenüber Premium-Nutzerinnen und -Nutzern zu verzichten.

4. Orientierungshilfe Apps

Für Entwickler und Anbieter von Apps wurde 2014 mit der „Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter" ein gemeinsam abgestimmtes Dokument der deutschen Datenschutzbehörden veröffentlicht.

Apps für Smartphones, Tablets, Smart-TVs oder neuerdings Smart-Watches erfreuen sich bei Nutzerinnen und Nutzern großer Beliebtheit. Obwohl mittlerweile bekannt ist, dass viele Apps „Nebenwirkungen" oder Schadfunktionen haben, werden sie in großer Zahl und ohne kritisches Hinterfragen von Zugriffsberechtigungen auf allen möglichen Geräten installiert. Meist verbleiben sie auch bei Nichtnutzung dort. Dies macht Apps zu interessanten Werkzeugen für Datensammler aller Art. Die Spanne der in Apps verborgenen Funktionen reicht von Werbenetzwerken, die das Nutzungsverhal-

ten erfassen, bis hin zu umfassenden Zugriffen auf nahezu alle Arten von Daten oder Dateien, die auf dem Gerät oder der Speicherkarte gespeichert sind, z.B. Kontakte, SMS-/MMS-Nachrichten, Fotos, Videos, Sprach-Memos usw. Im Extremfall können Apps auch wirtschaftlichen Schaden erzeugen, indem sie heimlich SMS-Nachrichten oder Anrufe zu teuren Sonderrufnummern tätigen. Oder es findet eine umfassende Überwachung der Nutzerin bzw. des Nutzers statt, mit Mitschneiden aller Tastatureingaben, permanenter Übermittlung der Standortdaten oder optischer und akustischer Bespitzelung über die eingebauten Kameras und Mikrofone (von beidem haben Smartphones mittlerweile meist zwei).

Auch die deutschen Datenschutzbehörden haben die App-Thematik aufgegriffen und die eigenen Kompetenzen gestärkt, z.B. durch Aufrüstung der Technikreferate und Prüflabore. Ein weiteres Ergebnis der Befassung ist die gemeinsam abgestimmte Handreichung „Orientierungshilfe Apps". Diese richtet sich an Entwickler und Anbieter von Apps vor allem im nicht-öffentlichen Bereich, d.h. Unternehmen und kommerzielle Organisationen. Sie zeigt datenschutzrechtliche und technische Anforderungen auf und macht diese anhand plakativer Beispiele verständlich. So bestehen an Apps, sofern diese personenbezogene Daten erfassen, verarbeiten oder speichern, nicht nur Anforderungen aus dem Bundesdatenschutzgesetz (z.B. Anwendung geeigneter Schutzmaßnahmen wie Verschlüsselung), sondern auch aus dem Telemediengesetz. Beispielsweise die Pflicht zur Hinterlegung von Informationen über den Anbieter innerhalb der App. Die „Orientierungshilfe Apps" kann hier heruntergeladen werden: *https://www.datenschutz-hamburg.de/uploads/media/Orientierungshilfe_Datenschutzanforderungen_an_App-Entwickler_und_App-Anbieter.pdf*

5. Orientierungshilfe Cloud Computing

Die Stellungnahme der Datenschutzbeauftragten zur Verarbeitung personenbezogener Daten in der Cloud wurde überarbeitet. Die in der Orientierungshilfe zum Ausdruck gebrachten Vorbehalte gegenüber Safe Harbor sind mittlerweile durch Aufhebung dieser Entscheidung durch den EuGH bestätigt worden.

Das Thema Cloud Computing haben wir bereits im letzten Tätigkeitsbericht angesprochen (24. TB VI. 2.2), und die Verarbeitung in der Cloud spielt auch bei Verfahren der öffentlichen Verwaltung vermehrt eine Rolle (z.B. VI. 1.5). Die in der aktuellen Orientierungshilfe Cloud Computing (abrufbar unter *https://www.datenschutz-hamburg.de/uploads/media/Orientierungshilfe_Cloud_Computing.pdf*) dargestellten Grundlagen, datenschutzrechtlichen und technischen sowie organisatorischen Aspekte bieten wichtige Hinweise für die Planung und die Bewertung von cloud-basierten Lösungen.

Besondere Aufmerksamkeit ist bei solchen Cloud-Lösungen geboten, die mit grenzüberschreitendem Datenverkehr in den außereuropäischen Raum verbunden sind. Viele Anbieter mit Hauptsitz in den USA haben bereits seit langem Cloud-Lösungen im Angebot und sind am Markt daher besonders präsent. Allerdings ist eines der wesentlichen Instrumente für die Begründung entsprechender Auftragsverhältnisse, die Safe-Harbor-Entscheidung der EU-Kommission, mittlerweile durch den europäischen Gerichtshof aufgehoben worden (siehe X. 1.). Ob andere Instrumente wie Standardvertragsklauseln bei US-Anbietern Bestand haben, wird im Kreis der nationalen und europäischen Datenschutzbehörden zurzeit noch intensiv diskutiert.

Die Initiativen einiger amerikanischer Unternehmen, gesonderte europäische oder sogar deutsche Cloud-Dienste zur Verfügung zu stellen, kann daher ein wichtiger Schritt sein, um die bestehenden rechtlichen Hürden zu überwinden.

6. Stellungnahme zu einer Verfassungsbeschwerde über Pressearchive

Unsere Dienststelle ist vom Bundesverfassungsgericht zur Stellungnahme zu einer Verfassungsbeschwerde über die Verarbeitung personenbezogener Daten in Pressearchiven aufgefordert worden. Dem sind wir gerne nachgekommen.

In der Rechtssache 1 BvR 16/13 hat sich das Bundesverfassungsgericht Ende 2013 mit der Bitte an die deutschen Datenschutzbehörden gewandt, Stellung zu einer Beschwerde im Zusammenhang mit dem Recht auf Vergessen zu nehmen. Hintergrund ist ein Strafprozess, der 1982 mit der rechtskräftigen Verurteilung wegen Mordes endete. In der damaliger Berichterstattung in einem Nachrichtenmagazin wurde der Name des Verurteilten vollständig genannt. Die entsprechenden Artikel waren damals lediglich in gedruckten Ausgaben erschienen, sind mittlerweile jedoch auch in digitalisierter Form im Archiv der Zeitschrift abrufbar. Dabei kann nach dem Namen des Betroffenen gesucht werden. Auch Suchmaschinen verweisen nach Eingabe des Namens auf diese Archivstellen.

Hiergegen hatte sich der damals Verurteilte nach über zehn Jahren nach Verbüßung seiner Strafe gewandt und die Entfernung seines (vollständigen) Namens aus den archivierten Artikeln des Nachrichtenmagazins gefordert. Während unterinstanzliche Gerichte den Unterlassungsanspruch des Betroffenenen anerkannten, wurden diese Entscheidungen durch Urteil des Bundesgerichtshofs im November 2012 (VI ZR 330/11) aufgehoben. Hierauf legte der Betroffene Verfassungsbeschwerde ein.

Die angeforderte Stellungnahme sollte sich insbesondere zu den Fragen äußern, inwieweit und auf welchen Wegen es Internetportalen wie einem Zeitschriften-Archiv

möglich ist, Einfluss auf die von Suchmaschinen aufgefundenen und ausgeworfenen Ergebnisse zu nehmen, und auf welche Weise und mit welchem Aufwand nachträglich die Erreichbarkeit personenbezogener Daten erschwert oder – im online-Zugriff – verhindert werden kann.

Da eine entsprechende Aufforderung auch an andere Datenschutzbeauftragte ging, haben wir angeboten, eine koordinierte Stellungnahme zu verfassen. Dieser sind elf andere Datenschutzbehörden vollständig und ein weiterer überwiegend beigetreten.

Wir haben dabei grundsätzlich für ein „Recht auf Vergessenwerden" plädiert, das jedenfalls in der Ausprägung eines „Rechts, nicht (einfach) gefunden zu werden" zu einem Ausgleich von kollidierenden Grundrechtspositionen – Persönlichkeitsrecht und Pressefreiheit – führen kann. Hierfür haben die Internetanbieter eigene Handlungsspielräume, die von der Suchmaschinensteuerung bis hin zu einer nachträglichen Anonymisierung archivierter Artikel reichen.

Das mittlerweile ergangene Urteil des EuGH zum Recht auf Vergessen bei der Suchmaschine von Google (mehr hierzu unter V 1.1) bestätigt unsere Auffassung. Die Abwägung von Persönlichkeitsrechten und Informationszugangsrechten der Allgemeinheit ist mittlerweile zu einer geübten Praxis von Suchmaschinenbetreibern und Datenschutzaufsichtsbehörden in ganz Europa geworden. Vor diesem Hintergrund wäre es nur konsequent, nicht nur die Vermittler, sondern auch die Anbieter von Informationen im Rahmen ihrer Möglichkeiten in diesem Ausgleichsprozess zu verpflichten. Das Verfahren ist vor dem Bundesverfassungsgericht aktuell noch anhängig.

7. Freies WLAN in Hamburg

Bereits frühzeitig haben wir auf Berichte reagiert, dass im Rahmen einer WLAN-Strategie der FHH Funknetzwerke großflächig bereitgestellt werden sollen. Über diese Hotspots, so die Planung, soll der Zugang zum Internet in der Hamburger Innenstadt scheller und einfacher als über die Mobilfunkinfrastruktur möglich und damit attraktiver werden.

Ende 2014 erreichten uns Pressemeldungen, die über Pläne des damaligen Senats berichteten, in der Hamburger Innenstadt für eine flächendeckende Versorgung mit WLAN-Hotspots zu sorgen. Diese begrüßenswerte Initiative wirft eine Reihe datenschutzrechtlicher Fragen auf. Wir haben daher Kontakt zu dem Hamburger Unternehmen willy.tel aufgenommen, das in diesem Zusammenhang als Vertragspartner für den Aufbau einer solchen Infrastruktur genannt wurde und uns die dortigen Pläne erläutern lassen. Erfreulicherweise sind wir dort auf eine große Bereitschaft gestoßen, uns Auskünfte zu geben.

Für uns war dabei vorrangig die Frage zu klären, um welche Art von Angebot es sich handeln soll, wer der Anbieter ist und wie das Verhältnis zwischen der öffentlichen und der privaten Seite ausgestaltet ist. Die Datenschutzaufsicht für die Verarbeitung personenbezogener Daten im Zusammenhang mit der geschäftsmäßigen Erbringung von Telekommunikationsdiensten liegt nach § 115 (4) bei der Bundesbeauftragten für den Datenschutz. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat dort eine eigene Zuständigkeit, wo über Hotspots ergänzend zur Telekommunikationsdienstleistung auch Telemedien angeboten werden oder wenn die FHH selbst als Anbieter auftritt. Letzteres ist allerdings nicht geplant. Der Beitrag der öffentlichen Seite besteht vor allem in der Bereitstellung geeigneter Infrastruktur in Gebäuden oder im öffentlichen Raum, wie etwa Licht- oder Ampelmasten.

Ein entscheidender Faktor bei einer solchen flächendeckenden Infrastruktur ist die Datensicherheit. Ziel muss es sein, ein Angebot zu schaffen, bei dem die Nutzer darauf vertrauen können, dass die übertragenen Daten gegen fremde Kenntnisnahme geschützt sind. Dies muss Bestandteil der Infrastruktur selbst sein, denn von den Nutzern kann nicht erwartet werden, dass sie Sicherheitsdefizite durch eigene Maßnahmen kompensieren. Eine Verschlüsselung der übertragenen Daten ist aus unserer Sicht daher zwingend. Eine von der FHH unterstützte Zugangsinfrastruktur zum Internet sollte bekannte Möglichkeiten zum Datenklau wie sie durch Hackingtools wie „Firesheep" oder „Faceniff" eindrücklich aufgezeigt werden, weitgehend minimieren.

Auch der aktuelle Senat hat sich den WLAN-Ausbau zum Ziel gesetzt und verfolgt die Pläne weiter. Dabei ist man weiterhin mit willy.tel, der Telekom und der Initiative Freifunk Hamburg im Gespräch. Offenbar sind die Ausbauziele jedoch nicht in dem ursprünglich angedachten Tempo zu erreichen. Wir werden die Sache im Rahmen unserer Zuständigkeit weiter verfolgen und stehen für Beratungsgespräche zur Verfügung.

8. Geltung des Medienprivilegs für Internetforen

Auch für Internetforen kann das im Bundesdatenschutzgesetz enthaltene Medienprivileg gelten, welches die Anwendung der materiell-rechtlichen Vorgaben auf die Verarbeitung personenbezogener Daten zu journalistisch-redaktionellen Zwecken ausschließt.

Bei der Prüfung von Internetdienstanbietern werden wir immer wieder mit der Frage konfrontiert, ob der jeweilige Anbieter vollumfänglich die Vorgaben des Bundesdatenschutzgesetzes bei der Verarbeitung personenbezogener Inhaltsdaten für den angebotenen Dienst beachten muss oder das Medienprivileg, § 41 BDSG, zur Anwendung

kommt (vgl. dazu auch Ziffer V. 11). Besonders schwierig ist die Antwort dann, wenn Nutzerinnen und Nutzer Kommentare zu den eingestellten Inhalten abgeben können und darüber weitere personenbezogene Daten verarbeitet werden.

Der Bundesgerichtshof hat in der Spickmich-Entscheidung (BGH Urteil vom 23.06.2009, Az. VI ZR 196/08) bei einem Personenbewertungsportal eine Antwort auf diese Frage gefunden. Wir orientieren uns bei unseren Entscheidungen an den dort gemachten Vorgaben des Gerichts. Dabei prüfen wir jeden Einzelfall genau und wägen das Interesse des Dienstanbieters auf Beachtung seines verfassungsmäßig garantierten Rechts auf Pressefreiheit gegen das Interesse des Schutzes des Grundrechts auf informationelle Selbstbestimmung der Betroffenen und damit der Anwendung datenschutzrechtlicher Vorgaben ab. Die pauschale Behauptung, es würden journalistisch-redaktionell bearbeitete Informationen veröffentlicht, reicht für die Annahme des Medienprivilegs nicht aus.
Denn Voraussetzung für die Beschränkung der Anwendung des Bundesdatenschutzgesetzes auf Medienangebote im Internet ist, dass durch den Anbieter personenbezogene Daten ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken verarbeitet werden. Maßgeblicher Prüfungspunkt ist also die konkrete Zwecksetzung der Veröffentlichung der Daten. Der Bundesgerichtshof hat 2009 diese Anforderung dahingehend konkretisiert, dass der jeweilige Telemediendienst unter den Pressebegriff des Art. 5 Abs. 1 GG fallen muss, um das Medienprivileg für sich in Anspruch nehmen zu können. Nach Ansicht des Bundesgerichtshofes müssen die Daten exklusiv für das eigene journalistische Angebot verwendet werden. Ein solches liegt immer dann vor, wenn die Informationen veröffentlicht werden, um eine meinungsbildende Wirkung für die Allgemeinheit zu erzielen. Diese Motivation muss zudem prägender Bestandteil des Angebots sein. Ist es hingegen „schmückendes Beiwerk" kann von einer pressemäßigen Veröffentlichung nicht gesprochen werden.

Anbieter, die personenbezogene Daten ohne eigene redaktionelle Bearbeitung im Sinne einer inhaltlich-wertenden Auseinandersetzung mit den Informationen veröffentlichen, unterfallen nicht dem Medienprivileg. Dies ist, z.B. dann der Fall, wenn Profile mit auf statistischen Berechnungen beruhenden „Wertungen" oder aus anderen Quellen erhobene Daten lediglich in einem anderen Format oder Kontext dargestellt werden. Anders wäre es, wenn sich die veröffentlichende Stelle mit den Inhalten, die sie verbreitet, auseinandersetzt, diese in einen politischen, wirtschaftlichen, sozialen oder anderweitig gesellschaftlichen Kontext setzt mit dem Ziel, auf die öffentliche Meinung prägend einzuwirken. Dazu würden dann z.B. auch Veröffentlichungen des Datenjournalismus zählen. In diesen Fällen wäre das Medienprivileg anzuwenden.

Kommentare zu den veröffentlichten Daten teilen in der Regel das rechtliche Schicksal des Angebotes. Unterfällt dieses dem Medienprivileg und sind Kommentare der Nutzer erkennbar Bestandteil des Angebotes mit einer identischen Zwecksetzung der Einwirkung auf die öffentliche Meinung, gilt für diese Beiträge ebenfalls das Medien-

privileg. Anderenfalls nicht.

Das bedeutet im Ergebnis, dass bei der Veröffentlichung personenbezogener Daten im Rahmen von Informationsangeboten, die erkennbar nicht als pressemäßige Veröffentlichung bewertet werden können, wie z.B. private Blogs, das Datenschutzrecht Anwendung findet. Wir legen jedoch die datenschutzrechtlichen Vorschriften verfassungskonform aus und lassen vor allem das Recht auf Meinungsäußerungsfreiheit in die datenschutzrechtliche Bewertung mit einfließen.

9. Indoor-Ortung von Personen in Geschäften

Die Erstellung von Bewegungsprofilen von Kunden oder Passanten durch die Ortung mobiler Endgeräte über deren WLAN- oder Bluetooth-Schnittstelle greift massiv in die Recht der Betroffenen ein und ist nur unter sehr engen Voraussetzungen zulässig.

Wir wurden verschiedentlich um Beratung zu der Frage gebeten, unter welchen Bedingungen die Erfassung von Kundenströmen und Bewegungsprofilen zu Zwecken der Werbung und des Marketings datenschutzrechtlich zulässig sein kann.

Diese Tracking-Verfahren basieren auf Techniken zur Ortung von mobilen Endgeräten unter Verwendung der WLAN- oder Bluetooth-Technologie. Anbieter und Verwender derartiger Systeme machen es sich zunutze, dass bei Smartphones aber auch Autoradios die WLAN- oder Bluetooth-Schnittstellen meistens aktiviert sind. Diese Schnittstellen sind in der Regel so konfiguriert, dass sie ohne Mitwirkung des Nutzers mit anderen Geräten in Kontakt treten oder ihre Bereitschaft, dies zu tun, regelmäßig signalisieren. Dadurch ist für einen WLAN-Access-Point bzw. Bluetooth-Master erkennbar, wann sich ein mobiles Endgerät in seinem Erfassungsbereich befindet. Da bereits bei einer Kontaktsignalisierung eindeutige Identifikatoren wie die individuelle MAC-Adresse (Media Access Control) ausgesendet werden, können die Geräte auch wiedererkannt und über mehrere Stationen verfolgt werden.

Durch die Installation mehrerer Empfangsstationen kann das vom mobilen Endgerät ausgesendete Signal verfolgt und dessen Bewegung aufgezeichnet werden. Über die einzigartige MAC-Adresse des Geräts ist dies damit auch dessen Besitzer eindeutig zuordnenbar. Auf diese Weise können sowohl weiträumige als auch langfristige Bewegungsprofile von Kundinnen und Kunden in Geschäften, Einkaufszentren oder anderen öffentlich zugänglichen Räumen erstellt werden. Eine Unterscheidung zwischen Kunden im engeren Sinne und Passanten, die an Geschäften lediglich vorbeikommen, ist dabei in der Regel kaum möglich.

Darüber sollen Erkenntnisse z.B. über das Kaufverhalten oder eine optimierte Platzierung von Werbung gewonnen werden. Genutzt wird diese Technologie aber auch für die Auswertung und Steuerung von Verkehrsströmen über die Erfassung von in Fahrzeugen eingebauten Geräten mit Bluetooth-Schnittstelle (vgl. VI 2.1).

Ausgangspunkt der technischen und datenschutzrechtlichen Bewertung ist der verfassungsrechtlich geschützte Anspruch des Einzelnen auf Schutz seiner Privatsphäre und Anonymität auch in der Öffentlichkeit. Die Erfassung eines Bewegungsprofils ist daher ohne entsprechende Rechtfertigung unzulässig. Diese Bedingungen gelten unabhängig davon, ob der Einzelne sich auf der Straße oder in einem Ladenlokal befindet. So muss niemand ohne Weiteres hinnehmen, dass erkennbar ist, wie häufig und auf welchem Weg er oder sie ein Geschäft betritt und sich in diesem bewegt, welchen morgendlichen Arbeitsweg man wählt, wo der Spaziergang am Wochenende entlang führt oder welche Geschäfte für den Einkaufsbummel besucht werden.

Dieses Thema beschäftigt derzeit nicht nur uns, sondern auch andere Aufsichtsbehörden. Wir beteiligen uns daher an einer entsprechenden Arbeitsgruppe der Datenschutzkonferenz. Sie hat das Ziel, die technischen und rechtlichen Rahmenbedingungen für den Einsatz der Erstellung von individuellen Bewegungsprofilen in einer Orientierungshilfe zu formulieren.
Bereits jetzt lassen sich erste Anforderungen formulieren, die durch Anbieter zu beachten sind. Sowohl die MAC-Adresse oder vergleichbare geräteindividuelle Kennzeichen als auch das individuelle Bewegungsprofil sind personenbezogene Daten i.S.d. Datenschutzrechts. Eine Erhebung, Verarbeitung oder Nutzung dieser Daten ist nur mit einer entsprechenden Rechtsgrundlage zulässig.

Die vollständige Beachtung datenschutzrechtlicher Vorgaben ist nicht erforderlich, soweit die erhobenen Daten wirksam anonymisiert werden. An die entsprechenden technischen Verfahren sind hohe Anforderungen zu stellen, insbesondere dort, wo individuelle Bewegungsprofile erstellt werden.

Damit stellt sich auch die Frage, welche konkreten rechtlichen Anforderungen an die Erhebung, Verarbeitung und Nutzung dieser Daten gestellt werden müssen.
Soweit Einwilligungen der Betroffenen unter Beachtung der Vorgaben des § 4a BDSG eingeholt werden, wird dies den datenschutzrechtlichen Anforderungen gerecht. Unter welchen praktischen Umständen dies möglich ist und ob andere Rechtsgrundlagen darüber hinaus tragfähig sein können, ist Gegenstand der derzeitigen Diskussion.
Unbestritten ist ebenfalls, dass Verwender derartiger Systeme in jedem Fall Transparenz über den Einsatz und die Erhebung der Informationen sowie dem dadurch verfolgten Zweck herstellen müssen. Dass kann durch geeignete Hinweise, z.B. eine Kombination aus Piktogrammen und Text vor Eintritt in den Erfassungsbereich erfolgen.

Betroffene können sich in gewissem Umfang vor der Erfassung durch solche Systeme

schützen, indem WLAN- und Bluetooth-Schnittstellen nur dann aktiviert werden, wenn sie für die Nutzung des Gerätes erforderlich sind. Dies ist allerdings bereits technisch nicht immer möglich. Solche Behelfslösungen können zudem nicht die Anforderungen an die Rechtskonformität der Tracking-Systeme verringern, etwa indem eine eingeschaltete Schnittstelle als Einwilligung für ein Tracking verstanden werden könnte.

10. Sportinformationsdienst im Internet

Ein Dienst, der Einzelprofile von Amateur- und Profisportlern mit deren Leistungsdaten, Wettkampfergebnissen und Sportnachrichten im Internet veröffentlicht, kann sich nicht ohne Weiteres auf das Medienprivileg berufen und hat die schutzwürdigen Interessen der betroffenen Sportler, insbesondere deren Widersprüche gegen die Veröffentlichung, zu beachten.

Aufgrund einer Beschwerde haben wir den in Hamburg ansässigen Betreiber eines sehr beliebten und im Internet hoch frequentierten Informationsangebotes über den Profi- und Amateurfußball überprüft. Dies war aufgrund der recht komplexen datenschutzrechtlichen und technischen Fragestellungen umfangreich und langwierig und ist derzeit noch nicht vollständig abgeschlossen. Bereits jetzt lassen sich jedoch erste Feststellungen treffen, die wir auf der Grundlage der sog. Spickmich-Entscheidung des BGH (Urteil vom 23. 6. 2009 - VI ZR 196/08) getroffen haben.

Wir sind durch eine Eingabe auf das Informationsangebot aufmerksam gemacht worden. Ein betroffener Sportler hatte sich an uns gewandt, weil der Anbieter des Dienstes seinen Widerspruch gegen die Veröffentlichung seines Profils nicht umsetzen wollte.

Das Informationsangebot des Anbieters besteht im Kern aus der Veröffentlichung von Informationen über einzelne Sportler in der Form eines Profils bzw. einer Informationskarte, auf der u.a. Namen, Alter, Nationalität, Vereinsmitgliedschaft und spielbezogene Informationen veröffentlicht werden. Die Veröffentlichung betrifft sowohl Profi- als auch Amateursportler. Teilweise finden sich auch Angaben zu Verletzungen, also gesundheitsbezogene Angaben.

Zudem werden die Ergebnisse von Liga- und Pokalspielen als auch einschlägige Sportnachrichten über diesen Dienst verbreitet. Die Informationen stammen aus öffentlichzugänglichen, jedoch nicht immer rein digitalen oder über das Internet abrufbaren Quellen (z.B. Sportzeitungen) oder werden von Unterstützern des Dienstes gesammelt. Der Anbieter speichert diese Informationen in sein Datenbanksystem ein.

Wir mussten vorrangig die Frage klären, ob sich der Anbieter des Dienstes bei der Veröffentlichung der personenbezogenen Informationen auf das Medienprivileg im Sinne des § 41 Abs. 1 BDSG berufen durfte, was zu einem Ausschluss maßgeblicher Normen des Bundesdatenschutzgesetzes geführt hätte. Wir haben dies für die Veröffentlichung der Profileinträge der betroffenen Sportler abgelehnt. Auch wenn die Zusammenstellung der einzelnen Informationen eine gewisse redaktionelle Gestaltung voraussetzt, ist aus unserer Sicht die Schwelle zur journalistischen Tätigkeit nicht überschritten worden. Denn die Darstellungen der einzelnen Sportler haben im Sinn der Spickmich.de-Entscheidung des Bundesgerichtshofes keine „meinungsbildende Wirkung für die Allgemeinheit" (vgl. Ziffer 9 des Tätigkeitsberichts), da lediglich Tatsacheninformationen wie Name, Geburtsdatum, Herkunft, Vereinszugehörigkeit usw. in einem Profil veröffentlicht werden.

Diese Bewertung ändert sich auch nicht dadurch, dass Nachrichten aus weiteren Drittquellen auf der Internetseite des Anbieters zu finden sind. Prägender Bestandteil des Angebots sind die Sportlerprofile. Die ebenfalls auf der Seite zu findenden Nachrichten haben den Charakter von Beiwerk und sollen das eigentliche Angebot nur ausgestalten. Deswegen unterfällt die Verarbeitung der Daten der Sportler vollumfänglich den datenschutzrechtlichen Regeln.

Im Hinblick auf die datenschutzrechtliche Zulässigkeit der Veröffentlichung der Informationen im Internet haben wir ein abgestuftes Konzept entwickelt und bei der Bewertung der schutzwürdigen Interessen der Sportler vor allem die besondere Reichweite der Veröffentlichung der personenbezogenen Daten durch den Informationsdienst in Betracht gezogen. Denn selbst wenn ein Großteil der gespeicherten personenbezogenen Daten bereits allgemeinzugänglich veröffentlicht waren, z.B. in Printmedien oder auf Seiten der Vereine der Sportler, führt die sehr große Beliebtheit des Dienstes zu einer deutlich höheren Verbreitung der veröffentlichten Informationen.

Dementsprechend haben wir die Schutzwürdigkeit minderjähriger Sportler als besonders hoch eingeschätzt und verlangt, dass die Speicherung und Veröffentlichung von personenbezogenen Daten nur mit einer rechtswirksamen Einwilligung erfolgt. Aus welcher Quelle die Daten stammen, ist dabei unerheblich.

Name, Alter und Verein aktiver erwachsener Amateursportler dürfen hingegen auf der Grundlage von § 29 BDSG in der Datenbank des Anbieters gespeichert und im Internet veröffentlicht werden. Sobald diese jedoch gegen die Veröffentlichung Widerspruch einlegen, hat der Betreiber dies zu beachten und umzusetzen. Darüber hinaus ist die Veröffentlichung weiterer personenbezogener Daten ohne Einwilligung datenschutzrechtlich nicht möglich.

Für Profisportler ist die Speicherung und Veröffentlichung personenbezogener Daten ebenfalls auf der Grundlage von § 29 BDSG jedoch in einem größeren Umfang als bei

Amateursportlern zulässig. Teile der beruflichen Tätigkeit erfolgen in der Öffentlichkeit und sind regelmäßig Gegenstand der Berichterstattung im Internet, den Printmedien sowie Rundfunk und Fernsehen. Dies führt bei der Speicherung und Veröffentlichung berufsbezogener personenbezogener Daten zu einer geringeren Schutzwürdigkeit der Betroffenen und insoweit zu einer datenschutzrechtlichen Zulässigkeit der Speicherung und Veröffentlichung. Zudem muss davon ausgegangen werden, dass aufgrund der Bedeutung des Dienstes für diesen Sport die betroffenen Profisportler regelmäßig ein eigenes Interesse an der Veröffentlichung ihrer Daten haben.

Beschränkt haben wir allerdings die Speicherung und Veröffentlichung von besonderen personenbezogenen Daten der Betroffenen aus dieser Sportlergruppe. Deren Veröffentlichung ist in der Regel ohne Einwilligung der Betroffenen nicht zulässig, es sei denn, sie haben diese Informationen selbst veröffentlicht. Die Darstellung muss dennoch in allgemeiner Form und lediglich sportbezogen sein. So wäre die Veröffentlichung z.B. von Gesundheitsinformationen, die das Betreiben des Sportes nicht beeinträchtigen, ohne explizite Einwilligung unzulässig.

Wir haben von dem Betreiber zudem die Implementierung eines Löschkonzeptes für nicht mehr aktive Amateur- und Profisportler gefordert. Auch wenn durch uns anerkannt wurde, dass aus sporthistorischem Interesse heraus auch die dauerhafte Speicherung und Veröffentlichung gewünscht wird, muss dem Recht der Betroffenen, nicht auf Dauer mit der Veröffentlichung ohne deren Einwilligung konfrontiert zu sein, Rechnung getragen werden.

Die Umsetzung der dargestellten Konzepte und Maßnahmen dauern über den Berichtszeitraum hinaus an.

11. Prüfung von Partnerschaftsbörsen im Internet

Mit den Aufsichtsbehörden der Länder Bayern, Baden-Württemberg und Berlin haben wir eine Branchenprüfung von Online-Partnerschaftsbörsen eingeleitet und dabei gemeinsame Datenschutzstandards für diese Angebote vereinbart.

Die Prüfung erfolgte in einem ersten Schritt über einen standardisierten Fragebogen, den wir an mehrere Betreiber von Online-Partnerschaftsbörsen mit Sitz in Hamburg versandt und danach ausgewertet haben. Um einen deutschlandweit einheitlichen Prüfmaßstab zu gewährleisten und Markteinheitlichkeit herstellen zu können, haben wir uns mit den anderen teilnehmenden Kontrollbehörden auf bestimmte grundsätzliche Festlegungen geeinigt und diese gegenüber den geprüften Unternehmen kommu-

niziert. Auch wenn die Prüfungen noch andauern, lassen sich bereits jetzt bestimmte Feststellungen treffen.

Die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten erfolgt in der Regel auf einer gesetzlichen Grundlage und ist nicht ausschließlich gestützt auf die Einwilligung der Betroffenen. Je nach konkreter Ausgestaltung des Dienstes können neben § 28 Abs. 1 Satz 1 Nr. 1 BDSG auch § 29 Abs. 1 Satz 1 BDSG in Betracht kommen.

Eine Einwilligung ist hingegen bei der Verarbeitung von besonderen personenbezogen Daten i.S.d. § 3 Abs. 9 BDSG, wie der sexuellen Orientierung erforderlich, weil die engen gesetzlichen Voraussetzungen der § 28 Abs. 6 bis 9, § 29 Abs. 5 BDSG unter denen diese Daten ohne die Einwilligung der Betroffenen erhoben, verarbeitet oder genutzt werden können, durch die Anbieter in der Regel nicht erfüllt werden können. Dieser Fall tritt bereits ein, wenn bei der ersten Registrierung nach der sexuellen Orientierung („Mann sucht Frau", „Mann sucht Mann" etc.) gefragt wird. Bereits die Anmeldung bei einer auf bestimmte sexuelle Orientierungen oder Interessen ausgerichteten Börse kann als sensibel eingestuft werden. In jedem Fall erheben Partnerschaftsbörsen dann besonders sensible Informationen, wenn über die sexuellen Präferenzen hinaus Angaben zur Religion, Gesundheit oder politischen oder gesellschaftlichen Einstellungen abgefragt werden.
Von einem hohen Schutzbedarf muss zudem ausgegangen werden, wenn die Anbieter Persönlichkeitstests anbieten und entsprechende Persönlichkeitsprofile der Nutzerinnen und Nutzer erstellen. Diese u.a. zum Matching verwendeten Profile geben detailliert Auskunft über die Persönlichkeit einer Person. Der Missbrauch derartiger Informationen kann zu einer gravierenden Verletzung der Persönlichkeitsrechte der Betroffenen führen.

Das automatische Filtern und Scannen von Kommunikationsinhalten der individuellen Kommunikation zwischen den Nutzerinnen und Nutzern zur Vermeidung von Missbrauch (z.B. romance scamming, d.h. das massenhafte Versenden von Mitteilungen u.a. mit dem Zweck der Heiratsschwindelei) des Dienstes ist ein Eingriff in das Fernmeldegeheimnis und ohne entsprechende Einwilligung der Betroffenen datenschutzrechtlich unzulässig.
Auch fordern wir von Anbietern, die Auskunftserteilung möglichst einfach und unkompliziert auszugestalten. Dazu gehört vor allem die Möglichkeit einer medienbruchfreien Erteilung der Auskunft. Idealerweise bieten Anbieter den Nutzerinnen und Nutzern proaktiv einen Downloadbereich an, so dass ein aufwändiger und personalintensiver Auskunftserteilungsprozess vermieden werden kann. In jedem Fall müssen Auskünfte vollständig und umfassend erteilt werden. Dazu zählen auch die mit anderen Nutzerinnen und Nutzern geführten Kommunikationsinhalte.

In der Regel bezweifeln wir gemeinsam mit den anderen Aufsichtsbehörden die Not-

wendigkeit einer Identifizierung der Nutzerinnen und Nutzer durch den Anbieter, soweit eine kostenlose Nutzung möglich ist. Darüber hinaus ist das Recht auf anonyme oder pseudonyme Nutzung von Telemediendiensten gemäß der Vorgaben des § 13 Abs. 6 TMG (dazu auch Ziffer 2.2) zu beachten.

Soweit eine Identifizierung aufgrund gesetzlicher oder vertraglicher Gründe (z.B. kostenpflichtige Accounts) erforderlich ist und der Betreiber eine Identifikation mittels des amtlichen Personalausweises vornehmen möchte, verlangen wir die Verwendung der e-ID des neuen Personalausweises. Die Verwendung von Kopien des Personalausweises wird ausnahmsweise geduldet, wenn die Betroffenen nur im Besitz eines alten Personalausweises sind, der Hinweis erfolgt, welche Daten geschwärzt werden können und die Kopie nach der Identitätsprüfung unverzüglich durch den Anbieter vernichtet wird.
Wir fordern zudem von Betreibern von Partnerschaftsbörsen die Festlegung eines Löschkonzeptes. Soweit durch die Anbieter keine plausiblen Gründe für eine längere Speicherfrist dargelegt werden, gehen wir davon aus, dass eine Speicherung eines nicht genutzten Accounts nach 1 Jahr nicht mehr erforderlich ist und sämtliche Daten nach vorheriger Ankündigung gegenüber dem Betroffenen gelöscht werden.

Bei den verarbeiteten Daten handelt es sich regelmäßig um solche mit einem hohen Schutzbedarf. Für die technischen und organisatorischen Maßnahmen bedeutet dies u.a. die Verwendung entsprechend komplexer Passwörter sowie weiterer Maßnahmen für eine sichere Authentifizierung. Die immer wieder festzustellende Praxis des unverschlüsselten Versendens von Passwörtern an die Nutzerinnen und Nutzer ist nicht zulässig. Außerdem führt die Festlegung des hohen Schutzbedarfes dazu, dass der Dienst nur noch unter Verwendung einer Verschlüsselung mit HTTPS angeboten werden darf, möglichst mit einer wirksamen Unterstützung von Perfect Forward Secrecy, HSTS (HTTP Strict Transport Security) und Key-Pinning.

12. Umsetzung der Cookie-Richtlinie

An der bereits im 24. Tätigkeitsbericht gemachten Feststellung (Ziffer V. 2),dass die Umsetzung des Art. 5 Abs. 3 der Richtlinie 2002/58/EG des Europäischen Parlaments und Rates mit Stand vom 18.12.2009 (E-Privacy Richtlinie) in nationales Recht gescheitert ist, hat sich trotz der Prüfung eines Vertragsverletzungsverfahrens durch die EU-Kommission nichts geändert.

Wie wir bereits im letzten Bericht darstellten, ist Ziel der Richtlinie ein verbesserter Schutz der Nutzerinnen und Nutzer bei der Verwendung von elektronischen Kommunikationsdiensten des Internets. Dienstanbieter werden durch diese Richtlinie verpflichtet, bei der Verwendung von Cookies und vergleichbaren Technologien, die

die Privatsphäre der Nutzerinnen und Nutzer beeinträchtigen können, z.B. durch die Auswertung des Nutzerverhaltens bei der Erstellung verhaltensbasierter Werbung im Internet, vorab eine Einwilligung einzuholen.

Zudem hatten wir festgestellt, dass bei der Umsetzung der Anforderungen des Art. 5 Abs. 3 E-Privacy Richtlinie eine erhebliche Unsicherheit bei den Anforderungen an die Einwilligung bestand und die Praxis der Umsetzung auf europäischer Ebene höchst unterschiedlich war. Dazu hatte die Art-29-Datenschutzgruppe mehrere Stellungnahmen (z.B. Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht vom 07. Juni 2012 oder Arbeitsunterlage 02/2013 mit Leitlinien für die Einholung der Einwilligung zur Verwendung von Cookies vom 02. Oktober 2013) veröffentlicht und den Versuch unternommen, eine einheitliche Anwendungsweise der Vorgaben europaweit sicherzustellen.

Aus nationaler Sicht war festzustellen, dass diese Bemühungen zum Scheitern verurteilt waren, weil nach Auffassung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder der deutsche Gesetzgeber die Vorgaben der Richtlinie nicht bzw. unvollständig umgesetzt hat (Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 05. Februar 2015 zur Verfolgung des Nutzerverhaltens im Internet).

Der Regulierungsstand des Telemediengesetzes (TMG) sah und sieht keine Verpflichtung der Dienstanbieter vor, den Nutzerinnen und Nutzern wirksame Einwirkungsmöglichkeiten einzuräumen, um den Einsatz von Cookies und vergleichbaren Techniken, die Eingriffe in deren Persönlichkeitsrechte vorbereiten, zu verhindern. Die Chance, über das im Herbst 2015 erlassene IT-Sicherheitsgesetz, durch welches auch das Telemediengesetz geändert wurde, die Umsetzung des Art. 5 Abs. 3 E-Privacy Richtlinie zu realisieren, wurde vertan.

Das Telemediengesetz enthält weiterhin lediglich die Pflicht, 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.

Die Inaktivität des Gesetzgebers führte dazu, dass die EU-Kommission die Einleitung eines Vertragsverletzungsverfahrens gegen die Bundesrepublik Deutschland wegen der unzureichenden Umsetzung der Richtlinie prüfte und erste Verfahrensschritte einleitete. Das für diese Thematik zuständige Bundeswirtschaftsministerium lud daraufhin die Datenschutzbeauftragten zu einer Anhörung im Frühjahr 2015 ein. Dort haben wir unseren Standpunkt erneut und eindringlich deutlich gemacht. Es muss jedoch festgestellt werden, dass diese Anhörung in der Sache, trotz entgegenstehender Zusagen durch das Ministerium, keine erkennbare Bewegung in die Umsetzung gebracht hat. Es drängt sich der Eindruck auf, dass wenig Interesse an dem effektiven Schutz

der Persönlichkeitsrechte der Nutzerinnen und Nutzer im Internet besteht.
Aufgrund dieser rechtspolitischen Rahmenbedingungen hegen wir große Zweifel, ob deutsche Nutzerinnen und Nutzer überhaupt in den Genuss der Regelung des § 5 Abs. 3 E-Privacy Richtlinie kommen werden. Einige Dienstanbieter haben mittlerweile reagiert und informieren zumindest prominent auf der ersten Seite über den Einsatz von Cookies und vergleichbaren Technologien. Ein Teilerfolg im Hinblick auf die Transparenz ist damit erzielt.

Von der Umsetzung des Rechts der Nutzerinnen und Nutzer selbst darüber entscheiden zu können, ob sie Dienste im Internet mit der Erfassung und Auswertung ihres Nutzungsverhaltens verwenden möchten, sind wir weiterhin meilenweit entfernt.

13. Heartbleed Bug – Sicherheitslücke bei Web-Servern

In der OpenSSL-Implementierung der Verschlüsselung von Datenübertragung über das Internet wurde 2014 ein schwerer Fehler entdeckt und unter dem Namen „Heartbleed" publik. Der Fehler ermöglicht unberechtigtes Auslesen von Daten. Betroffen waren auch Hamburger Web-Server.

Im April 2014 wurde in der OpenSSL-Implementierung, mit der für Web- und E-Mail-Server eine Verschlüsselung der Kommunikation über das Internet eingerichtet werden kann, eine schwerwiegende Sicherheitslücke entdeckt. Da diese in der sog. „Heartbeat"-Erweiterung des TLS-Verfahrens vorlag, erhielt sie den Namen „Heartbleed Bug". Die Sicherheitslücke, die zum Zeitpunkt der Entdeckung bereits über 2 Jahre bestand, ermöglichte es, Teile aus dem Arbeitsspeicher eines Servers abzufragen und auf diese Weise Informationen wie Benutzernamen, Passwörter oder private Schlüssel zu erlangen. Mit privaten Schlüsseln können aufgezeichnete TLS-Verbindungen auch nachträglich entschlüsselt werden, sofern für diese keine zusätzliche Schutzmaßnahme wie z.B. Perfect Forward Secrecy angewandt wurde.

Zur Behebung des Heartbleed Bugs hat das OpenSSL-Team binnen kurzer Zeit korrigierte Dateien veröffentlicht, welche die alten Versionen ersetzen. Da nicht nur IT- und Fachmedien, sondern auch Massenmedien über das Thema berichteten, war anzunehmen, dass Betreiber von Web-Servern auf das Problem aufmerksam wurden, Handlungsbedarf erkennen und die Sicherheitslücke auf ihren Systemen beheben. Ferner gab es spezielle Webseiten für die Überprüfung, ob der eigene Server vom Heartbleed Bug betroffen ist.

Das Bundesdatenschutzgesetz verpflichtet Betreiber von Internet-Servern oder Webangeboten, personenbezogene Daten, die über das Internet übermittelt werden,

durch geeignete Maßnahmen gegen z.B. unberechtigte Kenntnisnahme zu schützen. Die Verschlüsselung mit TLS gilt dabei als geeignete Schutzmaßnahme. Mit Bekanntwerden der Sicherheitslücke bei alten OpenSSL-Implementierungen waren diese durch ein Update zu aktualisieren. Zur Überprüfung, ob Betreiber in Deutschland ihrer Nachbesserungspflicht nachgekommen sind, hat das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) im August 2014 eine automatisierte Überprüfung mehrerer hundert E-Mail-Server in Deutschland vorgenommen. Dabei wurden insbesondere folgende Punkte betrachtet:

- Einsatz des Verschlüsselungsprotokolls SSL/TLS bzw. STARTTLS
- Einsatz von Perfect Forward Secrecy (PFS) als zusätzliche Schutzmaßnahme
- Verwundbarkeit durch die Sicherheitslücke Heartbleed

Bei festgestellten Schwachstellen bei einem Anbieter hat das BayLDA die jeweils zuständige Aufsichtsbehörde informiert. Auch für Hamburg ergab sich rund ein Dutzend Treffer bei kommerziellen Internetangeboten. Der HmbBfDI hat daraufhin die Betreiber der betroffenen Server kontaktiert und zur Behebung des Problems aufgefordert. In nahezu allen Fällen wurde der Anforderung kooperativ und fristgerecht entsprochen. Ferner wurden bei dieser Gelegenheit weitere Missstände wie fehlende Verschlüsselung bei Bestellungen im Web-Shop adressiert und behoben. Bei Servern, die von der FHH betrieben werden, sind dem HmbBfDI keine Heartbleed-Sicherheitslücken bekannt geworden.

14. Datenschutz-Kodex für Geodatendienste

Bereits seit mehreren Jahren befasst sich der Düsseldorfer Kreis mit dem Datenschutz-Kodex für Geodatendienste, der die schutzwürdigen Interessen der Eigentümerinnen und Eigentümer sowie Bewohnerinnen und Bewohner von im Internet veröffentlichten Grundstücks- und Gebäudeansichten wahren soll; auch die Neufassung entspricht nach Auffassung der Datenschutzaufsichtsbehörden nicht den gesetzlichen Vorgaben.

Der Düsseldorfer Kreis als Zusammenschluss der obersten Datenschutzaufsichtsbehörden des Bundes und der Länder hat das Ziel, sich im Bereich der Wirtschaft informell über eine möglichst gleichmäßige Anwendung und Auslegung des Bundesdatenschutzgesetzes (BDSG) zu verständigen. Für Fragen des Geodatenschutzes hat der Düsseldorfer Kreis eine „Unterarbeitsgruppe Geodaten" (UAG Geodaten) eingerichtet, in der auch wir Mitglied sind.

Der Verein „Selbstregulierung Informationswirtschaft e.V. (SRIW)" mit Sitz in Berlin

hat mit dem „Datenschutz-Kodex für Geodatendienste“ ein Regelwerk für Straßenpanoramadienste geschaffen, mit dem beigetretene Unternehmen sich die Selbstverpflichtung auferlegen, die detaillierten Datenschutzregelungen des Kodexes zu befolgen. Der Kodex soll einen angemessenen Ausgleich zwischen dem Schutz Betroffener beim Umgang mit in den Geodaten enthaltenen personenbezogenen Daten einerseits und den Interessen von Nutzerinnen, Nutzern und Anbietern von Straßenpanoramadiensten andererseits gewährleisten. Der im Jahr 2011 veröffentlichte Kodex wurde vom SRIW im Jahr 2015 überarbeitet (*http://geodatendienstekodex.de/images/pdf/Datenschutz-Kodex.pdf?layoutId=54130*). Er soll nunmehr neben den im Internet öffentlich zugänglichen Straßenpanoramaaufnahmen auch solche Aufnahmen erfassen, die nicht öffentlich zugänglich sind und beispielsweise für die Erfüllung kommunaler Aufgaben gemacht werden.

Grund der Einbeziehung der Aufsichtsbehörden des Bundes und der Länder in die Schaffung und Überarbeitung des Kodexes ist vor allem, dass der SRIW für die beigetretenen Unternehmen bei der Berliner Aufsichtsbehörde nach § 38a BDSG die Feststellung der Vereinbarkeit des Kodexes mit dem geltenden Datenschutzrecht erreichen möchte. Eine Empfehlung des Düsseldorfer Kreises wäre dafür hilfreich.

Im November 2014 übersandte uns der SRIW einen Evaluationsbericht über den Datenschutz-Kodex von 2011. In der Folge befasste sich die UAG Geodaten mit überarbeiteten Entwürfen des SRIW. Unabdingbare Voraussetzung für ein positives Votum des Düsseldorfer Kreises blieb allerdings, dass im Kodex das Recht Betroffener festgeschrieben werden müsse, bereits vor einer Veröffentlichung der Panoramaaufnahmen die Unkenntlichmachung ihrer personenbezogenen Daten zu verlangen. Doch auch in der Neufassung des Kodexes wird Betroffenen nach wie vor nur das Recht zugestanden, erst nach einer Veröffentlichung der Bilder die Unkenntlichmachung, z. B. durch Verpixelung der Gebäudefassade, zu verlangen. Dies verstößt nach Auffassung des Düsseldorfer Kreises gegen geltendes Datenschutzrecht. Der Düsseldorfer Kreis hatte in seiner Sitzung am 4. und 5. März 2015 zunächst beschlossen, sich zu dem Geodaten-Kodex und seiner Evaluation nicht mehr zu äußern, da die zentrale Forderung der Aufsichtsbehörden nach einem Vorabwiderspruchsrecht der Betroffenen nicht erfüllt wird.

Der SRIW hat sich dennoch um den weiteren Kontakt zu den Aufsichtsbehörden bemüht. Die Aufsichtsbehörden haben eine Liste erarbeitet, in der neben dem wichtigen Punkt des Vorabwiderspruchsrechts weitere Kritikpunkte erläutert wurden. Der Düsseldorfer Kreis hat sich in seiner Sitzung am 15. und 16. September 2015 mehrheitlich dafür ausgesprochen, die Gespräche mit dem SRIW aufrecht zu erhalten. Voraussichtlich wird sich die UAG Geodaten weiter mit dem Thema Datenschutzkodex befassen. Ziel eines Datenschutzkodex für Geodatendienste muss es nach unserer Auffassung sein, die gesetzlichen Regelungen z. B. des BDSG und des Telemediengesetzes einzuhalten und darüber hinaus einen echten Mehrwert an Datenschutz für die Betroffenen zu bieten.

15. Geobusiness Code of Conduct

Um den Zugang zu und den Umgang mit staatlichen Geoinformationen zu erleichtern, wurde eine Selbstverpflichtung für private Unternehmen geschaffen, an der die Datenschutzbehörden der Länder mitgewirkt haben.

Die Nutzung von Geoinformationen, die bei öffentlichen Stellen vorhanden sind, ist für viele Unternehmen von großem wirtschaftlichem Interesse, sei es, dass sie Auskunft über Rohstoffvorkommen, grundstücksbezogene Niederschlagsmengen oder Denkmalschutz von Gebäuden geben. Da viele Geodaten sehr genau sind oder in hochauflösenden Bilddaten bestehen und deshalb personenbezogene Daten enthalten, ist im Einzelfall die Prüfung der Behörden, ob einem anfragenden Unternehmen der Zugang zu staatlichen Geoinformationen erteilt werden kann, aufwändig. Der in Berlin ansässige Verein Selbstregulierung in der Informationswirtschaft e.V. (SRIW) hat mit Unterstützung der Kommission für Geoinformationswirtschaft beim Bundesministerium für Wirtschaft und Energie (GIW-Kommission) ein Instrument zur Selbstverpflichtung von Unternehmen geschaffen, den „Geobusiness Code of Conduct" (Geobusiness CoC). Hier können Unternehmen, die staatliche Geodaten nutzen wollen, online ihre datenschutzrelevanten Geschäftsprozesse akkreditieren. Ziel des SRIW war es, die Anerkennung des Geobusiness CoC durch den Berliner Datenschutzbeauftragten gemäß § 38a Bundesdatenschutzgesetz (BDSG) zu erreichen.

Der „Düsseldorfer Kreis" der Aufsichtsbehörden (siehe Näheres unter V. 14) hatte die Unterarbeitsgruppe Geodaten (UAG Geodaten), in der auch unsere Aufsichtsbehörde Mitglied ist, beauftragt, die Entwicklung des Geobusiness CoC zu begleiten. Wichtig war für uns, dass der CoC auch Anwendung findet, wenn Geodaten genutzt werden sollen, bei denen ein Personenbezug nicht völlig / eindeutig auszuschließen ist – im Zweifel für den Datenschutz. Außerdem haben wir auf klare Formulierungen, eindeutige Abgrenzungen der Zuständigkeiten für das Beitritts- und Akkreditierungsverfahren wie auch das Beschwerdeverfahren, mit dem Dritte, insbesondere Betroffene, und Beteiligte prüfen lassen können, inwieweit beigetretene Unternehmen den Geobusiness CoC befolgt haben.

Nachdem die UAG Geodaten dem Düsseldorfer Kreis in seiner März-Sitzung den GeoBusiness CoC in der in der Sitzung der UAG Geodaten vom 13. Januar 2015 besprochenen Fassung befürwortet hatte, hat der SRIW am 11.05.2015 die Fassung des Verhaltenskodexes vom 13.01.2015 der zuständigen Berliner Aufsichtsbehörde vorgelegt. Mit Feststellungsbescheid vom 27.07.2015 hat der Berliner Beauftragte für Datenschutz und Informationsfreiheit gemäß § 38a Abs. 2 BDSG die Vereinbarkeit des GeobusinessCoC mit geltendem Datenschutzrecht anerkannt. Unternehmen können dazu den Service unter *www.geodatenschutz.org* nutzen.

16. Kamerafahrten durch Hamburgs Straßen – ein Nachtrag

Überraschend teilte uns der Landesbetrieb Geoinformation und Vermessung (LGV) nach Redaktionsschluss zum 24. Tätigkeitsbericht mit, dass ein Unterauftragnehmer Panoramaaufnahmen, die für die erfolglose Machbarkeitsstudie erstellt wurden, nicht löschen will; die weitere Aufklärung stellt uns jedoch vor Probleme.

Im 24. TB (III. 9.2) berichteten wir über ein vom LGV in Auftrag gegebenes Projekt; eine Berliner Firma erhielt den Auftrag, ein Verfahren zur „automatisierten Texturierung" zu entwickeln. Dafür wurden vom Baden-Württembergischen Subunternehmer der Berliner Firma Panoramaaufnahmen in einigen Hamburger Straßen durchgeführt. Später hatten der LGV und das Berliner Unternehmen diese Testaufnahmen gelöscht, weil das Verfahren nicht für die Zwecke des LGV geeignet war. Anhaltspunkte für einen datenschutzrechtlichen Verstoß sahen wir nicht, so dass wir keine Veranlassung sahen, den Berliner Beauftragten für Datenschutz und Informationsfreiheit zu informieren.

Nach Redaktionsschluss zum 24. TB teilte uns der LGV mit, dass der in Baden-Württemberg ansässige Panoramadienst die Aufnahmen nicht gelöscht habe. Am Rande einer Besprechung zu einem anderen Thema haben wir Anfang 2014 den Geschäftsführer des Unternehmens darauf angesprochen, dass nach unserer Rechtsauffassung die Aufnahmen gemäß § 11 Abs. 2 Satz 2 Nr. 10 Bundesdatenschutzgesetz (BDSG) hätten gelöscht oder an den Berliner Auftraggeber herausgegeben werden müssen, weil der Auftrag als Auftragsdatenverarbeitungsvertrag zu qualifizieren sei. Dem widersprach das Baden-Württembergische Unternehmen mit Hinweis darauf, dass man sich regelmäßig vertraglich dauerhaft alle Rechte an den gemachten Aufnahmen vorbehalte. Nach unserer Rechtsauffassung, nach der ein Auftragsdatenverarbeitungsverhältnis vorgelegen hatte, ergab sich auch keine rechtliche Möglichkeit, den weiteren Besitz der Bilddaten mit einer Zweckänderung zu rechtfertigen.

Wir hatten keine rechtliche Handhabe, uns von den beiden Firmen die Vertragsunterlagen zeigen zu lassen, da die Firmensitze nicht in Hamburg lagen. Nachdem uns bekannt geworden war, dass der Landesbeauftragte für den Datenschutz Baden-Württemberg sich mit dem dort ansässigen Unternehmen befasst hatte, haben wir der Aufsichtsbehörde unsere Erkenntnisse und Einschätzungen mitgeteilt und uns nach den dortigen Ergebnissen erkundigt.

Im September 2015 teilte uns die Baden-Württembergische Aufsichtsbehörde mit, dass sie im Jahr 2012 erfahren habe, dass das Unternehmen Straßen von Kommunen ohne Auftrag abfilme und interessierten Kommunen die Aufnahmen anbiete. Im Jahr 2014 habe man in einer Diskussion mit der Firma die Ansicht geäußert, dass

Aufnahmen in erforderlichem Umfang für die kommunale Aufgabenerfüllung auf der Grundlage eines Auftragsdatenverarbeitungsvertrags möglich seien, wobei das Datenmaterial nicht in der Hoheitsgewalt des Unternehmens verbleiben dürfe. Man habe erfolglos um Vorlage von Standardverträgen der Firma gebeten. Die Firma wiederholte im August 2015 gegenüber der Baden-Württembergischen Aufsichtsbehörde, sie gehe nicht von Auftragsdatenverarbeitung aus. Inzwischen hat das Unternehmen seinen Firmensitz nach Hessen verlegt.

Wir bezweifeln, dass Unternehmen Straßenpanoramaaufnahmen ohne konkrete Zweckbestimmung behalten oder auf Vorrat ohne konkreten Auftrag erstellen oder behalten dürfen. Insofern raten wir den Behörden, im Falle einer Beauftragung von Panoramadiensten einen wirksamen Auftragsdatenverarbeitungsvertrag abzuschließen, wonach die personenbezogenen Daten am Ende des Auftrags zurückzugeben oder zu löschen sind. Wir sind daran interessiert, gemeinsam mit den anderen Aufsichtsbehörden eine Klärung der Frage herbeizuführen, ob sich Panoramadienste unabhängig von einem Auftrag die Rechte an den Aufnahmen aus Straßenbefahrungen vorbehalten dürfen.

17. Smart-TV und HbbTV, Orientierungshilfe Smart-TV

Viele Smart-TV-Geräte ermöglichen bei Internetanbindung eine Ausforschung des Nutzerverhaltens. Die „Orientierungshilfe Smart-TV" der Datenschutzbehörden nimmt Gerätehersteller und Anbieter von Smart-TV-Diensten in die Pflicht.

Fernsehgeräte mit Internetanbindung und computer-ähnlichen Funktionalitäten werden als „Smart-TV" bezeichnet. Diese Geräte bieten nicht nur Zugriff auf zahlreiche Dienste und Zusatzinformation im Internet, sondern fungieren häufig selbst als permanent sendende Informationsquelle. Beispielsweise für den Hersteller des Gerätes, für Rundfunkanbieter oder für Anbieter von Apps oder sog. „Smart-TV-Diensten". All diese Akteure neigen dazu, Daten darüber zu erheben, wie Nutzerinnen und Nutzer ihr Smart-TV-Gerät nutzen, welche Fernsehprogramme betrachtet werden, wann und wohin umgeschaltet wird oder welche Filme oder Musiktitel über angeschlossene USB-Sticks oder Festplatten aufgezeichnet oder wiedergegeben werden.

Möglich macht dies u.a. der sog. „HbbTV"-Standard („Hybrid Broadcast Broadband Television"), der von immer mehr Geräten unterstützt wird und Fernseh- und Internettechnik miteinander verbindet. Dabei wird über das Fernsehbild eine unsichtbare Webseite gelegt, auf der TV-Sender oder Dienstanbieter die Möglichkeit haben, in

das TV-Bild Informationen aus dem Internet einzublenden. So können Auswahlmenüs oder Verweise zu weiterführenden Inhalten angezeigt werden, die der Zuschauer über spezielle Funktionstasten auf seiner Fernbedienung anwählen kann. Dies funktioniert genauso, wie wenn mit der Maus auf einen Link oder ein Bild im Internet geklickt wird. Weiterhin können im internen Web-Browser des Gerätes Cookies gesetzt oder andere Technologien zur dauerhaften Identifizierung und Wiedererkennung angewandt werden (sog. „Tracking").

Bei Smart-TV-Geräten findet somit eine zunehmende Personalisierung und Übertragung personenbezogener Daten über das Internet statt, darauf aufbauend eine Profilbildung über Geräte oder deren Nutzerinnen und Nutzer. Datenschutzaspekte haben hier bislang zu wenig Beachtung gefunden. Von den deutschen Datenschutzbehörden wurde daher gemeinsam die „Orientierungshilfe Smart-TV" entwickelt und im September 2015 veröffentlicht. Sie definiert, was aus Datenschutzsicht zulässig ist und wo das Datenschutzrecht Grenzen setzt. Gleichzeitig dient die Orientierungshilfe den Aufsichtsbehörden als Prüfkatalog, an dem sich Hersteller von Smart-TV-Geräten, aber auch TV- und Rundfunkanstalten als Anbieter von HbbTV-Diensten oder externe Anbieter von Apps oder Smart-TV-Diensten zukünftig werden messen lassen müssen. Die Orientierungshilfe Smart-TV kann hier heruntergeladen werden:
https://www.datenschutz-hamburg.de/uploads/media/Orientierungshilfe_Datenschutzanforderungen_an_Smart-TV-Dienste.pdf

Begleitend zur Entwicklung der Orientierungshilfe hat das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) Ende 2014 im Auftrag der jeweils zuständigen Aufsichtsbehörden eine technische Prüfaktion durchgeführt, bei der Smart-TV-Geräte von 13 Herstellern, die etwa 90 Prozent des deutschen Marktes abdecken, daraufhin untersucht wurden, welche Daten bei der Nutzung der Geräte fließen. Das Ergebnis zeigte Verbesserungsbedarf vor allem im Bereich Nutzeraufklärung sowie Defizite beim Einholen von Einwilligungen für bestimmte Dienste oder Datenübermittlungen. Ferner wurde festgestellt, dass viele Geräte unzureichende Möglichkeiten zur Kontrolle ihrer umfassenden Funktionalitäten bieten. Dies ist vor allem wichtig, wenn sensible Hardware wie Kameras, Mikrofone oder Sensoren für Helligkeit oder Raumtemperatur verbaut sind. Das damit verbundene Risikopotential wurde im April 2015 von Forschern der Technischen Universität Berlin eindrucksvoll demonstriert, als diese von einem Lieferwagen auf der Straße aus über ein manipuliertes TV-Signal einem Smart-TV-Gerät in einem in der Nähe liegenden Haushalt zunächst Schad-Software unterschoben. Nachdem das Gerät die Software eigenmächtig installiert hat, konnten sich die Forscher live aufschalten und über Kamera und Mikrofon die (eingeweihten) Testpersonen unbemerkt im eigenen Wohnzimmer ausspionieren.

Die Ergebnisse der Smart-TV-Prüfung des BayLDA wurden den beteiligten Geräteherstellern mitgeteilt, ebenso der jeweils zuständigen Aufsichtsbehörde. Auch der

HmbBfDI ist für einen bekannten internationalen Gerätehersteller zuständig, da dieser seinen Deutschlandsitz in Hamburg hat. Von dem Unternehmen war bereits im Vorfeld der Prüfung Kooperationsbereitschaft gezeigt worden, und auch nach Vorliegen der Ergebnisse wurde die Absicht bestätigt, die festgestellten Schwächen im Bereich Nutzeraufklärung und -information zügig im Rahmen der Produktfortentwicklung zu beheben.

E-GOVERNMENT, IT-VERFAHREN UND INFRASTRUKTUR DER FHH VI.

1. E-Government und IT-Verfahren 160
2. Infrastruktur, Bauen, Wohnen, Energie 179

1. E-Government und IT-Verfahren

1.1. Sicherheit der Kommunikation (NGN, VoIP in der FHH)

Die Umstellung der Telekommunikation von Analogtechnik bzw. ISDN auf paketbasierende IP-Technik bringt neue Funktionalitäten, aber auch neue Risiken. Faxen hat damit seinen Sicherheitsvorteil gegenüber unverschlüsselter E-Mail-Kommunikation verloren.

Bereits im letzten Tätigkeitsbericht (24. TB, II 5) hatte der HmbBfDI kritisch Stellung zu der Umstellung des Telekommunikationsnetzes der FHH von Analog- bzw. ISDN-Technik auf paketbasierende IP-Übertragung geäußert, welche von der Finanzbehörde im Zeitraum 2012 bis 2014 unter dem Namen „NGN" für „Next Generation Network" umgesetzt wurde. Durch die neue Technologie wurden neue Funktionen an den Telefonen in den Dienststellen verfügbar, die aus Datenschutzsicht bedenklich waren. Hauptkritikpunkt war jedoch, dass das NGN-System ohne Übertragungsverschlüsselung realisiert wurde.

IP-Kommunikation – die Abkürzung „IP" steht für „Internet Protokoll" – bedeutet, dass Telekommunikationsverbindungen nicht durch leitungsmäßiges Zusammenschalten einzelner Endgeräte hergestellt werden, über welche dann der Kommunikationsfluss läuft, sondern die zu übertragenden Telekommunikationsinhalte (Sprachdaten, aber auch Telefaxe) werden digitalisiert und in Form kleiner Datenpakete, jeweils versehen mit einer Zieladresse, auf den Weg über ein Netzwerk geschickt. Das Netzwerk kann ein internes Firmen- oder Behördennetz sein, es kann aber auch das Internet sein. Die Übermittlung von Telekommunikationsinhalten gleicht damit der Übertragung von E-Mails oder Webseiten. Je nachdem, ob es sich beim Inhalt um Sprachdaten handelt, spricht man von „Voice over IP" (kurz „VoIP") bzw. bei Faxdaten von „Fax over IP" (kurz „FoIP").

Durch Reduktion der Telekommunikationsdaten auf Datenpakete, die praktisch unkontrolliert durch ein Netzwerk oder das Internet reisen, ergeben sich für Telekommunikationsinhalte die gleichen Risiken wie bei der E-Mail-Kommunikation: jedes Datenpaket kann an einer Zwischenstation abgefangen werden, der Inhalt kann verändert werden oder das Datenpaket geht verloren. Gegen den Paketverlust enthält das Internetprotokoll Schutzmechanismen, indem Pakete bei Bedarf erneut angefordert und übertragen werden. Gegen Risiken wie Abfangen, Mitschneiden oder Manipulieren von Datenpaketen müssen jedoch Sender und Empfänger selbst Schutzmaßnahmen ergreifen.

Die effektivste Methode hierfür ist die Verschlüsselung der Datenpakete. Techniken hierzu gibt es für die E-Mail-Kommunikation seit Jahrzehnten, allerdings haben diese trotz der bekannten Überwachung des Internets durch Geheimdienste und sonstige

Organisationen bis heute nur eine geringe Verbreitung. Stattdessen haben sich die Nutzerinnen und Nutzer von E-Mails im geschäftlichen wie im privaten Umfeld an die oft kolportierte Vorstellung gewöhnt, dass E-Mails „so vertraulich wie Postkarten" sind und sensible Inhalte aus Gründen der Vertraulichkeit besser per Telefax übermittelt werden. Mit Umstellung der Telekommunikation auf IP-Übertragung unterscheiden sich E-Mail- und Telekommunikationsdaten faktisch nicht mehr voneinander. Wird IP-Telekommunikation unverschlüsselt übertragen, wandern die Sprach- oder Faxdaten genau wie E-Mails offen lesbar durch das Netzwerk oder Internet und können an jedem Vermittlungs- oder Knotenpunkt ausgelesen, mitgeschnitten oder verändert werden.

Die bisherige Auffassung, vertrauliche Inhalte besser zu faxen als per E–Mail zu versenden, ist damit überholt und sollte schnellstens aus den Köpfen verbannt werden. Faxen ohne durchgängig verschlüsselte (="Ende-zu-Ende") IP-Übertragung bietet keinen Sicherheitsvorteil zu einer unverschlüsselten E-Mail und keinen höheren Grad an Vertraulichkeit oder Integrität für den übertragenen Inhalt. Dies gilt vor allem vor dem Hintergrund, dass alle großen Betreiber der deutschen Telekommunikationsnetze wie Telekom, Telefonica oder Vodafone bereits mit der Umstellung ihrer Leitungsnetze auf IP-Technologie begonnen haben und dies in den wenigen Jahren komplett abschließen wollen.

Auch das interne IP-Telekommunikationsnetzwerk der FHH, das NGN-System, wird ohne Übertragungsverschlüsselung betrieben. Dabei bestünde die Möglichkeit, das Netzwerk vom Systemhersteller auf Verschlüsselung umrüsten zu lassen, was jedoch aus Kostengründen nicht umgesetzt wird. Das aktuell im Probebetrieb befindliche, zukünftige Videokonferenzsystem der FHH soll ebenfalls ohne Übertragungsverschlüsselung betrieben werden. Dabei ließe sich diese Schutzmaßnahme sogar ohne Zusatzkosten realisieren, alleine durch Änderung der Systemkonfiguration.

Der HmbBfDI wiederholt daher die bereits im letzten Tätigkeitsbericht geäußerte Forderung (24. TB, II 5) an die Finanzbehörde, die zur Diensterbringung bereitgestellten Kommunikationssysteme mit Übertragungsverschlüsselung nachzurüsten. Die Kosten hierfür werden u.a. dadurch kompensiert, dass - nachdem das Faxen als nicht mehr vertraulich anzusehen ist - alle Korrespondenz mit personenbezogenem oder anderweitig vertraulichem Inhalt an externe Stellen oder an Bürgerinnen und Bürger ab sofort nur noch per Briefpost erfolgen sollte.

Für vertrauliche Kommunikation innerhalb der FHH steht mit der Erweiterung RMS ("Rights Management System", siehe VI 1.4) für Outlook und Office-Dateien ein sicherer Kommunikationskanal zur Verfügung. Die Funktionalität von RMS wird jedoch nach Erfahrung des HmbBfDI bislang eher verhalten genutzt, u.a. da Dateitypen wie z.B. PDF nicht unterstützt werden und bei zu restriktiver Anwendung der prinzipiell sinnvollen Berechtigungssteuerung tatsächlich Einschränkungen für den praktischen Dienstbetrieb auftreten können.

1.2 Umgang mit Apps und Mobilgeräten in der FHH

Die dienstliche Nutzung von Smartphones und Tablets in der FHH gefährdet die Sicherheit der Daten, die von und über Bürger oder zu politischen Entscheidungen verarbeitet werden. Ferner ermöglicht der unkritische Umgang mit Apple und Google eine Nutzerausforschung durch diese US-Konzerne.

Ein „Trend" in den letzten Jahren in der IT-Branche und in unzähligen Fachmedien und -veranstaltungen war „BYOD" („Bring Your Own Device"). Die Idee dahinter ist, dass Mitarbeiterinnen und Mitarbeiter, anstatt vom Arbeitgeber ein Mobiltelefon oder Tablet zu erhalten, ein eigenes Gerät zur Verfügung stellen und dieses auch für berufliche bzw. dienstliche Zwecke nutzen. Von Herstellern und Beraterfirmen werden hierfür zahlreiche Argumente geliefert, wie Kostenersparnis für den Arbeitgeber, da der Aufwand für Beschaffung und Entsorgung von Geräten entfällt. Weiterhin würde Mitarbeitermotivation und -performance steigen, wenn diese neben dem privaten Smartphone kein zusätzliches Arbeitsgerät mitführen müssen, sondern Beruf und Privatleben mit einem einzigen Gerät abdecken können.

Aus Datenschutzsicht lassen sich an diesem Konzept keine vernünftigen Aspekte finden. Der Arbeitgeber gibt die aktive Steuerung der von Mitarbeitern genutzten Hardware auf, was zu einem Wildwuchs an Geräten, Betriebssystemen und Systemversionen führt und in der Folge zu einem Verlust an Kontrolle und Administrationsfähigkeit. Ferner ergeben sich zahlreiche rechtliche Problemstellungen, da berufliche bzw. dienstliche Daten auf privaten Geräten von Mitarbeitern verarbeitet werden. Zur Eindämmung der Risiken muss der Arbeitgeber daher Schutzmaßnahmen ergreifen und vorschreiben, z.B. Einschränken von Berechtigungen oder Vorgabe von zu nutzenden oder verbotenen Anwendungen. Es besteht jedoch die Gefahr, dass Mitarbeiter diese Vorgaben ignorieren oder umgehen, weil dadurch das Nutzungsrecht am eigenen Gerät beschränkt wird. Dies zeigt die häufige Verwendung von Messenger-Apps wie WhatsApp auf dienstlich genutzten Geräten. WhatsApp widerspricht aufgrund der bei Installation stattfindenden Übermittlung aller auf dem Gerät gespeicherten Telefonnummern an den Anbieter in den USA nicht nur deutschen Datenschutzvorgaben, sondern vermutlich den meisten IT- und Sicherheitsrichtlinien deutscher Unternehmen oder Behörden.

Als weiteres Problem kommt hinzu, dass aktuelle Smartphones und Tablets nur sinnvoll verwendet werden können, wenn ein Nutzerkonto beim Hersteller des Betriebssystems eingerichtet ist. Es sind im Moment zwei Unternehmen, die rund 90 Prozent des Marktes mobiler Geräte abdecken: Apple und Google. Ein iPhone oder iPad mit dem Betriebssystem iOS lässt sich ohne eine auf dem Gerät hinterlegte „Apple-ID", die der Nutzer durch Offenlegen seiner persönlichen Daten bei Apple beantragen muss, nur

eingeschränkt nutzen. Optionen wie das Hinzufügen von Apps oder die aus Sicherheitsgründen wichtige Versorgung mit Software-Updates stehen ohne Apple-ID nicht zur Verfügung. Für Geräte mit dem Betriebssystem Android gilt dies analog. Android kommt u.a. in den Smartphones und Tablets von HTC, Huawei, LG, Motorola, Samsung oder Sony zum Einsatz, ist jedoch eine Entwicklung von Google und daher sehr stark auf das Online-Dienstangebot dieses Unternehmens ausgerichtet. Für fast alle Android-Geräte gilt, dass ohne „Google-Konto" nur eine reduzierte Nutzung möglich ist. Immerhin erlaubt Android im Gegensatz zu iOS die direkte Installation von Apps und lässt neben dem „Google Play Store" auch andere App-Stores für den Bezug von Apps zu.

Bei beiden Betriebssystemen findet, sobald ein Nutzerkonto eingerichtet ist, ein permanenter Datenaustausch mit den Servern von Apple bzw. Google statt. Ferner wird von den beiden Unternehmen über jede Nutzerin und jeden Nutzer ein Profil angelegt und sukzessive verfeinert. Apple bzw. Google kennt die Person hinter einem Nutzerkonto bald besser als diese sich selbst, da über das permanent mitgeführte Mobilgerät das persönliche Verhalten und – bei aktivierter Standortermittlung – auch die Aufenthaltsorte erfasst und gespeichert werden. Aus dieser Datensammlung sind leicht individuelle Gewohnheiten abzulesen. Der Nutzer wird nicht nur transparent, sondern berechenbar. All diese Informationen über die Person des Gerätenutzers stehen – davon ist spätestens seit den Snowden-Enthüllungen auszugehen - bei Bedarf auch den amerikanischen Geheimdiensten zur Verfügung.

Angesichts der engen Anbindung aktueller Mobilgeräte an US-Unternehmen, die, wie der EuGH in seiner Safe-Harbor-Entscheidung letztlich bestätigt hat, einer umfassenden Überwachung der elektronischen Kommunikation unterliegen, sollte man von Unternehmen und Behörden eigentlich erwarten, dass ein Gegensteuern zu dem Risiko der Ausforschung und Überwachung von Mitarbeitern versucht wird. Zumal dies auch für die eigene Organisation eine Gefährdung darstellen kann. Die aktuelle Praxis in der FHH widerspricht dieser Erkenntnislage: nachdem die Finanzbehörde (trotz der Kritik des HmbBfDI, siehe 24. TB, II 2) auf den BYOD-Zug aufgesprungen ist und die Nutzung privater Geräte zu dienstlichen Zwecken erlaubt hat, werden von dort zunehmend bedenkliche und unkritische Vorgaben erlassen, welche die Mitarbeiterinnen und Mitarbeiter der FHH in eine Abhängigkeit von Apple und Google bringen.

So enthalten die Benutzeranleitungen mehrerer Dienst-Apps für FHH-Mitarbeiter, wie z.B. „DME Excitor" (VI 1.3) oder für den sog. „WLAN-Komfort-Zugang" die Vorgabe, die jeweilige App aus dem App-Store von Apple bzw. Google zu beziehen und die dortigen Nutzungsbedingungen einfach per Klick zu bestätigen. Eine alternative Bezugsmöglichkeit für die Apps wird nicht dargestellt.

Von FHH-Mitarbeitern, die ein dienstliches Gerät bekommen, wird daher verlangt, im Rahmen der Dienstausübung den Nutzungsbedingungen dieser Unternehmen freiwillig zuzustimmen.

Auch Bürgerinnen und Bürger werden von der FHH an Apple oder Google verwiesen. So erstellen immer mehr Behörden oder Tochterorganisationen der FHH eigene Apps und bieten diese der Öffentlichkeit an, beispielsweise die „Hamburg-App“ oder die „HVV-App“. Diese Apps werden jedoch ausschließlich über „iTunes“, den App-Store von Apple bzw. den „Play-Store“ von Google bereitgestellt.

Die aktuelle Praxis im Umgang mit Mobilgeräten und die selbstverständliche Nutzung der App-Stores von Apple oder Google sollte aus Sicht des HmbBfDI dringend überdacht werden. Die FHH unterstützt damit nicht nur die Monopolstellung der US-Konzerne Apple und Google und deren Marktbedingungen, sondern gefährdet auch die Privatsphäre der Mitarbeiter. Vor allem für Mitgliederinnen und Mitglieder des Senats oder Mitarbeiter bzw. Schlüsselpersonen, die wichtige politische oder wirtschaftliche Entscheidungen für die Stadt oder das Land Hamburg treffen, besteht das akute Risiko, dass sie über ihr Profil bei Apple oder Google ausgeforscht und so für amerikanische Geheimdienste berechenbar oder auch manipulierbar werden.

Ebenso besteht für Bürgerinnen und Bürger, die Apps der FHH nutzen wollen, keine andere Möglichkeit, als sich bei den US-Konzernen zu registrieren. Dafür ist zumindest für Android keine Notwendigkeit erkennbar. Da das Betriebssystem die Möglichkeit der direkten Installation vorsieht, sollten Android-Apps der FHH neben der Bereitstellung im Play-Store gleichzeitig auf einem Server der Stadt als Datei-Download angeboten werden. Dieser in der Vergangenheit übliche und sicher gestaltbare (z.B. mit TLS-Verschlüsselung) Weg der Software-Verteilung sollte nicht leichtfertig aufgegeben werden, erst recht nicht vom öffentlichen Sektor. Dass US-Konzerne mit ihrer Strategie der Schaffung monopolistischer Märkte und Strukturen Erfolg haben und auf diese Weise immer mehr Kontrolle über Nutzerinnen und Nutzer mobiler Geräte aufbauen und an sich ziehen, sollte durch die zu besonderer Neutralität verpflichteten Stellen nicht unterstützt werden.

1.3 DME Excitor - Sensible Daten auf unsicheren Geräten?

Mobile Geräte, bei denen Sicherheit nicht erstes Designprinzip ist, werden weiterhin zur Datenverarbeitung auch bei hohem Schutzbedarf genutzt. Während die Geräte schon über drei Jahre im Einsatz sind und die Gefährdungen deutlich zugenommen haben, sind wichtige Themen immer noch nicht zufriedenstellend bearbeitet.

Seit Juli 2012 hat der IT-Dienstleister Dataport mit der Lösung „DME Excitor“ „Outlook für mobile Geräte“ zunächst für Geräte mit IOS und ab April 2013 auch für Android im Auftrag der Finanzbehörde in der FHH umgesetzt. 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 (BYOD - „Bring your own device“, vgl. VI 1.2) sein.

Die DME-Lösung stellt sicher, dass die Daten, die immer als Kopie aus der Exchange-Installation auf das mobile Geräte übertragen werden, auf dem gesamten Weg verschlüsselt sind und auch auf dem mobilen Gerät verschlüsselt gespeichert werden.

Im November 2014 haben wir gegenüber der Finanzbehörde eine Stellungnahme abgegeben.

- Dort gingen wir von einem flächendeckenden Rollout des Outlook Add-In RMS (Rights Management System) in der FHH aus, der allen Postfachnutzern die Möglichkeit einräumt, sensible Mails zu schützen (vgl. VI 1.4). In der DME-Lösung werden geschützte Mails nicht sichtbar. Diese technische Maßnahme zum Schutz der sensiblen Daten auf mobilen Geräten greift nur, wenn die Beschäftigten beim Versand von Mails mit sensiblem Inhalt RMS auch nutzen. Einheitlichkeit in den Behörden könnten Hinweise der Finanzbehörde erzeugen. Leider setzt die Finanzbehörde ihre Ankündigung, Hinweise zur verpflichtenden Nutzung von RMS beim Versand von Mails mit sensiblem Inhalt zu erstellen, nicht um. Die Nutzung bleibt jedem einzelnen Anwender somit überlassen.

- Wir forderten die Überarbeitung der unvollständigen Risikoanalyse. Die Finanzbehörde hat die Überarbeitung mit der Erstellung der Risikoanalyse zum „Community Cloud Mail Service (CCMS) verknüpft (vgl. VI 1.5). CCMS ist inzwischen produktiv, die Unterlagen sind weiterhin lückenhaft und unvollständig. Die überarbeitete Risikoanalyse bezogen auf DME Excitor liegt uns weiterhin nicht vor.

- Wir baten um Beteiligung bei der Gestaltung des Penetrationstestes. Unsere Beteiligung wurde nicht möglich gemacht. Die zusammengefassten und interpretierten Ergebnisse erhielten wir ein halbes Jahr nach Abschluss des Testes. Wir behalten uns vor, die für uns offenen Punkte in einer erweiterten Prüfung zu bewerten.

- Die PC-Richtlinie schreibt unter Ziffer 5 (1) vor, dass auf dienstlich zur Verfügung gestellten Rechnern grundsätzlich nur dienstlich beschaffte Software installiert und verwendet werden darf. Wir forderten, die Installation von nicht freigegebener Software auf dienstlichen mobilen Geräten zu unterbinden, weil andernfalls gegen IT-Richtlinien der FHH verstoßen wird. Die Finanzbehörde hält jedoch an der Installationsmöglichkeit nicht freigegebener Software auf dienstlichen Geräten unter Hinweis auf moderne Nutzungskonzepte fest. Sie hat im Januar 2015 angekündigt, die PC- und die Freigabe-Richtlinie entsprechend zu verändern. Auf Nachfrage im November

2015 erfuhren wir, dass die Änderung der IT-Vorschriften sich aufgrund interner Abstimmungen noch weit in das nächste Jahr hinziehen wird.

- Um die DME-App für Android-basierte 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.
  Wir forderten eine Registrierungsmöglichkeit ohne Nutzung persönlicher Daten der Beschäftigten.
  Die Finanzbehörde überlässt die Entscheidung zur Registrierung den Anwenderinnen und Anwendern und wird dazu weder Vorgaben machen noch eine alternative Registrierungsmöglichkeit anbieten.

Das CERT Nord, das für die Dataport-Trägerländer Einschätzungen für Gefährdungen im Bereich der Informationssicherheit vornimmt, hat in seinem Newsletter vom November 2015 festgestellt, dass Smartphones immer mehr zum Risikofaktor werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) kommt in seinem „Bericht zur Lage der IT-Sicherheit in Deutschland 2015“ auch zu diesem Ergebnis. Smartphones werden zunehmend das Ziel von Angriffen und Schadsoftware. Das CERT Nord empfiehlt

- die Nutzung eines Virenschutzes beim Einsatz von mobilen Geräten und den ausschließlichen Einsatz von Geräten, für die auch regelmäßig Sicherheitsupdates herausgegeben werden.
  Ein Großteil der eingesetzten Geräte sind IOS-Geräte, für die es faktisch keinen Virenschutz gibt und Samsung-Smartphones, für die es trotz gravierender bekannter Sicherheitslücken im Betriebssystem keine Sicherheitsupdates vom Hersteller gibt.

- die Nutzung eines MDM (Mobile Device Management), um die Installation von Apps zentral steuern zu können (die Nutzung eines MDM zur Sicherstellung der Richtlinien-Konformität von mobilen Geräten entspricht nach Ansicht des BSI dem Stand der Technik).
  Die Finanzbehörde hält den Einsatz eines MDM nicht für erforderlich. Diese Einschätzung hat sie uns gegenüber wiederholt bestätigt.

Grundsätzlich schätzen wir den Einsatz von Smartphones für dienstliche Aufgaben bei den heutigen besonderen Gefahren für mobile Endgeräte als sehr risikoreich ein. Ohne einen besonderen Schutz, insbesondere ein MDM, ohne durchgängigen Schutz vor Malware und ohne den Einsatz von Geräten, für die es zeitnah Sicherheitsaktualisierungen gibt, empfehlen wir daher DME Excitor nur zu nutzen, wenn gewährleistet werden kann, dass keine Daten mit hohem Schutzbedarf auf dem Gerät verarbeitet werden.

1.4 Sicherheit der E-Mail-Kommunikation der FHH – ein Schritt vor – mindestens ein Schritt zurück

Die flächendeckende Ausstattung der Arbeitsplätze mit Verschlüsselungssoftware für die interne E-Mailkommunikation ist immer noch nicht erreicht. Bei der Kommunikation nach außen wird seit Jahren der Stand der Technik nicht eingehalten.

Interne E-Mail-Kommunikation der FHH

Bereits im 24. Tätigkeitsbericht haben wir über diesen Dauerbrenner bei der FHH berichtet (vgl. 24. TB II 4). Vor dem Hintergrund der inhaltlichen Auseinandersetzung haben wir ab Mitte März 2014 die aktuelle IT-Lösung der E-Mail-Kommunikation der FHH geprüft, die die Finanzbehörde auf der Basis von Outlook/Exchange insbesondere für alle Behörden und Ämter betreibt. Schwerpunkt der Prüfung sind insbesondere die Möglichkeiten für die Administration, auf die Exchange-Server und die darauf verarbeiteten personenbezogene Daten zuzugreifen, sowie der Schutz gegen unberechtigte Zugriffe.

Wir mussten feststellen, dass die Finanzbehörde vor der Entscheidung über die Einrichtung des Verfahrens keine Risikoanalyse erstellt hat und somit gegen die Anforderungen von § 8 Abs. 4 Hamburgisches Datenschutzgesetz (HmbDSG) verstoßen hat. Aus der Schutzbedarfsfeststellung der Finanzbehörde geht hervor, dass das Verfahren lediglich auf normalen Schutzbedarf ausgerichtet ist. Diese Bewertung verkennt, dass über die E-Mail-Kommunikation auch häufig sensible personenbezogene Daten verarbeitet werden und bei der E-Mail-Kommunikation mit Externen das Fernmeldegeheimnis zu wahren ist. Aus unserer Sicht sind dies deutliche Belege dafür, dass das IT-Verfahren auf einen hohen Schutzbedarf ausgerichtet werden sollte.

Die E-Mails werden innerhalb des FHH-Netzes zwischen Client und Exchange-Server nur transportverschlüsselt. Auf dem Server selbst sind die E-Mails jedoch unverschlüsselt. Die Prüfung hat ergeben, dass die Personen mit Exchange-Administrationsberechtigungen bei Dataport mit wenigen Klicks in kurzer Zeit Zugriff auf die Inhalte nehmen können. Ein solcher Zugriff ist zwar durch organisatorische Regelungen geregelt, er wird aber in automatisiert auswertbaren Protokollen nicht festgehalten. Nur in den Videoprotokollen, die von allen Administrationstätigkeiten gemacht werden, kann der Zugriff nachvollzogen werden. Diese Videoprotokolle werden jedoch keiner regelhaften Stichprobenkontrolle unterzogen. Nur bei einem konkreten Anlass und bei einer zeitlichen Angabe, wann der Zugriff stattgefunden haben könnte, besteht die Chance, einen möglichen Missbrauch aufzudecken oder auch den Administrationsberechtigten vor unberechtigtem Verdacht zu schützen.

Microsoft unterstützt nicht das Speichern von Exchange-Datendateien auf verschlüs-

selten Datenträgern in verschlüsselnden Dateisystemen (Encrypting File Systems, EFS). Um einem sich daraus ergebendem Sicherheitsrisiko entgegenzuwirken empfiehlt Microsoft:

> *„Damit die Sicherheit der Exchange-Datendateien gewährleistet ist, empfiehlt es sich, den unbefugten Zugriff auf den Computer mit Exchange zu verhindern und Nachrichtendaten mithilfe des S/MIME-Nachrichtenformats zu verschlüsseln."*

Als Reaktion auf die laufende datenschutzrechtliche Prüfung hat die Finanzbehörde Ende April 2014 angekündigt, zwar nicht auf eine Ende-zu-Ende-Verschlüsselung mit dem verbreitete Verfahren S/MIME oder PGP zu setzen, aber an allen Arbeitsplätzen der FHH das Outlook Add-In RMS (Rights Management System) zu nutzen, mit dem zumindest innerhalb der FHH dann eine Ende-zu-Ende verschlüsselte Kommunikation möglich ist. Mit RMS wird der Mail-Body und insbesondere Anhänge im Format „docx" sicher verschlüsselt. Anhänge in nicht Microsoft-spezifischen Formaten werden mit RMS zugriffsgeschützt übertragen. In einer zukünftigen Version sollen auch Anhänge im pdf-Format verschlüsselt werden. Es ist als Schritt nach vorne zu werten, dass nunmehr alle Arbeitsplätze mit dem Outlook-Add-In RMS ausgestattet werden sollen und auch im Juni 2014 ein entsprechender Beschluss im Architekturboard der FHH gefasst wurde, der über die IT-Architektur-Richtlinie bindende Wirkung für alle Behörden und Ämter hat. Gleichwohl mussten wir feststellen, dass im Bereich der Behörde für Inneres und Sport die Polizei angekündigt hat, dass sie dieser Verpflichtung der Einführung nicht nachkommen wird. Auch haben wir bei der Prüfung des Landesbetriebs Verkehr im Oktober 2015 festgestellt, dass noch kein Arbeitsplatz ausgestattet worden ist. Wir werden uns mit Nachdruck dafür einsetzen, dass dies nun unverzüglich bei allen Behörden und Ämtern geschieht, so wie es die Senatsvertreter im Unterausschuss Datenschutz der Bürgerschaft am 14.05.2014 bereits für Herbst 2014 angekündigt haben (Protokoll der öffentlichen Sitzung des Unterausschusses „Datenschutz und Informationsfreiheit" Nr. 20/7, S. 4).

Neben der technischen Vorbereitung durch die Ausstattung aller Arbeitsplätze mit dem Outlook-Add-In RMS ist eine organisatorische Regelung von großer Bedeutung, die die verpflichtende Nutzung insbesondere für hohen Schutzbedarf vorschreibt. In der Stellungnahme zu unserem Prüfbericht hat die Finanzbehörde Ende 2014 noch angekündigt, solch eine verbindliche Regelung zu erarbeiten. Mittlerweile ist sie jedoch wieder mindestens einen Schritt zurückgegangen und führt aus, entgegen der konkreten Ankündigung keine verbindlichen Vorgaben für die Nutzung von RMS machen zu wollen. Damit hat sie einen jahrelang bestehenden Konsens, dass bei hohem Schutzbedarf zumindest dann eine Ende-zu-Ende Verschlüsselung erforderlich ist, wenn der Aufwand dafür nicht unverhältnismäßig ist, gebrochen. Wie wichtig eine solche Vorgabe wäre, belegt die Prüfung des IT-Verfahrens „Obacht – Gewalt unter 21 Jahren" bei dem neben der Polizei, das Familieninterventionsteam der Behörde für Arbeit, Soziales Familie und Integration, das Landesinstitut für Lehrerbildung und

Schulentwicklung der Behörde für Schule und Berufsbildung, die Staatsanwaltschaft sowie die Jugendbewährungshilfe und die Jugendgerichtshilfe des Bezirksamts Eimsbüttel im Zuge der Bearbeitung einzelner Fälle häufig sensible personenbezogenen Daten per E-Mail austauschen. Für die Nutzung dieser Kommunikationsform hat die Koordinierungsstelle, die der Polizei zugeordnet ist, keine Vorgaben gemacht. Bei der schriftlichen Befragung der zugriffsberechtigten Personen hat keine der Personen, die regelhaft E-Mail mit personenbezogenen Daten versenden, angegeben, dass sie die Möglichkeit der durchgehenden Verschlüsselung mit RMS nutzen.

Diese Einschätzung verkennt jedoch, dass nach § 8 HmbDSG die Vertraulichkeit der Daten zu gewährleisten ist und zum Schutz der Vertraulichkeit die erforderlichen Maßnahmen zu treffen sind, die in einem angemessenen Verhältnis zur Schutzwürdigkeit der Daten stehen. Hier ist zum einen die leichte Zugriffsmöglichkeit der Administratorinnen und Administratoren zu sehen und die geringe Wahrscheinlichkeit, dass ein unberechtigter Zugriff aufgedeckt wird. Zum anderen ist der Aufwand für eine Verschlüsselung denkbar gering, da alle Arbeitsplätze mit dem Outlook-Add-In ausgestattet sind. Es bedarf nur zweier zusätzlicher Klicks durch die Sachbearbeitung, um die Ende-zu-Ende-Verschlüsselung kurz vor dem Absenden auszulösen. Damit wäre auch der Festlegung in der §93-Vereinbarung „Bürokommunikation" Genüge getan, die eine Verschlüsselung beim Versenden sensibler Daten vorschreibt. Hier werden wir weiter die dicken Bretter bohren, bis eine datenschutzgerechte Lösung realisiert ist.

E-Mail-Kommunikation der FHH mit Externen

Bereits seit Dezember 2013 bemühen wir uns darum, dass bei der E-Mail-Kommunikation mit Externen außerhalb des FHH-Netzes die Transportverschlüsselung aktiviert wird. Mit StartTLS steht ein Verschlüsselungs-Verfahren mittels Transport Layer Security (TLS) zur Verfügung, das bereits 1999 spezifiziert wurde. StartTLS ist so ausgelegt, dass man die Transportverschlüsselung als zusätzliche Option nutzen kann, aber ein Kommunikationspartner, der die Verschlüsselung nicht unterstützt, weiterhin mit dem Server unverschlüsselt kommunizieren kann. Das TLS-Protokoll dient der Sicherstellung von Vertraulichkeit, Authentizität und Integrität bei der Übertragung von Daten in unsicheren Netzwerken. Neben der Absicherung der Auslieferung von Webseiten ist der sichere Transport von E-Mails ein bekannter Anwendungsfall. Beim Einsatz einer Transportverschlüsselung mittels TLS wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Bundesverwaltung das Protokoll TLS 1.2 in Kombination mit Perfect Forward Security als Mindeststandard vorgegeben. Das Ziel ist es, für diesen Anwendungsbereich einen zeitnahen und flächendeckenden Einsatz zu erreichen.

StartTLS wird von Microsoft Exchange seit Jahren unterstützt. Die Nutzung dieser Transportverschlüsselung ist weit verbreitet und als Stand der Technik einzustufen.

Nach § 8 Abs. 2 HmbDSG sind von der Daten verarbeitenden Stelle die technischen und organisatorischen Maßnahmen zu treffen, die geeignet sind, u.a. die Vertraulich-

keit der verarbeiteten personenbezogenen Daten zu gewährleisten. Dazu wurde in der Gesetzesbegründung ausgeführt, dass es dabei keiner ausdrücklichen gesetzlichen Festlegung bedarf, und dass Maßnahmen nach dem jeweiligen Stand der Technik zu treffen sind. Stand der Technik ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, der nach herrschender Ausfassung führender Fachleute das Erreichen des gesetzlichen Ziels gesichert erscheinen lässt. Verfahren, Einrichtungen und Betriebsweisen oder vergleichbare Verfahren müssen sich in der Praxis bewährt haben oder sollten – wenn dies noch nicht der Fall ist – möglichst im Betrieb mit Erfolg erprobt worden sein. Diese Merkmale treffen auf die Transportverschlüsselung nach dem Verfahren StartTLS zu, bei der nach herrschender Auffassung für E-Mails mit Daten, die einen normalen Schutzbedarf aufweisen, ein Mindestmaß an Schutz gewährleistet wird.

Spätestens mit dem Umzug in das neue Rechenzentrum RZ² wäre die Hardware-Voraussetzung durch die Bereitstellung einer ausreichenden Serverkapazität herzustellen gewesen, um für ein- und ausgehende E-Mails einen ausreichenden Schutz zu ermöglichen. Eine Verschiebung auf einen späteren Zeitraum ist nicht vertretbar. War im Frühjahr 2014 noch die Argumentation nachvollziehbar, dass im alten Rechenzentrum keine Ausweitung der Serverkapazitäten mehr erfolgen sollte, so ist die Begründung, StartTLS nunmehr erst mit der Einführung von Cloud Mail Service zu nutzen, nicht verständlich. Eine technische Begründung für diese weitere Verschiebung ist nicht ersichtlich. Dataport selber hatte mit E-Mail vom Februar 2014 darauf hingewiesen, dass noch ausreichend Zeit bis zum Umzug ins Rechenzentrum RZ² sei, ggf. die Serverkapazitäten anzupassen.

Auch Ende 2015 entsprechen die realisierten technischen Maßnahmen immer noch nicht den datenschutzrechtlichen Anforderungen. Der Fall zeigt exemplarisch, wie schwer es mitunter ist, selbstverständliche Belange des Datenschutzes auch gegenüber öffentlichen Stellen durchzusetzen. Sollte die Umsetzung nicht zeitnah erfolgen, wird dies zu einer Beanstandung durch den HmbBfDI führen.

Chronologie der Ereignisse:

Dezember 2013	Unsere Nachfrage beim Dienstleister Dataport ergibt, dass eine Transportverschlüsselung mit TLS nicht aktiviert ist. Ein Einsatz für die FHH ist jedoch möglich.
Februar 2014	Dataport teilt auf Nachfrage mit, dass bei der Planung des neuen Rechenzentrums RZ² die Anforderung TLS als Option mit berücksichtigt wird. Ein Planungstermin konnte von Dataport nicht genannt werden.
April 2014	Auf Nachfrage wurde von Dataport mitgeteilt, dass die Umstellung auf TLS noch in 2014 erfolgen wird.
Juli 2014	Der Umzug der laufenden Exchange-Anwendung der FHH ins neue Rechenzentrum ist erfolgt, ohne dass TLS aktiviert wurde.
November 2014	Im Rahmen der Prüfung des IT-Verfahrens Outlook/Exchange wird der Mangel aufgezeigt, dass bei der E-Mail-Kommunikation mit Externen der Stand der Technik nicht eingehalten wird. Die Finanzbehörde wird aufgefordert, TLS unverzüglich zu realisieren und binnen eines Monats einen Termin der Einführung mitzuteilen.
Dezember 2014	Die Finanzbehörde teilt mit, dass TLS mit der Einführung von Community-Cloud-Mail-Service im Laufe des 2. Quartals 2015 eingeführt wird.
April 2015	Die Behördenleitung der Finanzbehörde teilt auf Nachfrage mit, dass bis zum Ende des 2. Quartals 2015 CCMS produktiv gesetzt wird und damit auch die Transportverschlüsselung mit TLS realisiert wird.
August 2015	Die Finanzbehörde teilt mit, dass über die Einführung von CCMS im September 2015 beschlossen wird und die Migration und die Aktivierung von TLS sich bis ins 4. Quartal 2015 verschieben wird.
Ende Dezember 2015	Die Finanzbehörde und Dataport erklären, dass immer noch kein Termin zur Aktivierung von TLS feststeht.

1.5 Community-Cloud Mail Service – alles wolkig

Mit dieser Anwendung will die Finanzbehörde ein länderübergreifendes gemeinsames System einführen, ohne die Mandantentrennung einzuhalten. Die Migration der E-Mail-Anwendung in das produktive IT-System Community-Cloud-Mail-Service ist für Hamburg bereits abgeschlossen. Die erforderlichen datenschutzrelevanten Unterlagen liegen immer noch nicht vor.

Nachdem 2013 die Beratungen im IT-Planungsrat über die Machbarkeit eines nationalen Exchange-Dienstes „Cloud-E-Mail-Dienst" abgeschlossen waren und deutlich wurde, dass eine bundesweite Lösung vom IT-Planungsrat nicht weiter verfolgt wird, planten die Dataport-Trägerländer Schleswig-Holstein, Bremen und Hamburg eine Lösung für eine gemeinsam genutzte Infrastruktur zum elektronischen Mailverkehr, zur Terminverwaltung und zur Aufgabenplanung einzuführen. Dieses Messaging-System für diese drei Trägerländer von Dataport auf der Basis von Exchange 2013/Outlook trägt die Bezeichnung „Community Cloud Mail Service (CCMS)".

Die Datenschutzaufsichtsbehörden der Dataport-Trägerländer bemühen sich bei gemeinsamen IT-Verfahren und bei gemeinsam genutzter IT-Infrastruktur um eine enge inhaltliche Abstimmung untereinander. Zum Vorhaben CCMS wurden dazu aufgrund der vorliegenden Informationen Abstimmungsgespräche geführt, insbesondere zum ersten Entwurf „Architekturkonzept - High-Level-Design" und einem erstem Entwurf eines Mandantenkonzepts, dass jedoch zahlreiche Leerstellen aufweist. Die Finanzbehörde Hamburg hat uns eine Vielzahl von Unterlagen vorgelegt, die überwiegend einen unfertigen Stand haben. Dies gilt insbesondere für die datenschutzrechtlichen Aspekte der Spezifika der CCMS-Lösung. Viele Dokumente mit zentraler Bedeutung für eine Kontrolle der Einhaltung der gesetzlich geforderten technischen und rechtlichen Maßnahmen beinhalten nur Überschriften, erste Überlegungen oder Verweise auf Dokumente, die nicht einmal im Entwurfsstadium vorliegen. Aussagekräftige Unterlagen sind nicht zur Verfügung gestellt worden und daher ist die gesetzlich vorgesehene Vorabkontrolle nicht durchführbar. Die Aussagen der Finanzbehörde blieben auch bis zum Beginn der Migration in das neue Verfahren sehr wolkig, wenn es um die Frage ging, wann die datenschutzrelevanten Unterlagen bereitgestellt werden. Erst kurz vor dem Ende der Migration, als also schon ein Großteil der hamburgischen Nutzerinnen und Nutzer produktiv im neuen Verfahren arbeiteten, wurden uns Ende November 2015 die Unterlagen übermittelt.

Anforderungen an ein mandantengetrenntes IT-System

Die Datenschutzbeauftragten des Bundes und der Länder haben 2012 eine Orientierungshilfe „Mandantenfähigkeit" erarbeitet, die aus unserem Internetangebot abgerufen werden kann (*https://www.datenschutz-hamburg.de/news/detail/article/orientierungshilfe-mandantenfaehigkeit.html*). In dieser Orientierungshilfe sind die

technischen und organisatorischen Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur festgeschrieben. Ziel ist es, einen vergleichbar hohen Schutz der verarbeiteten Daten zu gewährleisten, wie das bei getrennten Verfahren der Fall ist.

Bei jedem IT-Verfahren ist zu gewährleisten, dass die Daten nur für den Zweck verarbeitet werden, für den sie erhoben wurden. Diese Trennungsgebot wird klassischer Weise durch getrennte IT-Installationen umgesetzt. Ein Austausch zwischen IT-Verfahren kann dabei nur über definierte Schnittstellen erfolgen. Um die Wirtschaftlichkeit in Rechenzentren zu erhöhen, wird verstärkt angestrebt, vergleichbare IT-Verfahren in einer gemeinsamen Infrastruktur zu betreiben. Um dies datenschutzgerecht umsetzen zu können, muss gewährleistet werden, dass die Trennung der Mandanten so erfolgt, dass alle Daten nur jeweils einem Mandanten zugeordnet sind und die Sachbearbeitung keinen Zugriff auf die Daten eines anderen Mandanten nehmen kann. Dieses muss durch technische Maßnahmen realisiert werden. Die Trennung allein durch Zugriffsrechte ist nicht ausreichend. Eine Datenübermittlung zwischen Mandanten muss ebenfalls über eine definierte Schnittstelle erfolgen. Falls keine Mandantentrennung gewährleistet ist, wird daraus ein gemeinsames IT-Verfahren, für das es nach § 11a Hamburgisches Datenschutzgesetz einer ausdrücklichen Zulassung durch eine Rechtsvorschrift bedarf.

Mandantenkonzept des CCMS

Der aktuelle Planungsstand zielt darauf ab, dass drei Ländermandanten und ein weiterer Mandant für den IT-Dienstleister eingerichtet werden. Der vorliegende Entwurf des Mandantenkonzepts geht davon aus, dass eine Öffnung für Kalender zumindest zwischen Hamburg und Schleswig-Holstein beabsichtigt ist. Die Öffnung für die Kalenderdaten führt nach Angaben der Finanzbehörde gleichzeitig dazu, dass auch E-Mailinhalte für Nutzerinnen und Nutzer des anderen Mandanten sichtbar geschaltet werden können. Diese Einstellung können alle Beschäftigten individuell vornehmen, sobald die Möglichkeit der gegenseitigen Einsichtnahme für Kalenderdaten mandantenweit oder zumindest behördenweit freigeschaltet wurde. Eine technische Hürde, die verhindern würde, dass Beschäftigte individuell entscheiden können, ob ihr Postfach für eine Nutzung aus einem anderen Mandaten freigegeben ist, besteht nicht. Es steht die gleiche Funktionalität der „Stellvertretung“ für die Exchange 2013/Outlook-Daten über Mandantengrenzen hinweg zur Verfügung, die auch innerhalb eines Mandanten besteht. Weder Freischaltung der E-Mail-Postfächer noch ein Zugriff auf diese aus einem anderen Mandanten wird protokolliert.

Durch die Öffnung der Frei/Gebucht-Zeiten werden somit auf Anwendungsebene lesende Zugriffe auf Kalenderinhalte und E-Mailinhalte eines anderen Mandanten möglich. Dies steht den Anforderungen der Orientierungshilfe „Mandantenfähigkeit“ der Datenschutzbeauftragten des Bundes und der Länder entgegen.

Die Migration der FHH in das CCMS soll im Januar 2016 abgeschlossen werden. Als Termin für die Migration der Outlook-Konten aus Bremen wurde zuletzt Anfang 2016 genannt. Der Umstieg in Schleswig-Holstein soll nach Aussage der Finanzbehörde anschließend erfolgen. Gemeinsam mit den beiden anderen betroffenen Landesdatenschutzbeauftragten werden wir uns weiterhin intensiv für eine datenschutzgerechte Lösung stark machen.

1.6 Keine Mandantentrennung im FHHportal umgesetzt

Für IT-Verfahren, die im FHHPortal betrieben werden, wird das Trennungsgebot nicht eingehalten.

Das FHHportal stellt zunehmend die Grundlage für behördeninterne und behördenübergreifende Zusammenarbeit dar. Rund 10.000 Beschäftigte nutzen das FHHportal aktiv für den Austausch von Informationen und die tägliche Arbeit mit Dokumenten. Es ist der Regelfall, dass alle IT-Nutzerinnen und -Nutzer der FHH einen Zugriff auf das FHHportal mit den darin für alle bereitgestellten Informationen haben. Zur Sicherung der Betriebssicherheit und gleichzeitig zur Erweiterung der Nutzungsmöglichkeiten wurde die Plattform zuletzt 2015 erneuert. Mit der Zusammenführung der Infrastrukturen für Zusammenarbeit und Intranet wurde eine einheitliche Informationsbasis für die Beschäftigten geschaffen, die das schnelle Auffinden der internen Informationen sicherstellt. In der Regel weisen derartige Dokumente keine personenbezogenen Daten von Bürgerinnen und Bürgern auf. Das FHHportal basiert auf der Microsoft Webanwendung Sharepoint.

Microsoft Sharepoint kann auch als Werkzeugkasten dazu herangezogen werden, um die Sachbearbeitung im Fachverfahren zu unterstützen. Der Schwerpunkt der Anwendung solcher Fachverfahren ist es aber, insbesondere personenbezogene Daten von Bürgerinnen und Bürgern oder die Daten der Beschäftigten der FHH zu verarbeiten. Dabei geht es regelhaft gerade nicht um die Bereitstellung von Informationen für viele. Für derartige Fachanwendungen ist wie auch sonst zunächst einmal die Frage nach den einschlägigen Rechtsgrundlagen zu beantworten. Zum einen wird aus diesen abgeleitet, welche Daten zu welchem Zweck verarbeitet werden dürfen. Zum anderen ist zu betrachten, ob ein automatisiertes Abrufverfahren nach § 11 Hamburgisches Datenschutzgesetz (HmbDSG) oder ein gemeinsames Verfahren nach § 11a HmbDSG eingerichtet werden soll, für die ein ausdrücklicher Erlaubnisvorbehalt durch eine Rechtsvorschrift besteht. Wenn eine solche Rechtsvorschrift für ein gemeinsames Verfahren nicht gegeben ist, ist das Trennungsgebot zu beachten, unabhängig davon, mit welcher Technik dieses Verfahren unterstützt werden soll. Dabei spielt es keine Rolle, ob es sich bei der IT-Lösung um eine Eigenprogrammierung oder eine Baukas-

tenlösung z.B. mit Sharepoint handelt. Es muss für ein solches Verfahren die Trennung in Mandanten gewährleistet werden, wenn eine IT-Infrastruktur genutzt werden soll, in der auch andere IT-Fachverfahren laufen (vgl. VI 1.5). Durch technische Maßnahmen muss sichergestellt werden, dass sowohl die Anwenderinnen und Anwender als auch die Daten nur genau einem Mandanten zugeordnet sind.

Wenn also ein Fachverfahren mit einer eigenständigen Sharepoint-Installation unterstützt wird, dem ausschließlich Nutzerinnen und Nutzer zugeordnet sind, die die Sachbearbeitung für dieses Verfahren betreiben, spielt die Mandantenfähigkeit keine Rolle. Wenn jedoch eine IT-Anwendung wie das FHHportal erweitert werden soll, um diese Installation als technische Grundlage und Werkzeugkasten auch für weitere Fachverfahren zu nutzen, müssen die Anforderungen der Orientierungshilfe Mandantenfähigkeit der Datenschutzbeauftragten des Bundes und der Länder eingehalten werden.

Dataport hat bereits 2012 in einem „Architektur und Betriebskonzept SharePoint Server 2010" differenziert die technischen Möglichkeiten zur Mandantentrennung beschrieben. Im Berichtszeitraum haben wir mit der Finanzbehörde die Anforderungen an die Mandantentrennung erneut beraten. Anlass war zum einen, dass die bestehende Infrastruktur des FHHportals für das IT- Fachverfahren der Polizei „Obachtverfahren – Gewalt unter 21 Jahren " genutzt werden sollte. Bei diesem Verfahren werden sensible personenbezogene Daten von unter 21-jährigen Personen produktiv verarbeitet, 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. Andererseits soll zukünftig auch für das IT-Verfahren der Senatskanzlei zur Unterstützung der Eingaben-Verarbeitung, das ebenfalls einen hohen Schutzbedarf hat, diese FHHportal-Infrastruktur nutzen.

Es wurde deutlich, dass die Anforderungen der Orientierungshilfe Mandantenfähigkeit sich nur umsetzen lassen, wenn für die unterschiedlichen Verfahren nur spezifische „Berechtigungsprovider" genutzt werden oder vergleichbare technische Maßnahmen ergriffen werden. Ein „Berechtigungsprovider" begrenzt die Menge der IT-Accounts, die zu einem Fachverfahren Zugriffsberechtigungen erhalten können. Auf diese Weise kann sichergestellt werden, dass die Berechtigten nur zu genau einem Mandanten gehören. Dies ist derzeit nicht der Fall. Dies hat zur Folge, dass innerhalb kürzester Zeit alle Nutzerinnen und Nutzer eine Zugriffsberechtigung auf solche IT-Verfahren mit hohem Schutzbedarf erhalten können. Weder die Zuordnung zu einer bestimmen Organisationseinheit als Voraussetzung wird technisch abgeprüft, noch ist technisch ein Vier-Augen-Prinzip sichergestellt.

Da keine Mandantentrennung gewährleistet ist, müssen diese IT-Verfahren als gemeinsame Verfahren gewertet werden, für die es keine ausreichende Rechtsgrundlage gibt.

1.7 Projekt „Intelligenter Bürgerservice“ (Kita-Gutschein)

Werden technische Lösungen zur hinreichenden Authentifizierung der Antragsteller nicht implementiert, müssen diese durch Änderungen im Verfahrensablauf sichergestellt werden. Die Antragsdaten fallen unter den Sozialdatenschutz.

Das Projekt „Intelligenter Bürgerservice“ gehört zu den mit der Firma Cisco International Limited (Cisco; vgl. VI 2.1) vereinbarten Pilotprojekten aus dem Bereich „Smart City“. Wir sind wie die behördliche Datenschutzbeauftragte in dieses Verfahren erfreulich früh und wiederholt durch die Projektleitung eingebunden worden.

Beim „Intelligenten Bürgerservice“ handelt es sich grundsätzlich um eine räumlich abgeschlossene, nicht einsehbare Box zur geschützten Fernkommunikation mit Kundendienststellen, über die öffentliche Leistungen zu einem bestimmten, durch die Freie und Hansestadt Hamburg definierten Thema abgewickelt werden können. Die geschützte Fernkommunikation erfolgt aus einer vorkonfigurierten, transportablen, in sich geschlossenen und vom Außenbereich visuell und akustisch abgeschirmten Einheit, die in anderen Ländern unter dem Titel „Smartbox“ bereits im Einsatz ist. Sie ermöglicht über eine flüchtige Bild- und Tonübertragung eine unmittelbare Kommunikation der Bürgerinnen und Bürger mit Publikumsdienststellen der Verwaltung. Zur Bearbeitung der Anliegen ist die Smartbox u.a. mit einer zoombaren Dokumentenkamera einschließlich Scannerfunktion und einem Drucker ausgestattet. Zur Kommunikation erfordert die Smartbox auf Seiten der Verwaltung einen Arbeitsplatz, der die Kommunikation ermöglicht und Ausdrucke freigibt.

Die Box soll für die Dauer eines Jahres im Alstertal-Einkaufszentrum aufgestellt werden. Zur Pilotierung wurde ausschließlich das Verfahren zur Erteilung von Kita-Gutscheinen im Bereich der Zuständigkeit des Bezirksamts Wandsbek ausgewählt. Anträge können in der Box gestellt werden und die Entgegennahme wird schriftlich bestätigt. Die interne Anbindung der Smartbox erfolgt beim Telefonischen HamburgService, um gegenüber der Fachdienststelle eine möglichst lange Erreichbarkeit zu gewährleisten. Als Mehrwert können weiterhin alle Auskünfte erteilt werden, die sonst telefonisch abgefragt werden müssten. Die Sitzung wird durch den Bürger oder die Bürgerin durch Betätigen eines Buttons auf dem Touchscreen eröffnet. Mit der ausdruckbaren Bescheinigung über die Beantragung kann die Kita-Leistung bereits beansprucht werden. Die weitere Sachbearbeitung (Weiterleitung, Bewilligung) erfolgt im Hintergrund für den Betroffenen unsichtbar.

Im Wesentlichen sind folgende Fragestellungen mit dem Projekt erörtert worden:

a) Authentifizierung
Die Authentifizierung des Antragstellers oder der Antragstellerin muss grundsätzlich revisionssicher erfolgen, damit die personenbezogenen Daten ihrem Ursprung zugeordnet werden können (§ 8 Abs. 2 Nr. 4 HmbDSG). Die Frage, ob dafür das sog. Videoident-Verfahren, das neuerdings im Rahmen des Geldwäschegesetzes bei Banken zum Einsatz kommt, genutzt werden kann, halten wir für kritisch. Dabei wird der Personalausweis an den Touchscreen gehalten und kann vom Mitarbeiter ausgelesen werden. Es ist weder die Wirksamkeit einer solchen Identifizierung geklärt, noch entspricht dies den Vorgaben des Personalausweisgesetzes. Außerdem ist nicht sichergestellt, dass die anfallenden personenbezogenen Daten datenschutzkonform verarbeitet werden.

Auch die Nutzung eines Unterschriftenpads bietet zwar Anhaltspunkte, kann aber ebenfalls eine sichere Authentifizierung nicht gewährleisten und ist schließlich schon aus Kostengründen verworfen worden.
Es obliegt der fachlichen Beurteilung, ob und welche authentifizierenden Maßnahmen letztlich erforderlich sind. Wird das Missbrauchsrisiko für beherrschbar gehalten, kann selbstverständlich auch ein anderer Verfahrensablauf gewählt werden, der die elektronische Authentifizierung erübrigt.

b) Einwilligung
Die Nutzung der Smartbox wird den Betroffenen parallel zur üblichen Antragstellung beim zuständigen Bezirksamt angeboten und ist mit einer zusätzlichen elektronischen Datenverarbeitung verbunden. Die Nutzung sollte daher mit Einwilligung der Betroffenen erfolgen. Dabei sollte es in diesem konkreten Rahmen ausreichend sein, wenn sie durch Anklicken auf dem Touchscreen erklärt wird.

c) Schutzbedarf
Bei den Daten zur Beantragung von Kita-Gutscheinen handelt es sich um Daten nach dem Hamburgischen Kinderbetreuungsgesetz, die zuständigkeitshalber von den Jugendämtern in den Bezirksämtern verarbeitet werden. Da es sich bei Sozialdaten grundsätzlich um sensible Daten handelt, wird im Rahmen der weiteren Projektentwicklung darauf zu achten sein, dass die Anforderungen an den Schutzbedarf in angemessenem Umfang erfüllt werden.

d) Technische Anbindung und Zuständigkeit
Die technische Anbindung an das FHH-Netz von dritten Stellen aus ist grundsätzlich sicher möglich, wurde hier aus Zeit- und Kostengründen jedoch zurückgestellt.
Die Beteiligung des Telefonischen HamburgService stellt die Bearbeitung durch eine an sich nicht zuständige Stelle dar und muss daher geregelt werden. Dies kann, da beide beteiligten Stellen zum Bezirksamt Wandsbek gehören, in diesem Fall durch eine Dienststellenleiterverfügung erfolgen; sollte der HamburgService auch für andere Bezirke tätig werden, müsste eine Regelung per Zuständigkeitsanordnung getroffen werden.

Wir haben dem Projekt geraten, die Fragen im Rahmen der noch ausstehenden Risikoanalyse zu behandeln, um in der Gesamtschau eine abschließende Restrisikobewertung vornehmen zu können.

1.8 Datenträgervernichtung: Nur geschreddert und vermischt

Bei Daten mit hohem Schutzbedarf sollte das Schreddergut immer vermischt werden.

Die neue DIN 66399 „Büro- und Datentechnik - Vernichten von Datenträgern" wurde im Oktober 2012 veröffentlicht. Der zuständige DIN-Ausschuss hat damit einen Standard erarbeitet, der den heutigen Stand der Technik in der Datenträgervernichtung abbildet und die veraltete Norm DIN 32757 ablöst. Die DIN 66399 verfolgt einen ganzheitlichen Ansatz, benennt Grundlagen und Begriffe sowie Anforderungen an Maschinen zur Vernichtung von Datenträgern und beschreibt einen sicheren Prozess der Datenträgervernichtung.

Durch das Vernichten von Datenträgern, auf denen personenbezogene Daten gespeichert sind, können öffentliche und nicht-öffentliche Daten verarbeitende Stellen ihrer Verpflichtung zum Löschen dieser Daten nachkommen. Die Verpflichtung ist sowohl im Hamburgischen Datenschutzgesetz (HmbDSG) in § 19 Abs. 3, im Bundesdatenschutzgesetz (§ 20 Abs. 2 bzw. § 35 Abs. 2 BDSG) als auch in spezialgesetzlichen Regelungen (z.B. § 84 Abs. 2 Sozialgesetzbuch Abschnitt X) verankert. Personenbezogene Daten sind insbesondere dann zu löschen, wenn ihre Speicherung unzulässig oder ihre Kenntnis für die Aufgabenerfüllung bzw. zur Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist.

Unter dem Begriff „Löschen" wird dabei das Unkenntlichmachen gespeicherter personenbezogener Daten (vgl. u.a. § 3 Abs. 4 Nr. 5 BDSG) und auch das Vernichten des Datenträgers (vgl. u.a. § 4 Abs. 2 Nr. 6 HmbDSG) verstanden. Der Prozess muss dauerhaft und irreversibel dazu führen, dass die betreffenden Informationen nicht mehr aus den gespeicherten Daten gewonnen werden können. Dies gilt sowohl für die Daten verarbeitende Stelle selbst als auch für Dritte.

Für Datenträger mit normalem Schutzbedarf ist für ein datenschutzgerechtes Entsorgen, das die Löschungsanforderungen erfüllt, mindestens die Sicherheitsstufe 4 der DIN 66399 erforderlich. Für die Bewertung der Sicherheitsstufe wird in erster Linie die Pixelgröße herangezogen, die beim Schreddern erreicht wird. Neben der maximalen Partikelgröße, die beim Vernichten erreicht wird, wird der Aufwand für die Rekonstruierbarkeit der Informationen auch durch weitere sicherheitstechnische Rahmenbedingungen des Vernichtungsprozesses beeinflusst. Hierzu zählen etwa Verwirbeln,

Verpressen oder Verbrennen von Vernichtungsrückständen.

Auf der Grundlage der neuen DIN 66399 hat die FHH ein Ausschreibungsverfahren für die Papier-Datenträgerentsorgung durchgeführt und 2015 den Auftrag vergeben. Hierbei wird als Standard die Gewährleistung der Sicherheitsstufe 4 festgeschrieben. Das Schreddergut wird durch Verwirbelung in großtechnischen Anlagen vermischt und verwirbelt. Damit können insbesondere Papier-Datenträger mit normalem und hohem Schutzbedarf datenschutzgerecht entsorgt werden.

Für die datenschutzgerechte Entsorgung von Daten mit sehr hohem Schutzbedarf müssen die Daten verarbeitenden Stellen eine zusätzliche Beauftragung auf der Grundlage des Rahmenvertrags veranlassen. Hierbei ist mindestens die Sicherheitsstufe 5 vorzugeben. Diese kann auch mit Büroaktenvernichtern der Klasse P5 erzielt werden. Wenn man das Schreddergut nur eines Dokuments vorliegen hat, das von solch einem Gerät erzeugt wird, wird man schnell feststellen, dass der Aufwand der Rekonstruktion nicht außergewöhnlich hoch ist. Daher sollte das mit Büroaktenvernichtern der Klasse P5 erzeugte Schreddergut zusätzlich über die „silbernen Tonnen" des Aktenvernichters entsorgt werden, da dann durch die Verwirbelung eine ausreichende Vermischung des Schredderguts gewährleistet ist.
Wir haben zur Problematik der Datenträgerentsorgung die Orientierungshilfe zur Ermittlung des Schutzbedarfs personenbezogener Daten für den Prozess der Datenträgervernichtung in unserem Internetangebot veröffentlicht. Dort sind für die unterschiedlichen Schutzbedarfe die datenschutzgerechten Vernichtungsanforderungen beschrieben.

2. Infrastruktur, Bauen, Wohnen, Energie

2.1 Smartes Hamburg, digitale Stadt

Die Ausrichtung des Senats auf die Digitalisierung aller urbanen Lebensbereiche muss bei dem Ziel, eine lebenswerte moderne Stadt für ihre Bewohner zu schaffen, auch sicherstellen, dass gleichzeitig ihr informationelles Selbstbestimmungsrecht gewahrt bleibt.

„Smart" im Sinne von intelligent wird verstärkt auf Verfahren angewendet, die durch technikorientierte Lösungen, zunehmend durch Vernetzung, in alle denkbaren Lebensbereiche einziehen. Gern einbezogen in die Betrachtung werden dabei die sogenannten Megatrends: Internet der Dinge, Mobility, Cloud Computing und Big Data.
Daneben gibt es zunehmend Begehrlichkeiten, vordergründig ohnehin anfallende Daten aus Smartphones, Kraftfahrzeugen u.ä. für Infrastruktur- und wirtschaftliche Zwecke abzugreifen und zu nutzen.

Neben Smart City und Smart Factory sind den Betroffenen Smart Car, Smart Ticketing, Smart Home und Smart TV gängige Begriffe, mittlerweile gefolgt von Industrie 4.0. Auf den Verkehrsbereich bezogen, heißt es zum intermodalen Ansatz in Echtzeiterfassung dann folgerichtig: Der größte Mehrwert entstehe dann, wenn Verkehrs-, Reise-, Routen- und Fahrgastinformationen sowie Informationen über Störungen bzw. Fahrplanabweichungen für möglichst viele bis alle Formen der Mobilität verknüpft und dargestellt werden könnten.
Mit dem Aufbau des Internets der Dinge und der zunehmenden Vernetzung wird es auch zunehmend komplexer, die Rechte des Einzelnen auf sein informationelles Selbstbestimmungsrecht zu schützen. Dabei wird die Schnelligkeit der technischen Entwicklung aus Rechtsgründen nicht dazu führen können, dass das im Datenschutz geltende und auch von der anstehenden EU-Datenschutzgrundverordnung übernommene Prinzip des Verbots mit Erlaubnisvorbehalt zugunsten eines wirtschaftsfreundlicheren risikoorientierten Modells aufgegeben wird. Der Europäische Gerichtshof hat mit seinen letzten wegweisenden Entscheidungen die Grundrechte der Betroffenen gegenüber den an einer Datennutzung bestehenden Wirtschaftsinteressen gestärkt.

Selbst wenn technische Neuerungen sinnvoll und erprobenswert erscheinen, müssen sie sich in den bestehenden und ggfl. rechtzeitig zu aktualisierenden Rechtsrahmen einordnen lassen. Eine frühzeitige Einbeziehung datenschutzrechtlicher Fragestellungen gewinnt daher zunehmend an Bedeutung.

Entsprechend hat die internationale Datenschutzkonferenz am 13./14.10.2014 folgende Empfehlung zum Internet der Dinge (Internet of Things, IoT) abgegeben:

„- Die Bedeutung der durch IoT erfassten Daten wird hinsichtlich Menge, Qualität, Aktualität und Sensibilität weiter wachsen. Daher sollten diese Daten grundsätzlich als personenbezogene Daten angesehen werden.

- Geschäftsmodelle, die auf IoT-Daten beruhen, müssen ausreichend transparent sein und darlegen, welche Dienstleistungen auf welche Daten zugreifen.

- Die Bedeutung des Ubiquitous Computing wird zunehmen, daher werden anonyme Nutzungsmöglichkeiten oder Verpflichtungen zur Datensparsamkeit (§ 3a BDSG) immer wichtiger.

- Die Privatsphäre der Verbraucher muss durch Konzepte wie Privacy by Design und Privacy by Default von Anfang an geschützt werden. Datenschutz und Sicherheit müssen als Wettbewerbsvorteil betrachtet werden.

- Das Internet der Dinge stellt auch eine beträchtliche Herausforderung für die IT-Sicherheit dar. Um die mit IoT verbundenen Risiken zu minimieren, ist Ende zu Ende Sicherheit nicht nur bei individueller Kommunikation (z. B. E-Mail), sondern

auch bei der Kommunikation zwischen „Dingen" erforderlich. Dadurch wird beispielsweise das Mitlesen durch unbeteiligte smarte Geräte verhindert.

- Die Datenschutzgesetze und die neue europäische Datenschutz Grundverordnung müssen den Anforderungen, die sich aus IoT Technologien ergeben, gerecht werden."

Die bekannten Datenschutzprinzipien können, sorgfältig angewandt, auch die Anforderungen der digitalen Vernetzung angemessen abbilden, wenn insbesondere der Grundsatz der Datensparsamkeit bei der Erhebung, die Anonymisierung, die Zweckbindung bzw. technische Unverkettbarkeit, die Verschlüsselung und die Transparenz für den Betroffenen beachtet werden.

Der aus dem mit der Firma Cisco geschlossenen Memorandum of Understanding (MoU) resultierende, programmatisch benutzte Begriff der Smart City ist selbst mangels Definition kaum fassbar. Für die Freie und Hansestadt Hamburg wird seitens des Senats deshalb das Ziel definiert, das moderne Hamburg als digitale Stadt zu formen und zu präsentieren. Dazu gehört neben dem Aufbau der E-Governance und der städtischen Infrastruktur unter dem Aspekt der Standortsicherung auch die Schaffung von Innovationsräumen für unternehmerisches Handeln (Regierungserklärung vom 06. Mai 2015). Hierzu sollen vielfältige Formen der Zusammenarbeit wie Messen, Workshops, Public Private Partnerships u.a. dienen.

Wir begrüßen, dass nach dem Willen des Senats Datenschutzbelange dabei ausdrücklich zum Bestandteil von Projektentwicklung gemacht werden sollen, werfen diese grundsätzlichen Überlegungen letztlich doch eine große Anzahl datenschutzrechtlicher Fragestellungen im Detail auf. Es wird darauf ankommen, die grundlegenden datenschutzrechtlichen Prinzipien wie Datensparsamkeit, Erforderlichkeit, Zweckbindung und Transparenz auch in der Anwendung neuer Techniken zu gewährleisten, u.a. durch Hinterfragen typischer Verfahrensabläufe und frühzeitiger Benennung von Regelungsbedarfen.

Im Berichtszeitraum sind wir an folgenden Aktivitäten beteiligt worden:

Smart City; Memorandum of Understanding (MoU)

Schon am 30. April 2014 haben der Senat und Cisco ein Memorandum of Understanding unterzeichnet, nach dem die Freie und Hansestadt Hamburg die Möglichkeit erhalten soll, unverbindlich verschiedene Ansätze des von Cisco entwickelten Konzepts „Smart+ Connected Communities" zu erproben. Ausdrücklich bleibt es bei der – auch datenschutzrechtlichen – Verantwortung der letztlich beauftragenden Stellen. Typischerweise handelt es sich bei den Projekten um vernetzte Anwendungen.
Als mögliche Pilotfelder wurden die Bereiche Verkehr und Bürgerdienstleistungen (Smart City), Hafen (Smart Port) und Hafencity (Smart Building und Mobilität) bestimmt.

Wir haben zunächst alle betroffenen Stellen angeschrieben und hatten in einer ersten Datenschutzveranstaltung des Projektmanagement-Büros (PMO) die Gelegenheit, mit diesem Kreis grundsätzliche und erste projektbezogene datenschutzrechtliche Fragestellungen und Hinweise zu erörtern. Parallel haben wir insbesondere die Projekte Smart Port (vgl. VI 2.4) und Intelligenter Bürgerservice datenschutzrechtlich beraten (vgl. VI 1.7).

Seit Sommer 2015 sind wir Mitglied in der sich ständig erweiternden Lenkungsgruppe MoU. Diesen Umstand begrüßen wir sehr, da sich der Kontakt zu den einzelnen Teilprojekten sehr heterogen gestaltet hatte. So hatte die Hamburg Port Authority (HPA) schon länger an einer smarten Gesamtlösung für den Hafen gearbeitet, während andere Projekte augenscheinlich immer noch in der Findungsphase sind, insbesondere dann, wenn erst mögliche Geschäftsfelder für angedachte Infrastrukturen erkannt werden müssen.

In dieser Position haben wir nun die Möglichkeit, datenschutzrechtliche Überlegungen frühzeitig anzustoßen. Hierfür haben wir vorgeschlagen, eine datenschutzrechtliche Arbeitshilfe für die Initialphase der Projekte zu erstellen, wie es sie für die etablierte Vorabkontrolle vor Inbetriebnahme von automatisierten Verfahren schon gibt.Ein erster Entwurf befand sich zu Redaktionsschluss in der Abstimmung.

Senatsbeschluss Digitale Stadt

Im Januar 2015 hat der Senat die Strategie „Digitale Stadt" beschlossen (Drucksache 2015/0014 vom 06.01.2015). Ziel ist es, zur Sicherung des Standortes technische Innovationen für die Entwicklung der Freien und Hansestadt Hamburg nutzbar zu machen. Dazu werden Initiativen und Projekte durchgeführt bzw. unterstützt, die die Chancen der Digitalisierung thematisieren.

Damit will Hamburg einen Raum bieten, um neue technologische Lösungen zur Verbesserung der Servicequalität und des städtischen Lebens in sozial- und umweltverträglicher Weise in praktischer Anwendung zu erproben.

Die Digitalisierung ist Bestandteil der jeweiligen Fachverantwortung unter Einbeziehung von Wirtschaftsclustern und StartUp-Unternehmen. Die Fachbehörden entwickeln Teilstrategien unter Berücksichtigung von IT-Sicherheit, Datenschutz, dem informationellen Selbstbestimmungsrecht der Betroffenen und angemessenere Beteiligungsmöglichkeiten.
Verantwortlich für die zentrale Steuerung behördenübergreifender Strategien der Digitalisierung der Stadt, für die Koordinierung und Außendarstellung ist die Staatsräterunde. Zur Umsetzung und als Ansprechpartner gegenüber strategischen Partnern und der Öffentlichkeit wurde in der Senatskanzlei eine Leitstelle Digitale Stadt eingerichtet.

Zur wissenschaftlichen Begleitung wurde bei der HafenCityUniversität (HCU) in Zusammenarbeit mit dem Massachusetts Institute of Technology (MIT) ein Digital City Science Lab eingerichtet. Durch Grundlagen- und angewandte Forschung sowie Beratung durch Think Tanks sollen interdisziplinär Stadtforschung und Strategien einer digitalen Stadt betrieben werden, um in Hamburg wissenschaftliche Expertise bei der Entwicklung einer digitalen Stadt oder Smart City nutzen zu können.

Das Konzept der Digitalen Stadt setzt dabei auf die bestehende Infrastruktur auf, statt einen umfassenden und durchstrukturierten Neuansatz zu betreiben.

Dazu wurden in den Tätigkeitsfeldern Infrastruktur, Kommunikation und Daseinsvorsorge folgende städtische Projektthemen beschrieben, an denen zum Teil auch private Betreiber beteiligt werden sollen:
Digitale Verwaltung, intelligente Verkehrssysteme, intelligente Bildungsnetze, smarte Geodaten, Smart Energy, Smart Port, Hamburg Open Online University und eCulture. Teile davon sind auch Gegenstand der Lenkungsgruppe zum Memorandum of Understanding.
Verschiedene dieser Vorhaben wurden von uns bereits betreut (vgl. u.a. III 1.4, III 2.1, V 8.1, VI 1.7, VI 2.4). Daneben wurden uns erste Überlegungen zur Strategie intelligenter Verkehrssysteme vorgestellt.

Nach einem ersten Kontakt mit der Leitstelle im September 2015 sind wir im November 2015 als Teilnehmer in die Koordinierungsrunde Digitale Stadt eingeladen worden. Auch in diesem Zusammenhang war der Bedarf an einer frühzeitigen orientierenden Arbeitshilfe zum Datenschutz signalisiert worden. Wir haben daher angeboten, ein einheitliches Papier für die Belange der Smart City und der Digitalen Stadt zu erstellen. Zu Redaktionsschluss befand sich unser Entwurf in der Abstimmung mit den beteiligten Stellen.

Im Übrigen werden wir die strategischen Überlegungen in der Koordinatorengruppe weiterhin begleiten, wobei darauf hingewiesen werden muss, dass dies ohne Verbesserung der personellen Ausstattung aufgrund der fortschreitenden Diversifizierung der Projekte nicht in der eigentlich erforderlichen Tiefe erfolgen kann.

2.2 Datenschutzgerechte Reisezeitermittlung auf Autobahnen

Die von uns vorgeschlagenen Anforderungen für eine datenschutzgerechte Reisezeiterfassung wurden zur Grundlage des Ausschreibungsverfahrens für die Sanierung der Autobahn A7 gemacht.

Die Autobahn A 7 soll in den kommenden Jahren zwischen dem Autobahndreieck Bordesholm in Schleswig-Holstein bis zum Elbtunnel 6- bzw. 8- spurig erweitert und aus Immissionsgründen im Hamburger Bereich teilweise eingehaust werden. Im Rahmen des Projektes ist geplant, die vorhandene Netzbeeinflussungsanlage auf den Autobahnen A 1, A 7, A 21 und der Bundesstraße B 205 so zu ertüchtigen, dass den Verkehrsteilnehmerinnen und Verkehrsteilnehmern bzgl. der Reisezeiten und der Sicherheit optimale Routen im Straßennetz angeboten werden können. Grundlage für eine Steuerungsanlage ist die Ermittlung von zuverlässigen aktuellen Reisezeiten auf allen Normal- und Alternativrouten. Damit sollen baustellen-, unfall-, betriebs- und sonstige überlastungsbedingte Verkehrsstörungen rechtzeitig und zuverlässig erkannt und der Verkehr auf weniger belastete Routen umgeleitet werden. Als Basis für die Ermittlung von Reisezeiten ist geplant, an 24 Standorten im betroffenen Straßennetz anonymisierte Kenndaten von vorbeifahrenden Fahrzeugen berührungslos und ohne Einbauten in die Fahrbahn zu erfassen. Dazu sollen die MAC-Adressen von allen Geräten wie z.B. Smartphones und Autoradios ausgelesen werden, die sich in den Fahrzeugen befinden und deren Bluetooth-Schnittstelle aktiviert ist.

Datenschutzrechtlicher Ausgangspunkt der Überlegung war, dass nach dem Intelligente Verkehrssysteme Gesetz (IVSG) die Reisezeiterfassung in Echtzeit grundsätzlich einer weiteren ausdrücklichen bundesgesetzlichen Grundlage bedarf. Diese besteht jedoch nicht und ist auch absehbar nicht zu erwarten. Etwas anderes ergibt sich auch nicht aus der zwischenzeitlich erlassenen Delegierten Verordnung (EU) 2015/962 der EU-Kommission vom 18. Dezember 2014 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates hinsichtlich der Bereitstellung EU-weiter Echtzeit-Verkehrsinformationsdienste (vgl. insbesondere Erwägungsgrund 9), da diese grundsätzlich anonymisierte personenbezogene Daten voraussetzt.

Andererseits liegt nach der Rechtsprechung des Bundesverfassungsgerichts zum Kennzeichen-Scanning (1BvR 29174/05) dann kein Eingriff in das informationelle Selbstbestimmungsrecht - mithin auch kein Verstoß gegen den Gesetzesvorbehalt - vor, wenn eine automatisierte Erfassung von Kennzeichen unverzüglich ausgewertet und das Kennzeichen (von dortigen sog. Nichttreffern) ohne weitere Auswertung sofort spurenlos gelöscht wird.

Diesen Gedankengang haben wir uns zu eigen gemacht und auf die Reisezeitermittlung übertragen: Auch anonyme und dauerhaft hinreichend wirksam anonymisierte Daten beinhalten keinen Eingriff in das informationelle Selbstbestimmungsrecht. Ziel der Überlegung war daher, ein technisches Verfahren zu etablieren, das in seiner anonymisierenden Wirkung faktisch einer solchen Behandlung der Daten wie im Kennzeichen-Scanning-Urteil gleich kommt.

Im Ergebnis haben die beteiligten Datenschutzbeauftragten der Länder Schleswig-Holstein, Hamburg und Niedersachsen in analoger Anwendung der Rechtsprechung des

Bundesverfassungsgerichts zum Kennzeichen-Scanning keine Bedenken gegen das Vorhaben, wenn das aus mehreren technischen und organisatorischen Komponenten bestehende Verfahren eingehalten wird.

Bei der Beurteilung haben wir uns von folgenden Überlegungen leiten lassen:

- MAC-Adressen sind personenbezogene Daten.
- Die Reisezeitermittlung in Echtzeit fällt unter § 2 IVSG (Verkehrsdaten).
- Nach § 3 Satz 2 IVSG bedarf es zur Verarbeitung personenbezogener Daten grundsätzlich einer ausdrücklichen bundesrechtlichen Ermächtigung. Eine ausdrückliche Ermächtigung liegt bisher nicht vor, weder § 98 Telekommunikationsgesetz (Informationsweiterleitung), das Bundesdatenschutzgesetz (vgl. § 1 Abs. 2 Nr.2) noch die Delegierte Verordnung (EU) 2015/962 der Kommission sind einschlägig.
- Eine Verarbeitung kann derzeit in Anlehnung an das Bundesverfassungsgerichtsurteil 1 BvR 2074/05 (Kennzeichen-Scanning) nur erfolgen, wenn durch ein mehrstufiges Verfahren eine solche faktische Anonymisierung erreicht wird, die der sofortigen Löschung in der o.a. Entscheidung gleich kommt, so dass unterstellt werden kann, dass das informationelle Selbstbestimmungsrecht von Betroffenen, wie dort entschieden, auch hier nicht tangiert wird.
- Anonymisierte Daten sind grundsätzlich fortlaufend darauf hin zu prüfen, ob die einmal erlangte Anonymität hinsichtlich des technischen Fortschritts und des Zusatzwissens Dritter (Big Data) noch weiter besteht. Um die Möglichkeiten der Reidentifizierbarkeit auch diesbezüglich weiter zu minimieren, sind grundsätzlich flankierend weitere Maßnahmen zu treffen, die den datenschutzrechtlichen Grundsätzen, insbesondere der Erforderlichkeit und der Datensparsamkeit, folgen.

Folgende technische Maßnahmen sind einzuhalten, damit ein datenschutzgerechtes Verfahren realisiert wird:

Erste Stufe: Kürzung der MAC-Adresse

Der erste Schritt der Anonymisierung der Kenndaten ist in durch eine unvollständige Übernahme des Kenndatensatzes (MAC-Adresse) unmittelbar bei der Erfassung zu realisieren. Bei dem Bluetooth-basierten System besteht die MAC-Adresse aus 3 Byte Herstellercode und 3 Byte Adressraum für das einzelne Gerät. Es ist zwingend sicherzustellen, dass bei der Erfassung das letzte Byte des Adressraumes nicht miterfasst und weiterverarbeitet wird. Dies ist ohne größere negative Auswirkungen auf die Genauigkeit des Erfassungssystems möglich, stellt aber sicher, dass kein eindeutiger Bezug des erfassten Datensatzes zum individuellen Quellgerät mehr möglich ist. Damit werden 256 MAC-Adressen auf eine gekürzte MAC-Adresse abgebildet.

Unmittelbar nach der ersten Stufe der Anonymisierung der Kenndaten bei der Erfassung der vorbeifahrenden Fahrzeuge sind die zweite und die dritte Stufe direkt im oder am Detektor wie folgt umzusetzen.

Zweite Stufe: Bildung eines Hashwertes

In der zweiten Stufe wird ein Hashing-Verfahren eingesetzt. Im vorliegenden Fall wird der „Secure-Hash-Algorithm (SHA 256)" eingesetzt. Dieses Verfahren ist nicht umkehrbar, d.h. eine Rückwärtsermittlung der originären Kenndaten aus dem Hashwert ist nicht möglich.
Hinzu kommt der sogenannte „Salt-Wert" als zufällig gewählte Zeichenfolge, die an einen gegebenen Klartext vor der Verwendung einer Hashfunktion angehängt wird, um die Entropie der Eingabe zu erhöhen. Der Salt-Wert muss systemweit, aber für den vertretbar kürzesten Zeitraum, identisch sein. Er wird als Zufallswert in der Reisezeit-Unterzentrale, dem Kontenpunkt, an dem die Messstationen angeschlossen sind, erzeugt und als Parameter an alle betroffenen Streckenstationen verteilt.
Weiterhin wird der Salt-Wert mindestens einmal täglich gewechselt, um eine Wiedererkennbarkeit sich zyklisch wiederholender Fahrtmuster einzelner Fahrzeuge (Profilbildung) auszuschließen. Zunächst ist vorgesehen, den Salt-Wert jede Nacht zu einer definierbaren Uhrzeit zu wechseln. Bei Bildung eines neuen Salt-Wertes werden in der Reisezeit-Unterzentrale alle noch vorhandenen aus dem Vorgängerwert gebildeten Kenndaten von Einzelfahrzeugen gelöscht, da diese ohnehin nicht mehr weiter verwendet werden können.
Es wird durch geeignete Maßnahmen, die in den Grundschutzkatalogen des Bundesamtes für Sicherheit in der Informationstechnik festgelegt sind, sichergestellt, dass die Salt-Werte der Vergangenheit nicht rekonstruiert oder anderweitig bestimmt werden können.

Dritte Stufe: Bildung eines Prüfwertes

Zur weiteren Verschleierung und gleichzeitigen Verkürzung des Hashwertes wird im dritten Schritt eine Prüfsumme gebildet. Vorgegeben hier ist das CRC64-Verfahren zur Bestimmung eines Prüfwertes für Daten, um Fehler bei der Übertragung oder Speicherung erkennen zu können. Damit entsteht ein Prüfwert, der mit maximal 8 Byte je Schlüssel dazu führt, dass eine größere Menge von Einzelfahrzeugdaten zur Reisezeit-Unterzentrale übertragbar ist.

Im vorliegenden Verfahren wurden folgende flankierende Maßnahmen vereinbart und in die Dokumentation aufgenommen:

- Zusammenfassung mehrerer Wegstrecken („Fahrten") eines Fahrzeugs nicht mit Hilfe des Hashwertes, sondern mit Hilfe einer Fahrt-ID (zufällig oder fortlaufend);
- Frühestmögliche Löschung der technisch bearbeiteten Hashwerte (jeweils nach Erfassung durch die nachfolgende Messstation, Berechnung dieser Teil-Reisezeit), sobald eine Teilstrecke einer Fahrt-ID zugeordnet werden kann;
- Beschränkung des Erfassungsbereichs auf den dem fließenden Verkehr gewidme-

ten Straßenraum;
- Aussonderung untypischer Reisezeiten (z.B. Rasten, Parken, Fußgängerinnen- und Fußgänger-, Fahrrad-Geschwindigkeiten) durch Löschung nach Erreichen einer Grenzzeit von drei Stunden;
- Unterbrechung der Erfassung nach dem Zufallsprinzip für eine Dauer zwischen zwei und fünf Minuten pro Stunde.

Das Verfahren der Reisezeitberechnung werden wir beim Aufbau und der produktiven Anwendung weiter begleiten.

2.3 HVV-Card

Das eTicketing ist grundsätzlich geeignet, Komfort und Effizienz von Verkehrsverbünden zu erhöhen. Die HVV-Card stützt sich mit der VDV-Kernappplikation auf einen guten Standard. Die beim Hamburger Verkehrsverbund (HVV) zum Einsatz kommenden Komponenten müssen auch in ihrem spezifischen Zusammenspiel den datenschutzrechtlichen Anforderungen genügen.

Schon seit langem ist der öffentliche Personennahverkehr (ÖPNV) dadurch gekennzeichnet, dass er möglichst effizient eine große Anzahl von Fahrgästen bequem und zeitsparend befördern soll. Vor genau 50 Jahren hat der Hamburger Verkehrsverbund (HVV) in diesem Sinne Pionierarbeit geleistet mit der Gründung des ersten Verkehrsverbundes der Welt: Erstmals war es möglich, im Geltungsbereich die Leistungen verschiedener Verkehrsbetriebe mit einer Fahrkarte zu benutzen.

Die daraus immer noch resultierenden besonderen Verbundstrukturen sind auch bei der mit der Einführung des eTicketing in Form der HVV-Card verbundenen personenbezogenen Datenverarbeitung zu beachten.

Im Zuge der Digitalisierung haben sich, auch unter Mitwirkung des HVV, die Verkehrsverbünde im Verband deutscher Verkehrsunternehmen (VDV) frühzeitig mit der Frage beschäftigt, wie ein elektronisches Ticket zur weiteren Steigerung von Effizienz und Komfort führen kann, und wie es ausgestaltet sein muss, um über die derzeit bestehenden Verbünde hinaus möglichst deutschlandweit nutzbar zu sein.

2007 hatte die International Working Group on Data Protection in Telecommunications (sog. Berlin Group) dazu folgende Forderungen aufgestellt:
- parallele anonyme Nutzung sollte ermöglicht werden;
- umfassende, verständliche Aufklärung der Betroffenen;
- Priorisierung von anonymen Daten und kürzestmögliche Speicherdauer;
- Werbung nur mit informierter, von der Zustimmung zu allgemeinen Geschäftsbedingungen abgehobener Einwilligung der Betroffenen;

- Verarbeitung von Zahlungsnachweisen und Bewegungsdaten ebenfalls unter Priorisierung anonymer Nutzung;
- Trennung von Stammdaten und Reisedaten;
- Durchführung einer Vorabkontrolle.

Als Ergebnis wurde die VDV-Kernapplikation (VDV-KA) vorgestellt und 2012 auch mit den Datenschutzbeauftragten des Bundes und der Länder abgestimmt.

Die VDV-KA ist ein offener Daten- und Schnittstellen-Standard für Electronic Ticketing bzw. elektronisches Fahrgeldmanagement im öffentlichen Personenverkehr. Die dazugehörigen Chipkarten („eTicket Deutschland") unterstützen rein technisch alle denkbaren Ausbauvarianten. Dazu gehören eBezahlen als bargeldloser Fahrscheinkauf, eTicket als elektronischer Fahrschein, insbesondere im Zeitkartensegment, und eTicket mit automatischer Fahrpreisberechnung durch berührungsloses Ein- und Auschecken pro Fahrt. Die Verkehrsverbünde können frei wählen, welche Optionen sie anbieten wollen, auch differenziert nach Einzelfahrscheinen, Zeitkarten und Abonnementsangeboten. Die Karten können u.a. mit und ohne Lichtbild personalisiert werden.

Der HVV hatte mit uns bereits 2008 bis 2011 eine örtlich begrenzte Pilotierung des Angebots mit Teilfunktionen auf freiwilliger Basis abgestimmt. Für das Ausrollen in die Breite wurde uns nun die HVV-spezifische Lösung für die Strukturen vor Ort vorgestellt:

Der HVV wird heute als Verbund von den Aufgabenträgern des ÖPNV (Länder und Kreise) mit ca. 30 teilnehmenden Verkehrsbetrieben und der HVV GmbH als Regiebetrieb gebildet. Er befördert zurzeit jährlich etwa 730 Millionen Verbundfahrgäste. Aus Effizienzgründen werden schon jetzt einzelne Aufgabenfelder von einzelnen Unternehmen im Wege der Geschäftsbesorgung für alle angeschlossenen Unternehmen wahrgenommen. Dies bedeutet für die Kunden, dass sie je nach Tarifangebot einen spezifischen Ansprechpartner haben. Da die Stammdaten der Kunden bisher je nur dort vorgehalten werden und auch von den Servicestellen noch nicht eingesehen werden können, bedeutet dies, dass die Kunden von den einzelnen Servicestellen und den einzelnen Unternehmen immer noch weiterverwiesen werden müssen. Dies gilt auch in den jährlich etwa 35.000 Fällen, in denen eine Ersatzkarte ausgestellt werden muss. Seit der HVV sich seit 2002 erheblich in das ländlicher strukturierte Umland ausgeweitet hat, stößt dies zunehmend auf das Unverständnis der Kundinnen und Kunden.

Als problematisch für die Tarifstruktur, die beim HVV von alters her auf personengebundene Fahrscheine mit Lichtbild ausgerichtet ist, haben sich die Zeitkarten im Abonnement erwiesen, die derzeit noch nicht mit einem Lichtbild ausgestattet sind. Gerade Schüler- und zum Teil auch Studierendentickets lassen sich noch durch einfaches Kopieren der von den Bildungseinrichtungen ausgestellten Bescheinigungen fälschen. Die Pflicht, für die Sichtkontrolle auch den Personalausweis vorweisen zu müssen, stößt insbesondere dort an Grenzen, wo innerstädtische Kontrollen an den Ausgängen

von U- und S-Bahnhöfen vorgenommen werden: um die zeitliche Verzögerung für die Kunden in vertretbaren Grenzen zu halten, wird derzeit regelhaft auf die Einsicht in den Personalausweis verzichtet.

Die Kunden sollen nun einen Grundvertrag über die HVV-Card abschließen, zu dem sie dann je nach Lebenslage die passenden Tarife auswählen können. Ergänzend können sie bestimmte Serviceleistungen wählen, die ihnen die Verfolgung ihrer Kontobewegungen per Internet oder teilweise in den Servicestellen und an den Automaten ermöglichen sollen. Bei Prepaidkarten soll eine Erinnerungsfunktion angeboten werden.

Die Karte soll mit einem Lichtbild ausgestattet werden. Die Stammdaten einschließlich Lichtbild sollen für die gängigen Serviceleistungen, soweit erforderlich, auch von den Servicestellen vor Ort einsehbar sein.

Von den Möglichkeiten der Applikation soll die Funktion eTicket mit Buchung des Fahrscheins oder der Abokarte und Abrechnung eingeführt werden. Dies soll sukzessive bis 2017 für alle Tarifangebote geschehen. Einzelfahrscheine sollen mit 3% gegenüber dem Barpreis rabattiert werden. Als Zahlungsarten sollten monatliche Abbuchungen im Nachhinein und Prepaid-Buchungen, zunächst im Wege des Lastschriftverfahrens, später auch als Bareinzahlung, angeboten werden. Die Einführung der automatischen Fahrgeldberechnung ist nicht vorgesehen.

Je nach konkreter Ausgestaltung der VDV-Kernapplikation muss auch das Angebot vor Ort den datenschutzrechtlichen Anforderungen entsprechen. Als kritisch hatten wir vor allem die Verarbeitung des Lichtbildes, die anonymen Nutzungsmöglichkeiten und die Einwilligungsanforderungen thematisiert. Auch die vertraglichen Beziehungen zwischen Kundenvertragspartnern, beteiligten Beförderungsunternehmen und Betreibern von Servicestellen müssen das Angebot datenschutzgerecht wiederspiegeln.

Grundsätzlich konnten wir die lichtbildgestützte Ausstattung nachvollziehen: Unbestritten führt die Speicherung des Lichtbildes auf der HVV-Card zum Komfortgewinn bei den Betroffenen. Die Wartezeiten bei innerstädtischen Kontrollen müssen nicht weitere Zeitverzögerungen zu Lasten der Betroffenen mit sich bringen. Auch die Ausstellung von Ersatzkarten in jeder Servicestelle erhöht den Kundenkomfort. Verglichen mit anderen Projekten sehen wir jedoch noch weiteren Erörterungsbedarf hinsichtlich der Einbindungsmodalitäten und der Speicherfristen.

Anders als bei übertragbaren Fahrkarten erfordert die personengebundene Tarifstruktur wirksame Kontrollmöglichkeiten der personengebundenen Angaben, gerade im Bereich der deutlich vergünstigten Zeitkarten im Abonnement. Die Kontrolle der Fahrgäste gehört als Annexfunktion zur Abwicklung des Beförderungsvertrages. Die Nutzung des Lichtbildes kann daher als eine Maßnahme nach § 28 Absatz 1 Nummer 1 des Bundesdatenschutzgesetzes (BDSG) zur vertragsgerechten Abwicklung des Beförderungs-

verhältnisses angesehen werden. Da der Schwerpunkt der Fahrten im Stadtbereich mit kurzen Fahrtzeiten erbracht wird, müssen die Kontrollen, anders als bei längeren Stationsabständen, zügig und zielführend durchführbar sein. Da den Kundinnen und Kunden, die eine möglichst anonyme Nutzung wünschen, die Möglichkeit eingeräumt wird, dass das Lichtbild nach Personalisierung der HVV-Card mit Aufdruck des Bildes im Stammdatensatz wieder gelöscht wird, erscheint die Lösung noch angemessen.
Für Kunden des sog. Großkundenabonnements, das zu weiter vergünstigten Bedingungen über die Arbeitgeber abgewickelt wird, haben wir die Anregung einbringen können, den Betroffenen auch die Möglichkeit zu geben, Lichtbilder selbst über das Internet hochzuladen.
Unsere Bedenken richteten sich auch gegen die Abläufe sogenannter anonymer Angebote: Wir haben verdeutlicht, dass das Konzept personalisierter Karten immer personenbezogen ist. Die immerhin als datenschutzfreundlicher zu bezeichnenden Prepaid-Karten werden so eingerichtet, dass dem HVV mit dem Erstantrag nur eine Vorgangsnummer bekannt wird, die dann bei der Personalisierung der HVV-Card mit einer Kartennummer verknüpft wird. Insoweit kann von einer Pseudonymisierung, maximal von einer faktischen Anonymisierung gegenüber dem Stammdaten haltenden Verkehrsbetrieb (Kundenvertragspartner), ausgegangen werden. Zunächst war auch nur eine Bezahlung per Lastschrift vorgesehen. Mittlerweile ist uns zugesichert worden, dass an den Automaten und in den Servicestellen zu einem späteren Zeitpunkt auch Barzahlungsmöglichkeiten vorgesehen sein sollen.

Zu der Variante eines Grundvertrages über die HVV-Card mit der Möglichkeit, anschließend die Tarifangebote nach Bedarf auszuwählen und zu wechseln, haben wir verschiedene Hinweise gegeben. Auch wenn die allgemeine Aufklärung bereits viel Raum einnimmt, müssen die Einwilligungen in die Serviceleistungen ebenso wie die in Werbung den gesetzlichen Anforderungen entsprechen.

Schließlich haben wir auch darauf hingewiesen, dass die Umsetzung der Servicefunktionen gegenüber den Mustervereinbarungen des VDV weiterer vertraglicher Regelungen mit den einzelnen Serviceunternehmen erfordert. Wir gehen davon aus, dass diese grundsätzlich im Wege der Auftragsdatenverarbeitung für die Kundenvertragspartner tätig werden können.
Wir werden die weiteren Überlegungen zur Umsetzung, wie dies datenschutzfreundlich und zielführend erfolgen kann, weiter begleiten.

2.4 Projekt smartPORT

Mit den 27 Teilprojekten von smartPORT hat die Hamburg Port Authority (HPA) aufgezeigt, welche Potentiale in einer digitalisierten Modernisierung der Infrastruktur liegen können. Die zum Teil komplexen Nutzungen müssen sich dort, wo sie auf die Verarbeitung personenbezogener Daten setzen, laufend an der Diskussion um effektiven Datenschutz für die Betroffenen messen lassen.

Anlässlich der Unterzeichnung des Memorandum of Understanding (MoU) mit der Firma Cisco (vgl. VI 2.1) hat uns HPA im August 2014 ein Bündel von Ideen vorgestellt, die einen modernen Hafen bei der Lösung der Herausforderungen des 21. Jahrhunderts digital unterstützen sollen. Dabei gliederten sich die Vorhaben grob in die zwei Bereiche smartPORT logistics mit 12 Teilvorhaben und smartPORT energy mit 15 Teilvorhaben.

Der Bereich smartPORT energy sollte die energetische Neuausrichtung des Hamburger Hafens als einem der größten zusammenhängenden Industriegebiete Europas hin zu einer ökonomisch und ökologisch zukunftsfähigen Energieversorgung unterstützen. Der Hafen sollte damit als Schaufenster für Wind- und Solarenergie, umweltfreundliche Mobilität und machbare Effizienzsteigerungen dienen. Im Wesentlichen sollten diese Ziele durch Maßnahmen der Wirtschafts- und Forschungsförderung erreicht werden. Umweltfreundliche Mobilität sollte durch Vermeidung von unnötigen Verkehren, Verlagerung der Transporte von der Straße auf Schiene und Wasserstraße sowie verbesserte Emissionswerte erreicht werden. Dafür sollten liegende Schiffe mit erneuerbaren Energien versorgt werden, eine Flotte von Elektrofahrzeugen für die Hafenlogistik eingesetzt werden und verbesserte Antriebssysteme bei Schiffen und Schwerlastverkehr genutzt werden.

Der Bereich smartPORT logistics sollte durch intelligente Infrastruktur den reibungslosen intermodalen Ablauf von Verkehrs- und Warenströmen managen. Dies sollte letztlich unter Verwendung der Elemente Bluetooth, Hotspots, WLan, Cloud, mobilen Endgeräten, dem Internet der Dinge und Big Data erfolgen.

Anders als die übrigen Projekte im Rahmen des MoU strebte HPA eine Pilotierung der Verfahren bereits zum Beginn der Welthafenkonferenz im Juni 2015 an, die zu diesem Zeitpunkt in Hamburg stattfand.

Im Rahmen unserer Kapazitäten hatten wir zunächst empfohlen, die Verfahren nochmals genauer auf die Verwendung personenbezogener Daten zu überprüfen, da auch Gerätenummern als zuordnungsfähige und damit personenbeziehbare Daten zu berücksichtigen sind. Gleiches galt für anfallende Arbeitnehmerdaten sowie den Einsatz von Videotechnik zu Detektionszwecken.

Im Mai 2015 erhielten wir auf Anfrage eine Liste der Projekte mit einer datenschutzrechtlichen Einschätzung des behördlichen Datenschutzbeauftragten sowie vereinzelt Kurzdarstellungen für eine kursorische Vorabkontrolle. Auf dieser Grundlage haben wir zu einzelnen Verfahren Nachfragen gestellt und Hinweise gegeben.

Während die Projekte aus dem Bereich smartPORT energy weniger datenschutzrechtliche Fragen aufwarfen, sollten mit smartPORT logistics zum Teil alle modernen Techniken eingesetzt werden, die durch Vernetzung Effektivitätssteigerungen versprechen.

Wie unter VI 2.1 dargestellt, haben diese Vorhaben die datenschutzrechtlichen Grundsätze zu berücksichtigen und die Rechte der Betroffenen zu gewährleisten. Dabei hatten wir uns zunächst auf die Sichtung der Teilprojekte beschränkt, zu denen wir zum Teil mit den betroffenen Stellen noch im laufenden Austausch stehen.

Werden die Teilprojekte zu umfassenderen Systemen wie etwa einem Port Road Management zusammengeschlossen und werden weitere Stellen beteiligt, erhöhen sich die datenschutzrechtlichen Anforderungen.

Grundsätzlich gilt, dass auch Pilotprojekte Echtdaten verarbeiten und deshalb durch gesetzliche Regelungen legitimiert sein müssen. Gerade im Verkehrsbereich sind die datenschutzrechtlichen Maßstäbe für die Nutzung personenbezogener Standortdaten noch unzureichend. In diesem Zusammenhang ist von Bedeutung, dass deshalb aktuell die Nutzung anonymisierter Standortdaten für Echtzeitanwendungen sowohl datenschutzrechtlich als auch technisch hinterfragt wird (vgl. VI 2.2 für Daten aus dem öffentlichen Verkehrsbereich). Bundesweit werden auch vertraglich mit den Betroffenen vereinbarte Auswertungen neu diskutiert. So wird auch im Verfahren smartPORT logistics zurzeit mit beim ADAC eingekauften anonymisierten Echtzeitdaten gearbeitet. Wir haben die HPA in diesem Zusammenhang auf unsere aktualisierten Anforderungen hingewiesen.

Eine weitere erfolgreiche Begleitung des Projekts smartPORT mit seinen vielen Unterprojekten durch uns wird auch gerade davon abhängig sein, wie sich die personelle Situation der Behörde künftig entwickelt.

2.5 Funkbasierte Ablesegeräte

Verbrauchsprofile über Mieter dürfen nicht erstellt werden, wenn Vermieter funkbasierte Ablesegeräte für Heizung sowie Wasser in ihren Wohnungen installieren.

Im Rahmen eines anstehenden regelmäßigen Austauschs der einfachen Heizkostenverteiler werden diese vermehrt durch ein funkbasiertes System ersetzt. Mieter sind damit allerdings vielfach nicht einverstanden und befürchten einen Eingriff in ihr Persönlichkeitsrecht, weil nun Verbrauchsprofile erstellt werden könnten.

In der Heizkostenverordnung (HeizkostenV) ist geregelt, dass der Eigentümer eine Pflicht zur Erfassung des Wärmeverbrauchs der Mieter hat. Dazu hat er die überlassenen Räume mit Ausstattungen zur Verbrauchserfassung zu versehen. Dies hat der Mieter nach § 4 Abs. 2 Satz 1, 2.Halbsatz HeizkostenV zu dulden. Diese Duldungspflicht erstreckt sich nach der Rechtsprechung (BGH, Urteil v. 28.09.2011- VIII ZR 326/10) auch auf den Einbau eines funkbasierten Ablesesystems zur Erfassung des Wärmeverbrauchs, sowie auf den Austausch vorhandener Messsysteme durch solche. Für den Austausch des Kaltwasserzählers folgt dieser Anspruch aus § 554 Abs. 2 BGB. Die Auswahl der Geräte obliegt allein dem Eigentümer. Eine Ablesetechnik, die das Betreten der Wohnung entbehrlich macht, erhöht nach der Verkehrsanschauung zudem den Wert einer Wohnung.

Die Wärmeverbrauchswerte von Nutzern zählen zu den vom Datenschutzrecht geschützten personenbezogenen Daten. Personenbezogene Daten dürfen nur im Rahmen des Erforderlichen und unter Beachtung des Prinzips der Datensparsamkeit verarbeitet werden. Um hinreichenden Datenschutz der Betroffenen zu gewährleisten, ist eine klare Regelung zu den Ablesemodalitäten erforderlich. Der Einsatz der Funkmessgeräte muss vertraglich zwischen Ablesedienstleister und Vermieter ausgestaltet sein und insbesondere die Häufigkeit der Erhebung von Verbrauchswerten regeln.

Es muss weiter konkret festgelegt sein, wie oft abgelesen wird, wer Zugriff auf diese Daten hat und wie lange diese gespeichert werden. Dabei darf keine Datenspeicherung auf Vorrat erfolgen, so dass die Erstellung von Nutzerprofilen ausgeschlossen wird. Weiterhin muss vertraglich sichergestellt sein, dass der Auslesevorgang nur von Berechtigten vorgenommen werden kann. Die Datenübertragung sollte in der Regel verschlüsselt an die Ablesefirma erfolgen.

Um datenschutzrechtliche Bedenken auszuräumen, muss vor allem sichergestellt sein, dass keine permanente Aufzeichnung und Speicherung der Verbrauchsdaten stattfindet, vielmehr eine Erhebung und Nutzung der Daten nur für die Heizkosten- oder Wasserabrechnung erfolgt.

Gegen eine jährliche, rückwirkende Ablesung, die dem bisherigen Vorgehen, wonach einmal im Jahr die Geräte ab- oder ausgelesen werden, entspricht, bestehen ebenso wie gegen die erforderliche Ermittlung von Zwischenergebnissen bei einem Nutzerwechsel keine Bedenken.

Die Verpflichtung zum Einbau von Wasserverbrauchszählern ergibt sich im Übrigen aus

§ 39 Abs. 3 Hamburgische Bauordnung (HBauO). Dem Vermieter obliegt die Pflicht, die Wasseruhren regelmäßig gemäß dem Eichgesetz zu tauschen.

2.6 Übermittlung von Mieterdaten durch Vermieter an Energieversorger

In bestimmten Fällen dürfen Vermieter Vor- und Zuname eines Mieters den Energieversorgern mitteilen.

Zeitgleich machten uns mehrere Anfragen von Wohnungseigentümern und Wohnungsbaugesellschaften auf ein datenschutzrechtliches Problem aufmerksam. Ursache waren Anfragen eines Energieversorgers beim Vermieter nach Vor- und Zuname des Mieters eines bestimmten Objektes, da Unklarheiten hinsichtlich des Vertragspartners für den Stromliefervertrag bestanden. Beim Grundversorger lag keine Anmeldung für die Lieferstelle vor. Für Verwirrung sorgte insbesondere die Formulierung: „Unsere Ermittlungen führten bisher nicht zum Erfolg, deshalb bitten wir Sie unter Berücksichtigung des § 28 Abs. 1 Nr. 2 BDSG um Auskunft." Die Vermieter hatten Zweifel, ob sie aus datenschutzrechtlicher Sicht berechtigt sind, Vor- und Zuname des Mieters dem Energieversorger mitzuteilen.

Nachdem wir die Angelegenheit mit dem Energieversorger ausführlich erörtert hatten, kamen wir zu folgendem datenschutzrechtlichen Ergebnis:

Der Vermieter darf Vor- und Zuname eines Mieters nach § 28 Abs. 2 Nr. 2a BDSG übermitteln. Ein schutzwürdiges Interesse des Betroffenen ist zu verneinen.

Nach § 36 des Gesetzes über die Elektrizitäts- und Gasversorgung (EnWG) sind in Hamburg zwei Energieversorgungsunternehmen Grundversorger für Strom und Gas. Nach § 2 Abs. 3 der Stromgrundversorgungsverordnung (StromGVV) besteht eine Mitteilungspflicht. Das OLG Nürnberg hat in einer Entscheidung (Urteil vom 23.05.2014 – 2 U 2401/12 – Rn. 29, 30) Folgendes ausgeführt:

„Nach der Rechtsprechung des Bundesgerichtshofs nimmt derjenige, der aus dem Verteilungsnetz eines Versorgungsunternehmens Elektrizität, Gas, Wasser oder Fernwärme entnimmt, das Angebot zum Abschluss eines entsprechenden Versorgungsvertrags konkludent an; eine etwaige Erklärung, er wolle mit dem Unternehmen keinen Vertrag schließen, ist unbeachtlich, da dies in Widerspruch zu seinem eigenen tatsächlichen Verhalten steht, d.h. er nimmt die Realofferte des Unternehmens durch sozialtypisches Verhalten an (BGH NJW-RR 2004, 928; NJWRR 2005, 639). Vertragspartner wird, wer auf Grund seiner Verfügungsmacht über den Versorgungsanschluss die Leistung entgegennimmt (BGH NJW 2003, 3131 ff. zur Wasserversorgung). Dies kann, muss aber nicht der Eigentümer sein.

Der Grundversorger hat, da der Vertragsschluss nicht durch übereinstimmende Willenserklärungen, sondern durch Annahme der Realofferte erfolgt, ein besonders schützenswertes rechtliches Interesse daran, unaufgefordert und unverzüglich darüber in Kenntnis gesetzt zu werden, wer sein Kunde ist. Nur wenn der Grundversorger die Person seines Vertragspartners kennt, kann er die mit dem Abschluss des Grundversorgungsvertrages verbundenen Entscheidungen sachgerecht treffen. So kann er zum Beispiel für den Elektrizitätsverbrauch eines Abrechnungszeitraums Vorauszahlungen verlangen, wenn er nach den konkreten Umständen Zahlungsausfall oder -verzögerung befürchten muss, § 14 Abs. 1 StromGVV."

Übermittelt wird letztlich nur der Vor- und Nachname eines neuen Mieters (oder mehrerer Mieter), Anschrift und Zählernummer sind ohnehin bekannt.

Die noch sonst auftretenden Sachverhalte (z.B. Auszug eines Mieters ohne neue Anschrift mit offenen Forderungen, Mitteilung einer eventuell neuen bekannten Anschrift) bleiben davon unberührt. In solchen Fällen ist wie bisher das berechtigte Interesse zu begründen.

Der Energieversorger hat mittlerweile seine Auskunftsersuchen geändert. Seitdem haben wir keine Beschwerden oder Anfragen mehr erhalten.

2.7 Prüfung der Kundendatenverarbeitung bei einer Wohnungsbaugesellschaft

Erhebliche datenschutzrechtliche Mängel offenbarten sich bei einer datenschutzrechtlichen Prüfung, die insbesondere die Auftragsdatenverarbeitung betrafen.

Ausgelöst durch mehrere Beschwerden von ehemaligen Mietern einer Wohnungsbaugesellschaft, die ein Informationsschreiben über das neue SEPA-Verfahren erhielten, aber schon seit Jahren keine Vertragsbeziehungen mehr unterhielten, hatten wir eine Prüfung der Mieterdatenverarbeitung vorgenommen. Themen waren

- die Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten,
- die Fachkunde des betrieblichen Datenschutzbeauftragten sowie seine Aufgabenwahrnehmung,
- das sog. Verfahrensverzeichnis,
- die Verpflichtungserklärung auf das Datengeheimnis,
- technische und organisatorische Maßnahmen bei der Verarbeitung von Mieterdaten sowie
- die Auftragsdatenverarbeitung.

Die umfangreiche Prüfung offenbarte erhebliche Defizite. Neben einer nicht den Anforderungen entsprechenden Übersicht über Verfahren automatisierter Verarbeitung (§ 4g Abs. 2 BDSG) mussten wir feststellen, dass die Anforderungen zur Auftragsdatenverarbeitung unzureichend erfüllt waren. Es fehlte ein Kontrollkonzept, obwohl § 11 Abs. 2 S. 4 BDSG den Auftraggeber verpflichtet, sich vor Beginn und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Dafür sind schriftliche Weisungen notwendig, die teilweise nicht mit dem Vertragsgegenstand in Einklang standen. Widersprüchliche oder fehlende Angaben zu Unterauftragsverhältnissen entsprachen ebenfalls nicht den Anforderungen.

Das Unternehmen hat aufgrund unserer zahlreichen Forderungen das Projekt Datenschutz ins Leben gerufen. Mit externer Unterstützung konnten die erheblichen Defizite behoben werden. Zudem wurde das Thema Datenschutz für das gesamte Unternehmen auf die Agenda gesetzt. Dazu gehörte auch, das Amt des betrieblichen Datenschutzbeauftragten intern in andere Hände zu geben.

Bei unserer Nachprüfung konnten wir uns von dem mittlerweile erreichten verbesserten Datenschutzstandard überzeugen.


NDELH

VIDEOÜBERWACHUNG VII.

1. Aktuelle Entwicklungen 200
2. Einzelfälle 202

1. Aktuelle Entwicklungen

1.1 Rechtsprechung

Im Berichtszeitraum erging durch den Europäischen Gerichtshof und deutsche Verwaltungsgerichte wegweisende Rechtsprechung zur Videoüberwachung öffentlich zugänglicher Räume durch private Stellen und Privatpersonen.

In Deutschland gibt es bisher nur verhältnismäßig wenig Rechtsprechung zum Datenschutzrecht. Umso bemerkenswerter ist es, dass im Berichtszeitraum mehrere, zum Teil wegweisende gerichtliche Entscheidungen zur Videoüberwachung öffentlich zugänglicher Räume durch private Stellen und Privatpersonen ergangen und rechtskräftig geworden sind.

So hat der Europäische Gerichtshof in seinem Urteil vom 11. Dezember 2014 - Rs. C-212/13 - festgestellt, dass eine Videoüberwachung des eigenen Grundstücks, die sich auch auf den öffentlichen Raum, wie zum Beispiel auf eine vor dem Grundstück gelegene Straße erstreckt, grundsätzlich in den Anwendungsbereich der Datenschutzrichtlinie 95/46/EG fällt. Ob eine solche Videoüberwachung im Einzelfall zum Schutz des Eigentums, der Gesundheit und des Lebens zulässig ist, muss im Rahmen der Interessenabwägung festgestellt werden. Ferner hat sich das Verwaltungsgerichts Ansbach (Urteil vom 12. August 2014 - AN 4 K 13.01634) mit dem Einsatz von sogenannten Dashcams in Pkw auseinandergesetzt. Im Ergebnis wird nach Auffassung des Gerichts durch eine im Fahrzeug angebrachte Kamera, welche nach dem Starten des Motors automatisch und permanent den Verkehrsraum vor dem Fahrzeug aufzeichnet, massiv in die Persönlichkeitsrechte anderer Verkehrsteilnehmer eingegriffen, ohne dass hierfür ein überwiegendes Interesse vorliege. Da die Voraussetzungen des § 6b BDSG nicht vorlägen, sei dies ein schwerer Verstoß gegen datenschutzrechtliche Vorschriften. Nicht ohne Kritik geblieben ist die Entscheidung des Oberverwaltungsgerichts Niedersachsen vom 29. September 2014 - 11 LC 114/13 - zur Zulässigkeit der Videoüberwachung des Treppenhauses in einem Bürogebäude. Danach kann sich die Eigentümerin und Verwalterin eines Objekts auch dann auf die Wahrnehmung berechtigter Interessen berufen, wenn sie im Fall eines Diebstahls in vermieteten Räumlichkeiten selbst gar nicht die Geschädigte ist, sondern die Mieter des Objekts. Dies wird von einigen Datenschutzaufsichtsbehörden abgelehnt. Wir halten es nicht für ausgeschlossen, dass sich verantwortliche Stellen auf „Schutzpflichten" gegenüber ihren Mietern berufen können. Dies gilt zumindest in den Fällen, in denen vertragliche Schuldverhältnisse zwischen den Parteien bestehen. Auch die vom Gericht als zulässig angesehene Löschfrist von 10 Tagen erachten die meisten Datenschutzaufsichtsbehörden mit Blick auf die Gesetzesbegründung des BDSG, die von einer Löschung nach ein bis zwei Arbeitstagen ausgeht, für zu lang. Das Verwaltungsgericht Schwerin befasste sich schließlich mit der Zulässigkeit einer touristischen Webcam (Beschluss vom 18.Juni 2015 - 6 B 1637/15 SN). Ein Vermieter von Ferienwohnungen hatte zu Werbungszwe-

cken und der Information potentieller Urlaubsgäste zwei Webcams installiert, die auf Strand, Marina, Fahrradweg und Strand-Promenade gerichtet waren. Die Live-Bilder der Kameras konnten von jedem Interessierten über das Internet betrachtet werden. Die Bildqualität der Kameras war nach Wertung des Gerichts so gut, dass Personen, die sich in den Erfassungsbereichen der Kameras aufhielten, zumindest bestimmbar waren. Das Gericht verneinte eine Zulässigkeit der Videoüberwachung nach § 6b BDSG für den dort entschiedenen Fall.

1.2 Orientierungshilfen und Beschlüsse der Datenschutzaufsichtsbehörden zur Videoüberwachung

Die Datenschutzaufsichtsbehörden haben mehrere Orientierungshilfen und Beschlüsse zur Videoüberwachung verabschiedet, die private Stellen und Privatpersonen über die Voraussetzungen eines zulässigen Einsatzes von Videotechnik informieren sollen.

Die AG Videoüberwachung des Düsseldorfer Kreises, an der wir mitwirken, hat im Berichtszeitraum die Orientierungshilfen „Videoüberwachung in öffentlichen Verkehrsmitteln" und „Videoüberwachung durch nicht-öffentliche Stellen" verabschiedet. Letztere wurde noch im Berichtszeitraum durch den Zusatz „Videoüberwachung in Schwimmbädern" ergänzt. Diese Orientierungshilfen sind ebenso wie der Beschluss „Nutzung von Kameradrohnen durch Private" auf unserer Homepage www.hamburg-datenschutz.de abrufbar.

Insbesondere die Orientierungshilfe „Videoüberwachung in öffentlichen Verkehrsmitteln" wurde im Kreis der Datenschutzaufsichtsbehörden kontrovers diskutiert. Dabei gilt es zu berücksichtigen, dass die Orientierungshilfe nicht nur über den zulässigen Einsatz von Videoüberwachungstechnik in den öffentlichen Verkehrsmitteln einer Großstadt wie Hamburg informieren will, sondern auch den länderübergreifenden Schienenverkehr mit mehrstündigen Fahrtzeiten und der Präsenz von Zugbegleitern im Blick hat. In diesem Licht ist auch die in der Orientierungshilfe getroffene Aussage zu sehen, eine generelle, zeitlich und räumlich durchgängige Videoüberwachung des gesamten Fahrgastbereichs sei nach § 6b BDSG in aller Regel unverhältnismäßig und somit unzulässig. In Hamburg sind seit einigen Jahren alle Busse, S- und U-Bahnen sowie HADAG-Fähren überwacht (vgl. 22.TB, IV. 1.1). Eine zeitlich und räumlich lückenlose Überwachung des Fahrgastraums, der sich die Fahrgäste nicht entziehen können, stellt unzweifelhaft einen intensiven Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen dar. Wir halten diesen aber mit Blick auf die überschaubaren Fahrtzeiten im Stadtgebiet Hamburg, der Ausgestaltung als Black-Box-Verfahren (vgl. 21. TB, 19.1) und zuletzt auch aufgrund der Gefährdungslage, wie sie in einer

Großstadt wie Hamburg besteht, nicht für unverhältnismäßig.

Wir erwarten mit Interesse ein Urteil aus Niedersachsen. Dort ist ein Verwaltungsgerichtsverfahren zum Einsatz von Videoüberwachungstechnik in öffentlichen Verkehrsmitteln anhängig. Das betroffene Verkehrsunternehmen hat gegen eine Anordnung des Niedersächsischen Datenschutzbeauftragten, die Kameras in Bussen und Bahnen abzuschalten, geklagt. Wir werden den Ausgang des dortigen Verfahrens genau beobachten.

2. Einzelfälle

2.1. Kfz-Kennzeichenerkennung in Parkhäusern am Hamburger Flughafen

Der Einsatz von Kennzeichenerkennungssystemen in Parkhäusern kann im Einzelfall zulässig sein.

Durch zwei Bürgerbeschwerden wurden wir auf den Einsatz eines Kennzeichenerkennungssystems in Parkhäusern des Hamburger Flughafens aufmerksam. Beim Befahren der Parkhäuser wird mit Hilfe einer Kamera ein Frontbild des Fahrzeugs inkl. des Kennzeichens gespeichert. Die Fahrerin oder der Fahrer und Insassen werden von der Kamera nicht erfasst. Dieses Bild wird mit dem Parkticket „verknüpft". Bei der Ausfahrt wird das erfasste Kennzeichen mit dem zur Ticketnummer hinterlegten Einfahrtskennzeichen verglichen. Im Falle einer Übereinstimmung und erfolgter Zahlung öffnet sich die Ausfahrtschranke. Wir konnten nach einem Gespräch mit der verantwortlichen Stelle bereits im Verlauf unserer Kontrolle erreichen, dass die Bilddaten spätestens fünf Minuten nach der Ausfahrt gelöscht werden. Dieses für Kurzparker eingesetzte Verfahren wird in ähnlicher Form auch für Dauerparker angewendet. Nach Aussage des verantwortlichen Flughafenunternehmens sollen durch die Kennzeichenerkennung vorrangig Betrugsversuche zu Lasten der Betreiberin verhindert werden. Parkhausnutzer würden nach einer langen Parkdauer häufig behaupten, das entsprechende Ticket verloren zu haben und machten auf Nachfrage nicht selten unwahre Angaben zur tatsächlichen Parkdauer, um Parkgebühren zu sparen.

Von einer Erforderlichkeit des Einsatzes eines Kennzeichenerkennungssystems in einem Parkhaus kann im Falle von Kurzparkern ausgegangen werden, wenn der Betreiber oder die Betreiberin für die in der Vergangenheit eingetretenen Einnahmeverluste entsprechende betriebswirtschaftliche Belege liefert und diese Verluste nicht unerheblich sind. Diese Belege wurden uns von dem verantwortlichen Flughafenunternehmen vorgelegt.

Unseres Erachtens stehen dem Einsatz des Kennzeichenerkennungssystems unter bestimmten Voraussetzungen auch keine überwiegenden schutzwürdigen Interessen der Parkhausnutzer entgegen. So muss weiterhin die Möglichkeit bestehen, Parkflächen am Hamburger Flughafen ohne Kennzeichenerkennung zu nutzen. Dies schließt einen flächendeckenden Einsatz der Technik in Parkhäusern des Hamburger Flughafens aus. Auch ist frühzeitig auf die Kennzeichenerkennung hinzuweisen, damit für die Fahrerinnen und Fahrer noch vor der Einfahrt in die betreffenden Parkhäuser realistische Wendemöglichkeiten gegeben sind. Ferner ist bei der Weiterentwicklung des Produkts eine automatische Löschung der Bilddaten unmittelbar nach der Ausfahrt vorzusehen. Bei Dauerparkern setzt ein datenschutzkonformer Einsatz des Kennzeichenerkennungssystems hingegen eine informierte Einwilligung der betroffenen natürlichen Personen voraus.

Das verantwortliche Flughafenunternehmen hat uns zugesagt, die Voraussetzungen für einen datenschutzkonformen Einsatz des Kennzeichenerkennungssystems einzuhalten. Dabei ist zu betonen, dass sich diese Bewertung nur auf den Einsatz des Systems in den Parkhäusern am Hamburger Flughafen bezieht. Eine generelle Zulässigkeit des Verfahrens z.B. in kleinen Parkhäusern in der Innenstadt oder auf Campingplätzen kann aus dieser Einzelfallbetrachtung nicht abgeleitet werden.

2.2 Open Library

Die Erforderlichkeit einer Videoüberwachung der Bücherhalle Finkenwerder während der personallosen Öffnungszeiten muss von der verantwortlichen Stelle noch belegt werden.

In den Niederlanden und Dänemark können Bibliotheken seit einigen Jahren auch außerhalb von „regulären" Öffnungszeiten, in denen Personal anwesend ist, in Selbstbedienung genutzt werden. Die Stiftung Hamburger Öffentliche Bücherhallen (HÖB) hat diesen Selbstbedienungsservice Ende 2014 im Rahmen eines Pilotprojekts eingeführt und uns hierüber vor der Inbetriebnahme informiert. Die Pilot-Bücherhalle Finkenwerder wurde räumlich umgestaltet und für die erweiterten personallosen Öffnungszeiten vorbereitet. Neben einer Selbstbedienungsausleihe gibt es auch eine Selbstbedienungsrückgabe. Hierbei kommt RFID-Technik zum Einsatz. Kundinnen und Kunden können die Eingangstür der Bücherhalle an einem Zugangsterminal zu den definierten Zeiten mit ihrer Bibliothekskundenkarte selbständig öffnen, ähnlich der Zugangspraxis zur Selbstbedienungszone in Banken. Das Terminal prüft dabei am Zentralserver anhand der Kundenkarte die Zugangsberechtigung. Während der Selbstbedienungs-Öffnungsstunden zeichnen vier Kameras das Geschehen in den Bibliotheksräumen auf. Auf die Videoüberwachung wird deutlich durch mehrere Schilder hingewiesen. Vor der Inbetriebnahme der Open Library wurde zudem eine Informationsveranstal-

tung für Kundinnen und Kunden der Bücherhalle Finkenwerder durchgeführt. Auf der Internetseite der HÖB wird ebenfalls über das Projekt informiert. Die Bücherhalle ist ferner mit einem RFID-Gitter zur Diebstahlssicherung ausgestattet. Während der personallosen Öffnungszeiten erhalten in der ersten Phase nur Kundinnen und Kunden ab 18 Jahren Zutritt und es wird nur eine begrenzte Anzahl von zusätzlichen Öffnungsstunden angeboten. Später sollen die Open Library-Zeiten sukzessiv erweitert werden. Bei erfolgreichem Projektverlauf soll die Open Library auch an weiteren Standorten der HÖB eingeführt werden. Geschäftsleitung und Betriebsrat der Stiftung haben eine Betriebsvereinbarung zum Pilotprojekt abgeschlossen. In dieser Betriebsvereinbarung ist festgehalten, dass die Open Library-Zeiten die bisherigen personalbesetzten Öffnungszeiten der Bücherhalle Finkenwerder nicht ersetzen sollen.

Die HÖB verfolgt mit dem Betrieb der Videoüberwachung während der personallosen Öffnungszeiten präventive und repressive Ziele. Einer Aufzeichnung der Überwachungsbilder stehen dem Grunde nach keine überwiegenden schutzwürdigen Interessen der Kundinnen und Kunden entgegen, sofern weiterhin die (Wahl-)Möglichkeit besteht, die Einrichtung überwiegend überwachungsfrei nutzen zu können, der Umstand der Videoüberwachung transparent ist und Lesebereiche von der Videoüberwachung ausgenommen sind.

Eine Videoüberwachung muss aber nicht nur verhältnismäßig, sondern auch erforderlich sein. Die abschreckende Wirkung von Kameras ohne Monitoring durch interventionsbereites Aufsichtspersonal ist umstritten. Wir haben somit Zweifel, ob die von der HÖB gewählte Form der Videoüberwachung als reine Aufzeichnungslösung geeignet ist, die Erreichung der überwiegend präventiven Ziele, wie die Verhinderung von Vandalismus, Gewalt gegen Personen und Diebstahl sowie die Erhöhung des Sicherheitsgefühls der Kunden zu fördern. Selbst wenn eine präventive Wirkung der gewählten Lösung anzunehmen wäre, müsste die HÖB noch belegen, dass keine milderen Mittel zur Erreichung der verfolgten Zwecke zur Verfügung stehen. Denkbar wäre hier der Einsatz von Aufsichtspersonal vor Ort und mit Blick auf die geplante Ausweitung auf andere Standorte auch ein zentrales Monitoring durch Aufsichtspersonal, welches die Möglichkeit hat, bei entsprechenden Vorfällen Aufzeichnungen zu starten. Es reicht jedenfalls nicht aus, lediglich darauf zu verweisen, dass derartige Projekte in den Niederlanden und Dänemark erfolgreich und nach dortigem Recht zulässig waren. Wir haben die HÖB daher gebeten, uns eine entsprechende (Kosten-) Vergleichsrechnung vorzulegen, in der der Betrieb von Videoüberwachungstechnik einem möglichen Personaleinsatz gegenübergestellt wird. Eine aussagefähige Vergleichsrechnung liegt noch nicht vor. Wir haben mit der HÖB vereinbart, die Gespräche hierzu im Jahr 2016 fortzuführen.

2.3 Videoüberwachung in Fitness- und Wellnessclubs

Eine Videoüberwachung in Umkleidebereichen von Fitness- und Wellnessanlagen ist datenschutzrechtlich nicht zulässig.

Im Berichtszeitraum haben uns wieder mehrere Beschwerden zur Videoüberwachung in Fitness- und Wellnessclubs erreicht. Im Wesentlichen richteten sich diese Beschwerden gegen die zumindest teilweise Videoüberwachung der Gemeinschaftsumkleideräume. Wir haben diese Beschwerden zum Anlass genommen, die Videoüberwachung in den Anlagen zweier unterschiedlicher Betreiberinnen zu kontrollieren. Bei unserer Kontrolle stellten wir fest, dass beide Betreiberinnen eine reine Aufzeichnungslösung für die Überwachung der Umkleideräume gewählt haben. Eine dauerhafte Beobachtung am Monitor findet nicht statt. Aufgrund der Gestaltung der Umkleidebereiche in den kontrollierten Anlagen führt die Videoüberwachung der Spinde/Schränke auch immer zu einer Überwachung der nackten oder nur teilweise bekleideten Mitglieder und Gäste, die sich direkt vor den Schränken umziehen und die Ablageflächen vor den Schränken nutzen.

Im Ergebnis halten wir die Videoüberwachung der Umkleideräume nicht für erforderlich und mit Blick auf die Schutzwürdigkeit der erhobenen und gespeicherten Bilddaten auch nicht für verhältnismäßig. Die schutzwürdigen Interessen der von Videoüberwachung im Spind- und Umkleidebereich betroffenen Mitglieder und Gäste können nur dann zurückstehen, wenn der Schutz überragender Rechtsgüter eine Aufzeichnung dieser Bilder erfordert. Ein solches höherwertiges Interesse an der Videoüberwachung ist allein mit dem Schutz des Eigentums an den Spinden/Schränken oder der Gewährleistung einer guten Reputation nicht zu begründen. Dass keine dauerhafte Beobachtung stattfindet und nur bei Hinweisen auf konkrete Vorfälle Einsicht in die Bilder genommen wird, ändert nichts an der Eingriffsintensität, die durch die Speicherung der Videobilder gegeben ist. Diese ist aufgrund der Missbrauchsmöglichkeiten bei gespeicherten Nacktbildern hoch. Ferner ist der Grundsatz zu berücksichtigen, dass die Anforderungen an die Wahrscheinlichkeit eines Schadenseintritts umso niedriger sind, je schwerer der eintretende Schaden wäre. Der Schaden für das Persönlichkeitsrecht der Betroffenen wäre bei der Verbreitung von Nacktaufnahmen gerade in Zeiten des Internet denkbar hoch. Weiterhin ist auf die zur Videoüberwachung ergangene Rechtsprechung abzustellen. Das AG Hamburg hat zur Überwachung von Sitzbereichen in einem Kaffeehaus festgestellt, dass die Persönlichkeitsrechte der sich in den Sitzbereichen länger aufhaltenden Kunden durch eine ständige Videoüberwachung erheblich beeinträchtigt werden und diese Rechtsverletzungen schwerer wiegen als die Interessen des Kaffeehausinhabers an einer effektiven Strafverfolgung in seinen Filialen (AG Hamburg, Urt. v. 22.April 2008 - 4 C 134/08). Wenn jedoch eine ebenfalls dem Freizeitbereich zuzuordnende Aktivität, wie der Besuch eines Cafés, schon über-

wachungsfrei sein soll, so muss dies erst recht für Umkleidebereiche von Schwimmbädern sowie Fitness- und Wellnessanlagen gelten, in denen Menschen nicht nur miteinander kommunizieren, sondern sich sogar entkleiden.

Dieser Bewertung steht auch nicht entgegen, dass wir in der Vergangenheit eine Videoüberwachung von Teilbereichen der Umkleideräume in Fitness- und Wellnessanlagen für zulässig erachtet haben (vgl. 21.TB, 19.3). Nach dieser Bewertung im Jahre 2007 sind verschiedene Änderungen eingetreten: Das o.g. Urteil des AG Hamburg erging erst nach unserer ersten Einschätzung zur Zulässigkeit der Videoüberwachung in Gemeinschaftsumkleidebereichen. Da in einem Rechtsstaat jedoch die Gerichte abschließend über die Auslegung des anwendbaren Rechts entscheiden, ist dieser Auslegung zu folgen. Ferner gab es seit 2007 kontinuierlich Eingaben/Bürgerbeschwerden zu der in den Umkleideräumen vorgenommenen Videoüberwachung. Unsere Entscheidung, eine abgrenzbare Videoüberwachung der Umkleidebereiche als zulässig zu erachten, sofern es ausreichend und als solche gekennzeichnete überwachungsfreie Umkleidemöglichkeiten für Besucherinnen und Besucher gibt, führte nicht zu einer Verringerung des Beschwerdeaufkommens. Dies ist ein deutlicher Anhaltspunkt für das Überwiegen der schutzwürdigen Interessen der Betroffenen in diesen Bereichen, den wir bei der notwendigen Interessenabwägung berücksichtigen müssen.

Wir haben die Betreiberinnen daher aufgefordert, die Videoüberwachung der Umkleideräume während der Geschäftszeiten einzustellen. Ein Unternehmen hat als Reaktion hierauf schon mitgeteilt, die Videokameras in den Umkleideräumen sämtlicher Anlagen bis Mitte 2016 zu demontieren. Wir werden über den weiteren Verlauf dieser Kontrollverfahren berichten.

2.4 Videoüberwachung in einer Kindertagesstätte

Der Wunsch einer Leitungskraft, während der eigenen Abwesenheit „nach dem Rechten sehen zu wollen", rechtfertigt keine dauerhafte Videoüberwachung von Beschäftigten.

Aufgrund einer Beschwerde sind wir an eine Kindertagesstätte herangetreten, die in ihren Räumlichkeiten mehrere Videoüberwachungskameras installiert hat. Bei unserer Kontrolle der Einrichtung stellten wir fest, dass sämtliche Gruppenräume, in denen sich die Kinder und ihre Betreuerinnen regelmäßig aufhalten, mit Überwachungskameras ausgestattet sind. Die Leitung räumte ein, nur selten selbst vor Ort zu sein, da sich ihr Büro in einer weiteren Kindertagesstätte befinde, die sie ebenfalls leite.

An der Aussage der Leitung, sie würde die Überwachung nur außerhalb der Öffnungszeiten der Kindertagesstätte zur Abschreckung von Einbrechern vornehmen, hatten wir erhebliche Zweifel. Unsere Zweifel beruhten auf mehreren Umständen. So fanden sich

im Außenbereich der Kindertagesstätte kaum sichtbare Hinweise auf die Videoüberwachung, was mit Blick auf die behauptete abschreckende Wirkung der Videoüberwachung nicht nachvollziehbar war. Auch die mangelnde Qualität der Überwachungsbilder bei Dunkelheit und widersprüchliche Angaben zum Remote-Zugriff bestärkten unsere Zweifel an der Aussage, die Videoüberwachung diene nur zur Abschreckung potentieller Einbrecher und zur Erlangung von Beweismitteln im Falle von Einbrüchen. Schließlich sprach auch der Versuch, von den Mitarbeiterinnen Einverständniserklärungen in eine Videoüberwachung einzuholen, für einen anderen Überwachungszweck, da solche Einverständniserklärungen für eine außerhalb der Öffnungszeiten stattfindende Videoüberwachung gar nicht notwendig gewesen wären. Die Ausgestaltung der Videoüberwachung legte vielmehr den Schluss nahe, dass sich die Leitung während ihrer Abwesenheit per Remote-Zugriff die Möglichkeit eröffnen wollte, „nach dem Rechten zu sehen".

Da wir der Leitung einen Betrieb der Videoüberwachungsanlage während der Geschäftszeiten nicht nachweisen konnten, mussten wir es bei der Darlegung der Rechtslage belassen und auf aufsichtsbehördliche Maßnahmen verzichten. Wir haben der Leitung der Kindertagesstätte daher mitgeteilt, dass eine Überwachung (Live-Beobachtung am Monitor) und/oder Speicherung der Aufnahmen während der Öffnungszeiten - insbesondere mit Blick auf die damit einhergehende Überwachung der Mitarbeiterinnen - nach § 32 BDSG nicht zulässig ist. Das Beschäftigteninteresse, von einer derartigen Dauerüberwachung verschont zu bleiben, überwiegt zumindest dann, wenn der Arbeitgeber mit der Überwachung nur befürchteten Verfehlungen seiner Beschäftigten präventiv begegnen will, ohne dass hierfür konkrete Anhaltspunkte bestehen oder er „einfach nur mal nach dem Rechten sehen will". Wir haben weiterhin mitgeteilt, dass wir bei zukünftigen Hinweisen, die auf einen Einsatz der Videoüberwachungsanlage zu Zwecken der Beschäftigtenkontrolle schließen lassen, nicht zögern werden, ein Bußgeld zu verhängen.

2.5 Polizeiliche Videoüberwachung als automatisiertes Verfahren

Nach einem Urteil des Europäischen Gerichtshofs ist eine Videoaufzeichnung auf einer kontinuierlichen Speichervorrichtung eine automatisierte Verarbeitung. An diese Rechtsauslegung ist auch die Polizei gebunden.

Die Polizei Hamburg vertritt seit langer Zeit die Auffassung, eine Videoüberwachung stelle kein automatisiertes Verfahren dar und beruft sich hierbei auf eine Kommentierung in der Literatur zum Bundesdatenschutzgesetz. Hiernach soll mit Blick auf eine Videoüberwachung erst dann eine automatisierte Verarbeitung vorliegen, wenn die

Datenverarbeitung in einem automatischen Verarbeitungssystem erfolgt, welches zwischen den Daten unterschiedlicher Personen unterscheiden und darauf aufbauend die Verarbeitung steuern kann, wie dies zum Beispiel bei Videosystemen mit integrierter Gesichtserkennung der Fall ist. Das bloße Abspielen und Aufzeichnen von Videosequenzen sei daher keine automatisierte Verarbeitung. Gestützt auf diese Argumentation erstellt die Polizei auch keine Risikoanalysen (vgl. zuletzt 24.TB, 1.4), die nach § 8 Abs. 4 Satz 1 HmbDSG bei Einführung oder wesentlicher Änderung eines „automatisierten Verfahrens" zu fertigen sind.

Wir haben in der Vergangenheit die Auffassung der Polizei in dieser Frage nicht geteilt und halten sie im Lichte des zwischenzeitlich ergangenen Urteils des Europäischen Gerichtshofs (EuGH) vom 11. Dezember 2014,- Rs. C-212/13 - auch nicht mehr für vertretbar. Das Urteil des EuGH ist hier eindeutig: „Eine Überwachung mittels einer Videoaufzeichnung von Personen auf einer kontinuierlichen Speichervorrichtung, der Festplatte, stellt eine automatisierte Verarbeitung personenbezogener Daten gemäß Art. 3 Abs. 1 der Richtlinie 95/46 dar" (Rn. 25). Der in § 8 Abs. 4 HmbDSG verwendete Begriff des „automatisierten Verfahrens" dient laut Gesetzesbegründung der Umsetzung der Datenschutzrichtlinie 95/46 (vgl. Bü.-Drs. 16/3995, Seite 9), zu der der EuGH geurteilt hat. Es gibt daher keinen Grund anzunehmen, dass der Begriff des „automatisierten Verfahrens" im HmbDSG anders zu verstehen ist als der Begriff der „automatisierten Verarbeitung" in der Richtlinie 95/46/EG. Als Teil der vollziehenden Gewalt ist die Polizei an die Rechtsauslegung durch die Gerichte gebunden. Der EuGH ist das höchste Gericht für die Auslegung der Richtlinie 95/46/EG, deren Umsetzung § 8 Abs. 4 HmbDSG dient. Wir können daher nicht erkennen, dass die Ansicht der Polizei, polizeiliche Überwachungen mittels Videoaufzeichnung auf einer kontinuierlichen Speichervorrichtung fielen nicht unter § 8 Abs. 4 HmbDSG, weiterhin vertretbar ist. Auch die bislang von der Polizei zitierte Kommentarstelle dürfte so keinen Bestand haben. Auf Nachfrage der Bürgerschaft konnten die Senatsvertreter bei der öffentlichen Sitzung des Ausschusses für Justiz, Datenschutz und Gleichstellung am 15. Januar 2015 zum Tagesordnungspunkt 5 nicht begründen, was gegen die Erstellung einer Risikoanalyse sprechen könnte (siehe Protokoll Nr. 20/42, Seite 17 a.E.). Die Abgeordneten der SPD-Fraktion hatten sich dafür ausgesprochen, der Polizei Zeit für die Umsetzung des EuGH-Urteils einzuräumen (siehe Protokoll Nr. 20/42, Seite 18). Wir gehen davon aus, dass die Polizei das Urteil des EuGH zeitnah zum Anlass nimmt, von der bisherigen, nun nicht mehr vertretbaren Rechtsansicht abzurücken.


HANDELSKAMM

WIRTSCHAFT UND FINANZEN VIII.

1. Kreditwesen und Auskunfteien 212
2. Finanzen, Steuern und Rechnungswesen 225
3. Versicherungswirtschaft 231
4. Handel und Werbung 234
5. Unterlassungsklagengesetz 234

1. Kreditwesen und Auskunfteien

1.1 Scoring-Gutachten bei einer Auskunftei

Für Datenschutzaufsichtsbehörden ist es nahezu nicht möglich, selbst zu prüfen, ob die zur Berechnung eines Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind.

Uns erreichten in der Vergangenheit immer wieder Eingaben, die sich auf die Tatsache bezogen, dass Auskunfteien über Betroffene Scorewertberechnungen an Dritte übermitteln, die einerseits nicht konkret nachvollziehbar sind und andererseits nicht der individuellen Bonität der Einzelnen entsprechen. Die Aufsichtsbehörden haben auch schon früher immer wieder ihr Augenmerk auf diese Scorewertberechnungen gerichtet, konnten jedoch die Betroffenen angesichts der Undurchschaubarkeit einzelner Berechnungen nicht in jedem Fall zufrieden stellen.

Grund dafür ist die geltende Rechtslage, die es den Auskunfteien gemäß § 28b Bundesdatenschutzgesetz (BDSG) ermöglicht, derartige Berechnungen anzustellen und nach § 29 BDSG bei berechtigtem Interesse auch an Dritte zu übermitteln. Neben der Tatsache, dass sich die Unternehmen an die Voraussetzungen der Auskunfteienregelungen, insbesondere auch der Information der Betroffenen über erstmals erfolgte Übermittlungen (vgl. 23. TB, VI. 6.4) und Benennung in Selbstauskünften halten müssen, stellt § 28b BDSG die Regeln auf, unter denen Scorewertberechnungen zulässig sind.

Danach müssen die Voraussetzungen für eine Übermittlung nach § 29 vorliegen, das heißt, es dürfen nur personenbezogene Daten in die Berechnung einfließen, die durch die Auskunftei in zulässiger Weise gespeichert sind und auch übermittelt werden dürften. Sofern Anschriftendaten genutzt werden, dürfen diese nicht die alleinige Berechnungsgrundlage sein und die Betroffenen müssen bereits im Vorwege über die beabsichtigte Nutzung zu einer Berechnung des Wahrscheinlichkeitswertes unterrichtet werden – in der Regel geschieht dies durch Vertragspartner der Auskunfteien. Diese Merkmale sind durch die Datenschutzaufsichtsbehörden ohne weiteres nachprüfbar.

Mehr Schwierigkeiten macht jedoch die wichtige Voraussetzung, dass die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind. Eine vollständige Überprüfung dieses Erfordernisses ist außerordentlich schwierig und setzt eine entsprechende Ausbildung voraus, die in den Aufsichtsbehörden regelmäßig nicht verfügbar ist. Gleichwohl bestehen immer wieder Zweifel daran, dass die

Auskunfteien mit den ihnen zur Verfügung stehenden personenbezogenen Daten tatsächlich aussagekräftige Wahrscheinlichkeitswerte berechnen können. Letztlich fehlt es an diesem Punkt an der sonst für das Datenschutzrecht so wichtigen Transparenz.

Aus diesem Grund haben wir eine in Hamburg ansässige Auskunftei aufgefordert, uns durch Beibringung eines entsprechenden externen wissenschaftlichen Gutachtens nachzuweisen, dass die in § 28b Nr.1 Bundesdatenschutzgesetz (BDSG) genannten Voraussetzungen zur Berechnung des Wahrscheinlichkeitswertes eingehalten werden. Nachdem dieses Gutachten seitens des Unternehmens bereits für etwa Mitte 2014 avisiert worden war, hat es diesbezüglich immer wieder erhebliche Verzögerungen gegeben. Das endgültige Gutachten lag dann erst im März 2015 vor. Eine inhaltliche Bewertung des Gutachtens konnte von uns zwar nicht vollständig vorgenommen werden. Allerdings erscheint es plausibel und kommt zu dem Ergebnis, dass die gesetzlichen Vorgaben beachtet werden.

1.2 Betrugspräventions-Dateien für Kreditinstitute

Im Berichtszeitraum wurden zwei neue Betrugspräventions-Dateien für Kreditinstitute errichtet, die auch in Zukunft sehr genau im Hinblick auf datenschutzgerechte Gestaltung von den Aufsichtsbehörden beobachtet werden.

Erstmals im Jahre 2007 erhielten die Datenschutzaufsichtsbehörden Informationen über Planungen, ein Betrugspräventionssystem für Kreditinstitute bei einer Auskunftei einzurichten. Die erste Entwurfsfassung sah vor, zwischen einzelnen Kreditinstituten und einer Auskunftei Auftragsdatenverarbeitungsverträge abzuschließen, um einen bankenübergreifenden Informationsaustausch zum Schutz vor Betrügern zu ermöglichen. Nach intensiver bundesweiter Befassung der Aufsichtsbehörden mit dieser Thematik und Erörterung der kritischen Punkte wurde das Vorhaben zunächst aufgegeben.

Im Zuge eines Ausschreibungsprojekts des Bankenfachverbandes griffen jedoch mehrere Auskunfteien – darunter auch ein hamburgisches Unternehmen – die Idee der Einrichtung einer Betrugspräventions-Datei 2013 wieder auf und informierten darüber auch die Datenschutzaufsichtsbehörden. Erste Gespräche zu Einzelheiten der Planungen zeigten jedoch, dass diese noch nicht in einer Weise vorangeschritten waren, die eine seriöse datenschutzrechtliche Begleitung durch die Aufsichtsbehörde sinnvoll erscheinen ließ.

Anfang 2014 erreichten uns dann Unterlagen, die eine Auseinandersetzung auch unter Beteiligung weiterer Datenschutzaufsichtsbehörden ermöglichten. Eine Einbeziehung aller Aufsichtsbehörden war unumgänglich, da die Meldungen an die Auskunftei von

jedem angeschlossenen Kreditinstitut erfolgen können sollen und daher die Datenschutzaufsichtsbehörden nahezu aller Bundesländer betroffen sind. Schon die Übermittlungen an die Auskunftei müssen nämlich auf ihre Vereinbarkeit mit dem Datenschutzrecht kontrolliert werden.

Neben etlichen Einzelpunkten der datenschutzrechtlichen Ausgestaltung einer solchen Auskunftei wurde insbesondere die Frage ausführlich diskutiert, ob es sich bei § 25h des Kreditwesengesetzes (KWG) um eine abschließende Vorschrift handelt, die die Anwendbarkeit des Bundesdatenschutzgesetzes (BDSG) ausschließt. § 25h KWG ermöglicht lediglich eine Übermittlung besonders benannter personenbezogener Daten zwischen Kreditinstituten im Einzelfall, nicht jedoch den Abruf aus einer Sammlung personenbezogener Daten, die von einer Auskunftei betrieben wird. Gerade um die Einrichtung einer solchen institutsübergreifenden Warnfunktion im Zusammenhang mit möglichen Straftaten gegen Kreditinstitute geht es jedoch der Kreditwirtschaft. Nach eingehenden Diskussionen in den federführenden Arbeitsgruppen Kreditwirtschaft und Auskunfteien, Erörterungen im Düsseldorfer Kreis der Datenschutzaufsichtsbehörden des Bundes und der Länder, der Einholung von Stellungnahmen des Bundesfinanzministeriums und der Bundesanstalt für Finanzdienstleistungsaufsicht hat der Düsseldorfer Kreis sich mit großer Mehrheit zu diesem Thema positioniert und Kriterien verabschiedet, bei deren Berücksichtigung Betrugspräventions-Dateien in der Kreditwirtschaft zulässig sein können.
Dazu wurden bundeseinheitliche Mindeststandards entwickelt, die es gewährleisten sollen, dass in zulässiger Art und Weise geführte Datenbanken mit dem geltenden Datenschutzrecht vereinbar sind. Grundlage dafür ist eine Abwägung zwischen den Interessen der Kreditwirtschaft an der Minimierung des jeweiligen Vermögensrisikos und den schutzwürdigen Interessen der Betroffenen. In diesem Zusammenhang wurden Mindeststandards zur Betrugsprävention bei Banken aufgelistet, die sich auf die Einmeldung seitens der Kreditwirtschaft in den Pool, die Speicherung und Nutzung dieser Daten in dem Pool sowie auf die Übermittlung von Daten aus dem Pool beziehen. Im Einzelnen werden dabei folgende Anforderungen aufgestellt:

a) Für die Einmeldung in den Pool: Es dürfen grundsätzlich keine Daten auf Einwilligungsbasis und keine besonderen Arten personenbezogener Daten (= rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) eingemeldet werden. Hinsichtlich der Einwilligungseinschränkung gilt die Ausnahme, dass etwa Opfer von Identitätsbetrug gerade nur mit ihrer Einwilligung eingemeldet werden dürfen. Hinsichtlich der von qualifiziertem Personal einzumeldenden Sachverhalte muss es im Vorwege klare Fallgruppenbildungen geben, die erhebliche und beweisbare Vorwürfe beinhalten müssen.

b) Für die Speicherung und Nutzung im Pool: Der Betroffene muss über seine konkrete Einmeldung in den Pool unterrichtet werden. Darüber hinaus muss gewähr-

leistet werden, dass alle Auskunfts-, Löschungs- und Berichtigungsrechte beachtet werden. Für Bonitätsauskünfte oder zur Berechnung von Scorewerten dürfen diese konkreten personenbezogenen Daten nicht genutzt werden.

c) Für die Übermittlung aus dem Pool: Das Vorliegen eines berechtigten Interesses an der Auskunft ist zu überprüfen. Darüber hinaus dürfen nur die zur Warnung der anfragenden Stelle absolut notwendigen Daten übermittelt werden. Die übrigen für Auskunfteien immer geltenden Anforderungen wie etwa die Dokumentation des berechtigten Interesses und die Durchführung von Stichprobenverfahren sind selbstverständlich einzuhalten. Bei der anfragenden Stelle darf die Warnung nicht zu einem Ablehnungs-Automatismus führen, sie darf sie nur zum Anlass einer genaueren Überprüfung des Sachverhalts heranziehen.

Wichtig ist in diesem Kontext, dass es sich keineswegs um die allein anzulegenden Kriterien handelt, sondern lediglich um Mindeststandards, die eingehalten werden müssen. Ob eine Auskunftei tatsächlich den rechtlichen Voraussetzungen – auch unter Einbeziehung der Problematik des § 25h KWG - entspricht, ist einzelfallbezogen zu kontrollieren.

Die Begleitung der Planungen des bereits erwähnten hamburgischen Unternehmens setzte sich 2014 und 2015 sehr intensiv fort. Dabei wurden sowohl die Frage der Zulässigkeit eines solchen Portals vor dem Hintergrund der Vorschriften des Kreditwesengesetzes, als auch die vom Düsseldorfer Kreis aufgestellten Mindeststandards eingehend erörtert. Das Unternehmen teilte uns zunächst mit, dass es die Verantwortung für die Einholung etwaiger Genehmigungen des Bundesamtes für Finanzdienstleistungsaufsicht bei den einzelnen Kreditinstituten sehe und in den abzuschließenden Verträgen darauf hinweisen werde. Vorbehaltlich weiterer Prüfungen konnte zumindest dieser Punkt akzeptiert werden. Bedauerlicherweise nahm das Unternehmen von dieser Zusage dann aber wieder Abstand. Hierzu hat inhaltlich eine intensive rechtliche Auseinandersetzung stattgefunden.
Darüber hinaus gab es jedoch noch weitere Problematiken, die Anlass zu einer Vielzahl von schriftlichen und mündlichen Diskussionen mit dem Unternehmen führten. Besonders hervorzuheben ist, dass die Planungen darauf hinausliefen, dass die angeschlossenen Kreditinstitute sämtliche Anträge und Verträge mit den darin enthaltenen personenbezogenen Daten in diesen Pool einmelden sollten. Neben der Prüfung, ob es sich eventuell um einen Betrugsfall handeln könnte, sollten diese Daten zum Abgleich zukünftiger Fälle gespeichert, ausgewertet und mit den personenbezogene Daten anderer Institute abgeglichen werden. Datenschutzrechtlich ist eine solche Verarbeitung von Daten, bei denen in keiner Weise ein etwaiger Verdacht gegen den Kunden der Bank besteht, unzulässig. Das Unternehmen hat uns zugesagt, die entsprechenden Datenverarbeitungsvorgänge (nach dessen Aussagen: Bis zur Klärung der Rechtmäßigkeit) nicht umzusetzen.

Wichtig war insbesondere auch die Zusicherung des Unternehmens, dass die Inhalte der Betrugspräventions-Datei nicht mit anderen Dateien desselben oder eines anderen Unternehmens zusammengeführt werden.

Angesichts der bisher vorgenommenen ständigen Anpassungen des Vorhabens sowohl an Änderungen des Geschäftsmodells, als auch an unsere datenschutzrechtlichen Anforderungen, war eine vollständige Prüfung der Datei nicht möglich. Allerdings besteht die Erwartung, dass das Unternehmen sich vor dem Hintergrund der wiederholt deutlich geäußerten Kritik an die vom Düsseldorfer Kreis aufgestellten und die darüber hinaus von uns geforderten Mindestanforderungen hält. Anderenfalls werden wir uns nicht scheuen, die zur Verfügung stehenden Maßnahmen zu ergreifen.

1.3 Meldung von Forderungen bei Abfrage aus einer Auskunftei

Unternehmen, die bei einer Auskunftei offene Forderungen einmelden, müssen in jedem Fall die Voraussetzungen des § 28a Abs. 1 BDSG beachten.

Durch eine Eingabe wurde uns bekannt, dass eine Auskunftei eine Abfragemöglichkeit für ausgewählte Kunden und Kundinnen unterhält, bei der nicht nur eine Auskunft abgefragt wird, sondern gleichzeitig eine Forderung in den Datenbestand eingemeldet wird. Dabei handelt es sich um ein Produkt nur für der Auskunftei angeschlossene Unternehmen. In dem konkreten Fall hatte ein Mitarbeiter des einmeldenden Unternehmens offensichtlich in Unkenntnis dieser Tatsache oder fehlerhaft eine Forderung, die zum Zeitpunkt der Abfrage noch nicht einmal fällig war, gemeldet. Dadurch verschlechterte sich der Scorewert des Betroffenen erheblich.

Erst durch diverse eigene und erfolglose Auskunftsersuchen des Betroffenen und anschließende mehrfache Aufforderungen des Unternehmens zur vollständigen Aufklärung des Sachverhalts durch uns stellte sich dann heraus, dass es sich um eine besondere Meldeform von Forderungen für spezielle Unternehmen handelte. Dieses Verfahren war uns bis dahin nicht bekannt gewesen. Vorliegend hatte das abfragende (und gleichzeitig die Forderung einmeldende) Unternehmen einen Fehler begangen, der von der betreibenden Auskunftei nicht ohne weiteres sofort erkennbar war.

Unabhängig davon war die Aufklärung jedoch deswegen außerordentlich schwierig, weil die Auskunftei nicht sofort transparent und deutlich genug darstellen konnte, dass es sich hier um einen Sonderfall der Forderungsmeldung handelte, der durch das meldende Unternehmen fehlerhaft behandelt worden war.

Üblicherweise fragen Unternehmen bei Auskunfteien über Betroffene an, wenn sie ein

berechtigtes Interesse an einer Auskunft haben, das heißt, wenn sie etwa in finanzielle Vorleistung gehen. Völlig getrennt davon, werden offene Forderungen an Auskunfteien gemeldet. Letzteres ist auch nur unter ganz bestimmten, gesetzlich festgelegten Voraussetzungen zulässig. Nach § 28a Abs. 1 Nr. 4 BDSG dürfen offene, nicht titulierte oder ausdrücklich anerkannte Forderungen an Auskunfteien grundsätzlich nur dann gemeldet werden, wenn

- die Betroffenen nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden sind,
- zwischen der ersten Mahnung und der Übermittlung mindestens vier Wochen liegen,
- die verantwortliche Stelle den Betroffenen rechtzeitig vor der Übermittlung der Angaben, jedoch frühestens bei der ersten Mahnung über die bevorstehende Übermittlung unterrichtet hat und
- die Betroffenen die Forderung nicht bestritten haben.

Dieser zufällig wegen der fehlerhaften Meldung einer noch gar nicht bestehenden Forderung an uns herangetragene Fall hat große Zweifel daran aufkommen lassen, dass dieses Meldesystem in einer Weise ausgestaltet ist, die diese Voraussetzungen auch in jedem Einzelfall berücksichtigt. Verstärkt wurden diese Zweifel durch die Tatsache, dass es der Auskunftei nicht möglich war, Unterlagen darüber vorzulegen, dass die Verträge mit den Nutzerinnen und Nutzern in einer Weise ausgestaltet waren, die diesen ausdrücklich verdeutlichen, wie die Auskunftei für sie zu nutzen ist und welche Forderungen überhaupt nur in der beschriebenen Weise eingemeldet werden dürfen. Seitens der Auskunftei wurde lediglich darauf hingewiesen, dass dies den Nutzerinnen und Nutzern „bekannt sei“, weil es schon seit Jahren funktioniere. Dem musste jedoch seitens der Aufsichtsbehörde entgegengehalten werden, dass gerade der Beschwerdefall gezeigt hat, dass eben nicht alle Mitarbeiter und Mitarbeiterinnen der Unternehmen entsprechende Kenntnisse aufweisen und darüber hinaus die Einschränkungen des § 28 a Bundesdatenschutzgesetz (BDSG) erst vor wenigen Jahren in das Gesetz aufgenommen worden sind.

Neben der Durchführung eines Bußgeldverfahrens in dem konkreten Fall haben wir wenigstens erreichen können, dass die Auskunftei die eingehende Prüfung durch uns zum Anlass genommen hat, die entsprechenden Unternehmen in einem Rundschreiben deutlich auf die Rechtslage hinzuweisen.

1.4 Warndatei im Versandhandel

In langen Verhandlungen ist es gelungen, verschiedene Warndateien des Versandhandels auf eine datenschutzrechtlich zulässige Basis zu stellen.

Bereits im letzten Tätigkeitsbericht haben wir über eine unzulässige Datenverarbeitung durch einen Versandhändler berichtet, gegen den daraufhin ein Bußgeld verhängt wurde (vgl.24.TB, VI 5.1). Dieses Verfahren haben wir zum Anlass genommen, die bei diesem Versandhändler existierenden Warndateien genauer zu kontrollieren.
Dabei stellte sich heraus, dass die bei dem Unternehmen zuletzt 1998 kontrollierte Neukundenkreditprüfung besonders vor dem Hintergrund neu eingeführter Änderungen des Bundesdatenschutzgesetzes (BDSG) nicht den rechtlichen Zulässigkeitsanforderungen entsprach.

Vielmehr wurde deutlich, dass das Unternehmen selbst drei Datenbanken unterhielt und darüber hinaus für zehn angeschlossene Unternehmen jeweils weitere drei verschiedene Datenbanken unterhielt. Es existierten für jedes der Unternehmen eine Kundendatei, eine Inkasso- sowie eine Warndatei. In diesen Datenbanken wurden zentral die Kundendaten der an diese Datenbanken angeschlossenen Unternehmen – inklusive der eigenen Kundendaten des hamburgischen Unternehmens – verarbeitet und verwaltet. In Bezug auf die Kundendaten der angeschlossenen Unternehmen wurde das geprüfte Unternehmen als Auftragsdatenverarbeiter tätig. Im Rahmen einer sogenannten Neukundenkreditprüfung fragten die Tochterunternehmen bonitätsrelevante Kundendaten aus den drei Datenbanken ab, wobei jedes der Unternehmen dabei auch (eingeschränkten) Zugriff auf die Kundendaten der anderen Unternehmen hatte.

Das gesamte Konstrukt dieser 33 verschiedenen Dateien, auf die – zwar unter gewissen Voraussetzungen, aber dennoch – übergreifend zugegriffen werden durfte, war in einer Weise gestaltet, die mit den datenschutzrechtlichen Vorschriften des BDSG nicht in Einklang standen. Zwar ist es für Versandhandelsunternehmen durchaus notwendig und auch gesetzlich zulässig, sich gegen Ausfälle zu schützen. Das ist insbesondere deswegen ohne weiteres nachvollziehbar, weil die Lieferungen in den allermeisten Fällen ohne vorherige Zahlung an Kunden ausgeliefert werden, die den Unternehmen nicht bekannt sind und die keinerlei Sicherheiten bieten.

Genau für derartige Fälle gibt es jedoch schon nach dem BDSG Möglichkeiten, sich etwa Auskünfte bei Auskunfteien zu verschaffen und auch eigene „Problemfälle" dort einzumelden, damit andere Unternehmen gewarnt werden können. Der Betrieb von Auskunfteien unterliegt jedoch strengeren Regelungen. Einerseits dürfen die Meldungen dorthin, etwa wenn ein Kunde oder eine Kundin seine oder ihre Rechnung nicht bezahlt hat, nur unter Beachtung einer Reihe von Voraussetzungen erfolgen. Andererseits haben die Auskunfteien selbst etliche Vorgaben zu beachten, die unter anderen Stichprobenverfahren, Benachrichtigungs- und Auskunftsrechte etc. umfassen.

Zunächst hat es längere Zeit gedauert, bis die beteiligten Aufsichtsbehörden sich einen Überblick über die Konstruktion verschafft hatten. Dabei war es nicht immer einfach, nachzuvollziehen, wer welche personenbezogenen Daten unter welchen Voraussetzungen abfragen durfte. Genau das ist jedoch erforderlich, um im Einzelfall

etwa bei Beschwerden Betroffener konkret beurteilen zu können, ob die rechtlichen Grundlagen eingehalten wurden und insbesondere etwaige Abwägungen in zulässiger Weise stattgefunden haben. Angesichts des Gesamtumfangs der Betroffenendaten in diesem kontrollierten Fall, der Beteiligung von 11 größeren Unternehmen, der Nichtbeachtung der datenschutzrechtlichen Auskunfteienregelungen, aber auch der schwer durchschaubaren Voraussetzungen, unter denen im jeweiligen Einzelfall Zugang zu den Dateien anderer Unternehmen gewährt wurde, ohne dass die Betroffenen darüber unterrichtet waren, haben wir eine Umgestaltung dieses Systems gefordert. Zwar bezieht sich unsere Zuständigkeit nur auf das kontrollierte hamburgische Unternehmen und ein weiteres der angeschlossenen Unternehmen. Wir haben jedoch Kontakt zu den für die übrigen Unternehmen zuständigen Datenschutzaufsichtsbehörden der Länder aufgenommen und die Angelegenheit gemeinsam bearbeitet. Parallel dazu hat der Düsseldorfer Kreis der Aufsichtsbehörden folgendes beschlossen:

Ein konzernangehöriges Unternehmen, das personenbezogene Kundendaten auch zu dem Zweck speichert, sie anderen Unternehmen zur Verhinderung von Forderungsausfällen zu übermitteln, betreibt eine Auskunftei und muss sich insoweit an den Auskunfteienregelungen messen lassen.

In mehreren Sitzungen mit dem kontrollierten Unternehmen, teilweise unter Beteiligung weiterer Aufsichtsbehörden und langen schriftlichen Ausführungen ist es uns gelungen, die wesentlichen Punkte, die einer Änderung zugeführt werden mussten, herauszuarbeiten. Nachdem das Unternehmen sich zunächst strikt weigerte, dem Gedanken der Errichtung einer Auskunftei näherzutreten, hat es sich letztlich jedoch dazu bereit erklärt, das System den Auskunfteienregelungen des BDSG anzupassen und auch eine Auskunftei zum Register beim HmbBfDI zu melden. Darüber hinaus ist es gelungen, in den vielen kritischen Punkten Einigkeit über den Änderungsbedarf zu erzielen und insbesondere auch das Stichprobenverfahren und die Betroffenenrechte angemessen zu berücksichtigen. Zwar sind noch nicht alle Umstellungen komplett erfolgt, das Unternehmen hat jedoch durch engen Kontakt und laufende Informationen über den Stand der Umsetzung bisher gezeigt, dass der richtige Weg verfolgt wird.

Wir werden im Falle eingehender Beschwerden dann konkret kontrollieren, ob sich die Änderungen im Alltag etabliert haben.

1.5 Warndatei Elektronisches Lastschriftverfahren

Bei der Einrichtung einer Warndatei für das Elektronische Lastschriftverfahren konnte erreicht werden, dass Rücklastschriften, bei denen bekannt ist, dass sie wegen eines Rechts aus dem zugrunde liegenden Geschäft geltend gemacht werden, nicht in die Sperrdatei gemeldet werden.

Mitte 2014 wurde bei uns von einem im Auskunfteienbereich tätigen Unternehmen eine neue Sperrdatei angemeldet, in der Rücklastschriften von Kunden und Kundinnen, die am Elektronischen Lastschriftverfahren (ELV) teilnehmen, von betroffenen Händlern eingemeldet werden können.

In der Sperrdatei werden Rücklastschriften im Rahmen des ELV zusammengetragen. Im Falle einer Einmeldung wird der Kunde oder die Kundin für das ELV gesperrt. Sofern er oder sie erneut eine Kartenzahlung vornehmen möchte, erfolgt eine Abfrage des Händlers bzw. des Netzbetreibers bei der Sperrdatei. Dem Kunden oder der Kundin wird daraufhin die Zahlung per ELV verwehrt und er wird auf das girocard-Verfahren verwiesen. Dies geschieht automatisiert im Hintergrund, ohne dass dies für den Kunden oder die Kundin und auch für den Verkäufer oder die Verkäuferin überhaupt ersichtlich ist.

Allein die Vorlage einer Rücklastschrift genügte für die Eintragung in die Sperrdatei. Irrelevant war dabei, ob die Rücklastschrift aufgrund fehlender Deckung oder sogar Nichtbestehens des zu belastenden Kontos oder aufgrund eines Widerspruchs gegen die Lastschrift erfolgt war. Im Falle eines Widerspruchs des Karteninhabers oder der Karteninhaberin erfolgte eine Speicherung in der Sperrdatei bis zur Klärung des Widerspruchs. Die Eintragung in die Sperrdatei wurde erst gelöscht, wenn ein Handelsunternehmen mitteilte, dass es sich um eine berechtigte Stornierung der Lastschrift gehandelt hat oder sofern der Karteninhaber oder die Karteninhaberin die getätigte Rücklastschrift nach Klärung mit dem Unternehmen erneut beglichen hat. Insofern kam es zur Einmeldung und damit einhergehender, zumindest vorübergehender Sperrung von Karteninhabern für das ELV-Verfahren, die berechtigt Widerspruch gegen eine Lastschrift eingelegt hatten.

Die Eintragung in die Sperrdatei erfolgt dabei zumindest taggenau, im besten Fall minutengenau mit der Einlegung des Widerspruchs durch den Karteninhaber. Dies ist nach Aussage des Unternehmens erforderlich, um etwaigen (weiteren) Kartenmissbrauch zu vermeiden, da der jeweilige (vermeintliche) Karteninhaber oder die Karteninhaberin nach dem Ausüben des Widerspruchs ungehindert weiter mittels des ELV in missbräuchlicher Absicht einkaufen könnte.

Datenschutzrechtlich dürften die schutzwürdigen Interessen der Betroffenen der Speicherung nicht entgegenstehen. Dies gilt gleichermaßen für die Übermittlung der Daten an anfragende Händler.

Die Zulässigkeit der Einmeldungen der Rücklastschriften seitens der Händler muss zur Wahrung des eigenen bzw. systemischen berechtigten Interesses an der Funktionsfähigkeit der Sperrdatei sowie der Sicherheit des ELV erforderlich sein. Ferner dient diese Zweckverfolgung dem berechtigten Interesse Dritter, vorliegend also der weiteren an die Sperrdatei angeschlossenen Händler, an der Vorbeugung von Missbrauchsfällen

im Rahmen des ELV.

Auch die die Zulässigkeit der Abfrage bei der Sperrdatei seitens der Händler im Rahmen der Zahlungsvorgänge war unsererseits genauer zu untersuchen.

In sämtlichen der genannten Datenverarbeitungsvorgänge stellte sich das Problem, dass in der Sperrdatei nicht zwischen berechtigten und unberechtigten Rücklastschriften differenziert wurde. Sofern es sich um Rücklastschriften infolge mangelnder Kontodeckung oder sogar missbräuchlicher Widersprüche handelte, war dem Interesse an der Funktionsfähigkeit der Sperrdatei und Sicherheit des ELV regelmäßig der Vorzug zu gewähren.

Die Frage war jedoch anders zu beurteilen, sofern es sich um die Einmeldung berechtigter Widersprüche handelte. In derartigen Fällen hat der jeweils betroffene Karteninhaber ein schutzwürdiges Interesse daran, dass die berechtigte Rücklastschrift infolge seines berechtigten Widerspruchs nicht in die Sperrdatei aufgenommen und er somit vom ELV, wenn auch nur bis zur Klärung und erneuter Freigabe, ausgeschlossen wird.

Nach Angaben des Unternehmens sollte zunächst eine Differenzierung zwischen berechtigten und unberechtigten Rücklastschriften unter Beibehaltung der Funktionsfähigkeit der Sperrdatei nicht möglich sein. Es wurde vorgetragen, dass eine solche Differenzierung nur bei einer nicht taggenauen Eintragung in der Sperrdatei zu erzielen wäre. Gerade auch Missbrauchsfälle würden in unmittelbarer zeitlicher Abfolge nach der Erklärung eines Widerspruchs erfolgen. Insofern könne man die Funktionsfähigkeit der Sperrdatei nur durch taggenaue, besser noch minutengenaue Eintragungen sicherstellen.

Ungeachtet der Frage nach der Zulässigkeit der Eintragung berechtigter Rücklastschriften bedarf es aus Transparenzgründen sowie aufgrund der Benachrichtigungspflicht des § 33 Abs. 1 BDSG einer Aufklärung gegenüber den Karteninhabern über die Eintragung in die Sperrdatei, sofern sie der Lastschrift widersprechen. Bislang werden die Karteninhaber über die Eintragung in der Sperrdatei lediglich für die Fälle einer mangelnden Deckung oder des Nichtbestehens des zu belastenden Kontos unterrichtet. Diese Belehrung erfolgt mittels eines entsprechenden Texts, welcher zusammen mit der Einzugsermächtigung für die jeweils getätigte Zahlung auf einem Kassenausdruck vom Karteninhaber zu unterschreiben ist. Die bisherige Belehrung enthielt keinen Hinweis darauf, dass eine Eintragung in die Sperrdatei im Falle eines unberechtigten oder auch eines berechtigten Widerspruchs erfolgt.
Nach längeren Verhandlungen mit dem Unternehmen haben wir erreicht, dass die beim Kauf zu unterzeichnende Einwilligungserklärung in einer Weise geändert wurde, durch die dem Kunden bzw. der Kundin deutlich wird, dass eine Meldung an die Warndatei auch bei einem Widerruf erfolgt. Entscheidend war in diesem Zusammenhang, dass darin auch die datenschutzrechtlich zu begrüßende Änderung verdeutlicht

wird: Sofern bereits bei Erklärung des Widerrufs Rechte aus dem zugrundeliegenden Kaufvertrag geltend gemacht werden, wie etwa einen Mangel der erworbenen Sache, erfolgt von vornherein keine Meldung mehr an die Warndatei.

1.6 Onlineportal zur Kreditvergabe

Die ausländischen Töchter eines Hamburger IT-Startups vergeben im Internet Kleinkredite, ohne dabei die Grundwerte des deutschen Datenschutzrechts zu beachten.

Eine in Hamburg ansässige Holding besitzt mehrere Tochterunternehmen im europäischen und außereuropäischen Ausland, die Kreditvergaben an Verbraucherinnen und Verbraucher in den jeweiligen Ländern vornehmen. Die Dienste richten sich ausschließlich an Kundinnen und Kunden in den jeweiligen Ländern und stehen Deutschen nicht offen.

Die Abwicklung des Kreditvergabeprozesses erfolgt in der Regel automatisiert über Onlineportale, die von der Holding bereitgestellt und technisch betreut werden und von den Töchtern im außereuropäischen sowie innereuropäischen Ausland betrieben werden. Sämtliche für die Kreditentscheidung relevanten Informationen geben die Antragstellerinnen und Antragsteller auf der jeweiligen länderspezifischen Internetseite ein und laden dort auch entsprechende digitalisierte Nachweisdokumente hoch. Ein von der Hamburger Holding entwickelter und der jeweiligen Tochter modifizierter Scoring-Algorithmus überprüft die eingegebenen Daten, sodass die Antragstellerin oder der Antragsteller bereits nach wenigen Minuten eine Entscheidung über die Gewährung und die Konditionen des beantragten Kredits erhält. Unabhängig davon, ob ein Kreditvertrag zustande kommt, werden die sensiblen Kundendaten weiterhin zur Optimierung des Scoring-Algorithmus gespeichert. Eine Löschung innerhalb regelmäßiger Fristen erfolgt derzeit nicht. Auch Löschersuchen der Betroffenen werden nicht nach den Maßstäben des Bundesdatenschutzes (BDSG) umgesetzt. In der Vergangenheit haben wir Kenntnis von einem Fall erhalten, bei dem zahlreiche Antragstellerdaten infolge eines Sicherheitsbruchs frei verfügbar im Internet zu finden waren.

Die Datenerhebungen bei den Antragstellerinnen und Antragstellern entsprechen in mehrfacher Hinsicht nicht den Anforderungen des BDSG. Dies folgt insbesondere aus dem unverhältnismäßigen Umfang der Datenerhebung, die beispielsweise die Interaktion der Nutzerinnen und Nutzer mit Elementen auf verschiedenen Internetseiten beinhaltet. Zudem werden Nutzer aufgefordert, die Zugangsdaten ihres Facebook-Accounts einzugeben und in eine zusätzliche Auswertung ihrer Timeline einzuwilligen, wodurch Daten Dritter einbezogen werden. Hinsichtlich der abgegebenen Einwilligungen bestehen massive Zweifel an deren Freiwilligkeit, weil sich die Dienste vordring-

lich an Personen richten, die auf dem regulären Kapitalmarkt keine Kredite erhalten. Zudem nehmen die Unternehmen entgegen § 6a BDSG automatisierte Einzelfallentscheidungen vor.

Die umfangreiche Prüfung der in Hamburg ansässigen Holding hat ergeben, dass diese im Wesentlichen Auftragsdatenverarbeitungen nach § 11 BDSG im Auftrag ihrer Tochterunternehmen vornimmt. Die Verantwortlichkeit für die Datenverarbeitung liegt deshalb bei den ausländischen Töchtern. Die zentralen Kritikpunkte unserer Behörde an dem Geschäftsmodell des Konzerns entziehen sich somit unserer Zuständigkeit. In Fällen der Auftragsdatenverarbeitung beschränkt sich diese auf die von uns in diesem Fall auch wahrgenommene Überprüfung der technischen und organisatorischen Schutzmaßnahmen für die in Hamburg verarbeiteten Daten. Hinsichtlich der Verantwortlichkeiten der Tochterunternehmen haben wir die Datenschutz-Aufsichtsbehörden der jeweiligen Staaten informiert, damit diese entsprechende Maßnahmen einleiten können.

1.7 Bargeldloses Bezahlen in Fußballstadien

Bezahlkarten für Veranstaltungshallen und Stadien enthalten häufig NFC-Chips, deren Daten kontaktlos ausgelesen werden können. Sind auf dem Chip personenbezogene Informationen gespeichert, ist deshalb besondere Sorgfalt geboten.

In zahlreichen Stadien der Fußball-Bundesliga sowie weiteren Veranstaltungshallen können die Besucherinnen und Besucher Speisen, Getränke und anderen Artikel mit der Karte eines Hamburger Unternehmens bargeldlos bezahlen. Der Abgleich des Kartenguthabens mit den Verkaufsstellen erfolgt kontaktlos, indem der NFC-Chip (Near Field Communication-Chip) der Karte in die direkte Nähe des Zahlungsterminals gehalten wird. Dabei besteht grundsätzlich die Gefahr, dass Unbefugte ein eigenes Lesegerät installieren, um den Inhalt der NFC-Chips ebenfalls auszulesen. Werden die Karten im Stadion ohne die Angabe der eigenen Identität erworben, ermöglichen sie anonymes Bezahlen. Unbefugte Dritte können dann ebenfalls nur anonyme Daten auslesen. Das Kartenguthaben kann jedoch alternativ auch über das Internet aufgeladen werden. Dies erfordert die persönliche Registrierung und Verknüpfung der eigenen Identität mit der Karte. Obwohl der NFC-Chip in dem Fall nicht den Namen der Inhaberin oder des Inhabers, sondern lediglich eine Zuordnungsnummer enthält, kann die Identität anhand dieser Nummer ermittelt werden, wenn entsprechende Zusatzinformationen vorliegen. Auf dem NFC-Chip sind dann schutzbedürftige personenbezogene Daten gespeichert.

Gemäß der rechtlichen Bewertung der bundesweiten AG Kreditwirtschaft und des AK

Technik der Datenschutzbeauftragten der Länder zum Einsatz von NFC-Technologien bei personalisierten Geldkarten sind die folgenden technischen und organisatorischen Maßnahmen zu treffen:

1. Es ist eine Datenschutzfolgenabschätzung in Form eines sogenannten PIA (Privacy Impact Assessment) durch das Unternehmen zu erstellen.

2. Die Karten ausgebenden Unternehmen sind zu verpflichten, zumindest auf Verlangen der Kundin/des Kunden eine Schutzhülle in der Standardversion für Geldkarten mit NFC-Funktion auszugeben.

3. Die Karten ausgebenden Unternehmen sind verpflichtet, sämtlichen Kundinnen und Kunden entsprechende Hinweise zum Datenverarbeitungsprozess zugänglich zu machen.

4. Die Möglichkeit der jederzeitigen Abschaltung der NFC-Funktion auf Wunsch der Karteninhaberin oder des -inhabers ist schnellstmöglich umzusetzen.

5. Die Karten ausgebenden Unternehmen werden darauf hingewiesen, dass etwaige Drittanwendungen, die geeignet sind, das Pseudonymisierungskonzept der Karte zu unterlaufen, eine neue datenschutzrechtliche Bewertung erforderlich machen.

Aufgrund unserer Intervention hat das in Hamburg geprüfte Unternehmen eine Datenschutzfolgeabschätzung erstellt und seine technischen und organisatorischen Maßnahmen so systematisiert. Zudem haben wir erwirkt, dass das Unternehmen in seinem Onlineshop nun Schutzhüllen aus Aluminium für die Bezahlkarten anbietet. Diese verhindern wirkungsvoll den Datenabruf durch Unbefugte, indem sie die NFC-Signale abschirmen. Durch beide Maßnahmen setzt das Unternehmen die rechtlichen Anforderungen nunmehr um.

1.8 Abruf von Angehörigendaten durch Beschäftigte eines Kreditinstituts

Gegen eine Bankmitarbeiterin, die sich unrechtmäßig über Kontodaten ihrer Familienmitglieder informiert hat, haben wir ein Bußgeld verhängt.

Die bei Kreditinstituten gespeicherten Kundendaten können einen umfassenden Einblick in die Lebenssituation des dahinter stehenden Menschen bieten und sind deshalb besonders sensibler Natur. Deshalb sind Kreditinstitute verpflichtet, den Zugriff auf personenbezogene Daten so weit wie möglich zu beschränken. Dies betrifft ins-

besondere auch den Zugriff durch Mitarbeiterinnen und Mitarbeiter der Bank, sodass sicherzustellen ist, dass diese nur auf die Daten derjenigen Kundinnen und Kunden zugreifen können, die sie auch betreuen. Dieser Kreis zugriffsberechtigter Beschäftigter kann jedoch nicht zu eng gezogen werden. Viele Kundinnen und Kunden überregional tätiger Filialbanken erwarten, dass sie auch in jeder Filiale sowie in Callcentern beraten werden und Bankgeschäfte tätigen können. Aus dieser Notwendigkeit folgt eine vielfach große Zahl an Personen, die auf Kundendaten zugreifen können. Um das damit verbundene Missbrauchspotential zu verringern, sind die Kreditinstitute verpflichtet, die jeweiligen Zugriffe zu protokollieren.

In einem Fall in einem Hamburger Kreditinstitut haben diese Protokolldaten zur Überführung einer mit der Kundenbetreuung betrauten Mitarbeiterin geführt. Diese hatte die Kontodaten mehrerer bekannter Personen abgerufen, weil sie die betreffenden Informationen im Zuge einer privatrechtlichen Auseinandersetzung nutzen wollte. Wir haben wegen des Verstoßes § 43 Abs. 2 Nr. 3 Bundesdatenschutzgesetz (BDSG) ein Bußgeld gegen die Mitarbeiterin persönlich verhängt. Darüber hinaus war sie arbeitsrechtlichen Konsequenzen ausgesetzt. Dem Kreditinstitut hingegen war insbesondere aufgrund seiner etablierten technischen und organisatorischen Maßnahmen kein Vorwurf zu machen.

2. Finanzen, Steuern und Rechnungswesen

2.1 Einheitspersonenkontenverordnung

Mit der neuen Verordnung über die gemeinsamen Personenkontendateien der ressourcensteuernden Verfahren (Einheitspersonenkontenverordnung - EPKVO) konnten wir verhindern, dass alle Beschäftigten mit Zugriff auf diese Verfahren die Felder „Geburtstag“ und „Geburtsort“ aller „Geschäftspartner“ einsehen dürfen.

Die EPKVO ist datenschutzrechtlich von besonderer Bedeutung: Auf ihrer Grundlage dürfen mehrere tausend Beschäftigte der Freien und Hansestadt Hamburg, die für Buchungen auf der Grundlage der LHO zuständig sind, mittels SAP oder anderer Fachverfahren auf gemeinsame Dateien mit über 2 Mio. Datensätzen zu sog. Geschäftspartnern zugreifen. Die EPKVO bietet die Rechtsgrundlage für den Zugriff auf gemeinsame Dateien i. S. d. § 11a HmbDSG, die alle Daten enthalten, die für die Abwicklung der Buchführung, des Zahlungsverkehrs, der Rechnungslegung, des Mahnwesens und der Beitreibung von Forderungen relevant sind.

Nach § 11a HmbDSG ist der Senat ermächtigt, die Einrichtung gemeinsamer oder verbundener Dateien durch Rechtsverordnung zuzulassen. Die Datenverarbeitung als solche muss den Vorschriften des HmbDSG oder einschlägiger Spezialnormen genü-

gen; insoweit bietet die Rechtsverordnung keine Rechtsgrundlage, von den datenschutzrechtlichen Vorschriften abzuweichen. Wir haben uns dafür eingesetzt, dass die wesentlichen Grenzen der Datenverarbeitung nach dem HmbDSG in der EPKVO deklaratorischen Niederschlag fanden, damit sie den zahlreichen Anwendern mahnend vor Augen geführt werden.

Wir wurden im Jahr 2013 durch einen SAP-Anwender darauf aufmerksam gemacht, dass u. a. in den gemeinsamen Dateien die Merkmale „Geburtsdatum" und „Geburtsort" verarbeitet würden, ohne dass die damals geltende Einheitspersonenkontenverordnung dafür eine Rechtsgrundlage bot. Daraufhin nahmen wir mit der zuständigen Finanzbehörde Kontakt auf und konnten uns bald darauf einigen, dass eine neue Verordnung gemäß § 11a HmbDSG erforderlich war. In konstruktiver Zusammenarbeit konnten wir uns nach und nach darauf verständigen, dass man mit technisch-organisatorischen Maßnahmen die für einzelne Benutzergruppen notwendigen Zugriffe bedarfsgerecht differenziert gestalten muss.

Bei der Formulierung des neuen Verordnungstextes legten wir Wert darauf, dass Anwender in der EPKVO wiederholt darauf hingewiesen werden, dass Zugriffe auf Datensätze der Geschäftspartner

- nur zu buchungsrelevanten Zwecken i. S. der EPKVO sowie
- nur im erforderlichen Umfang und
- einzelfallbezogen

erfolgen dürfen. Letztlich haben wir auch anerkannt, dass eine geringere Zahl von Mitarbeiterinnen und Mitarbeitern der Finanzbehörde zu einer Aktualisierung und Bereinigung der Geschäftspartner-Datensätze (Dubletten-Prüfung) berechtigt ist, zumal dies der eindeutigen Identifizierung betroffener Geschäftspartner und dem Ziel der Datensparsamkeit dient. Zum Zweck der Dubletten-Prüfung und für die Bearbeitung von Ordnungswidrigkeiten-Verfahren hielten wir es deshalb für gerechtfertigt, den Geschäftspartner-Datensätzen die Felder „Geburtsdatum" und „Geburtsort" hinzuzufügen, wenn diese Felder nicht allen mit Buchungsarbeiten Beschäftigten zugänglich gemacht werden. Diese Daten wurden daraufhin in der EPKVO als „erweiterte Stammdaten" kategorisiert und können auf diese Weise einer Kenntnisnahme der Zugriffsberechtigten, die diese Daten nicht zwingend benötigen (z. B. zur Begleichung von Rechnungen), entzogen werden.

Um nachhaltig zu verhindern, dass Ordnungs-, Gruppierungs- und Identifikationsbegriffe Rückschlüsse darauf zulassen, aus welchem Anlass für einen Geschäftspartner ein Personenkonto angelegt wurde, wird in der Verordnung klargestellt, dass durch diese Begriffe keine schutzwürdigen Interessen der Betroffenen gefährdet werden dürfen. So darf etwa die Geschäftspartnernummer des Betroffenen nicht erkennen lassen, dass der Datensatz aus Anlass eines Ordnungswidrigkeitenverfahrens erfasst wurde.

Die Arbeiten an der Neufassung zogen sich über das Jahresende 2014 hin. Anfang 2015 erreichten uns im Zuge des Roll-Out der letzten Stufe des Verfahrens HERAKLES mehrere Beschwerden von Beschäftigten darüber, dass ihre Einheitspersonenkonten samt Konto- und Adressdaten für eine Vielzahl von Kolleginnen und Kollegen, die HERAKLES-Berechtigungen haben, einsehbar wären, obwohl sie diese Daten nicht zur Aufgabenerfüllung benötigten. Zugriffsberechtigte Beschäftigte könnten ihre Rechte im Einzelfall ohne dienstlichen Anlass unzulässig nutzen. Außerdem würden bei der Geschäftspartner-Suche viele Datensätze Betroffener angezeigt, die mit der Einzelfallsachbearbeitung in keinem Zusammenhang stünden (siehe dazu VIII 2.2).

Nach unserer Auffassung lagen diese Mängel nicht an dem bis dahin abgestimmten Verordnungstext, sondern an der Umsetzung. In der Behördenabstimmung wurde deshalb in der Drucksache unser eindringlicher Hinweis aufgenommen, dass sich die EPKVO in der Praxis bewähren müsse, dass es erforderlich sei, ihre Einhaltung zu überwachen und dass Zugriffsberechtigungen ausreichend differenziert erteilt werden müssten.

2.2 HERAKLES: Freie Suche nach Bankkonten und Privat-Adressen möglich

Im IT-Verfahren HERAKLES können ca. 5.000 Beschäftigte in dem riesigen Datenbestand aller über zwei Millionen Geschäftspartner der FHH recherchieren und so in unberechtigter Weise sensible Daten u.a. von Kolleginnen, Kollegen und Bekannten ermitteln, ohne dass es dafür einen dienstlichen Anlass gibt. Erst nach langwierigen und zähen Verhandlungen mit der Finanzbehörde wurden einzelne Verbesserungen vorgenommen. Dennoch steht die Beseitigung der erheblichen Mängel immer noch aus.

Mit dem Projekt HERAKLES der Finanzbehörde soll eine revisionssichere, IT-gestützte und soweit wie möglich automatisierte und papierlose Rechnungsbearbeitung mit Buchungen in ein doppisches Kontensystem realisiert werden. Der Einbindung der Sachbearbeitung in den Behörden und Ämtern kommt dabei eine besondere Bedeutung zu; einige Fachverfahren wurden über Schnittstellen an das Verfahren HERAKLES angebunden. Durch die Dezentralisierung hat sich die Zahl der zugriffsberechtigten Personen auf den gemeinsamen Datenbestand mit den Personenkontendaten sehr stark erhöht. Zum 01.01.2015 wurde die flächendeckende Einführung in der FHH mit der Produktivsetzung in den Bezirksämtern, der Behörde für Gesundheit und Verbraucherschutz, der Behörde für Wirtschaft, Verkehr und Innovation, der Senatskanzlei, dem Personalamt sowie der allgemeinen Finanzwirtschaft abgeschlossen.

Durch zahlreiche Eingaben von Beschäftigten der FHH wurden wir Anfang 2015 darauf aufmerksam, dass Nutzerinnen und Nutzer des IT-Verfahrens HERAKLES Zugriff auf (teils sensible) Daten haben, die weit über das erforderliche Maß hinausgehen. In den Beschwerden machten die Beschäftigten deutlich, dass viele ihrer Kolleginnen und Kollegen die Möglichkeit haben - und teilweise genutzt haben -, sich ihre personenbezogenen Daten anzeigen zu lassen. Das Verfahren HERAKLES steht derzeit nach freier Schätzung des Projekts ca. 4.000 - 5.000 Nutzerinnen und Nutzern zur Verfügung. Die genaue Anzahl konnte das Projekt trotz wiederholter Nachfragen nicht mitteilen.

Unsere Prüfung des IT-Verfahrens hat ergeben, dass die Nutzerinnen und Nutzer weit überwiegend den beiden Rollen „Feststellungsbefugte“ und „Anordnungsbefugte“ zugeordnet sind. Beide Rollen verfügen über die Berechtigung, eine freie Suche nach Personen („Geschäftspartnern“) durchzuführen und sich zu einem Datensatz Namen, Vornamen, Anschrift, Geschäftspartnernummer und - soweit gespeichert - Kontoverbindung anzeigen zu lassen. Insgesamt sind in diesem Datenbestand, in dem gesucht werden kann, nach Angaben des Projekts mehr als 2 Millionen personenbezogene Geschäftspartner-Datensätze gespeichert.

Um eine Geschäftspartner-Suche in den gemeinsamen Datenbanken durchzuführen, müssen keine Mindesteingaben in die Felder der Suchmaske eingegeben werden. Es reicht z. B. als Suchkriterium ein Vor- oder Nachname oder ein Straßenname oder ein Teil davon, um sich u.a. vollständige Adressdaten von bis zu 50 Betroffenen anzeigen zu lassen. Zusätzlich steht die Möglichkeit einer sogenannten unscharfen Suche zur Verfügung, bei der auch Treffer angezeigt werden, bei denen ein Name in ähnlicher Schreibweise gespeichert ist oder die die eingegebenen Namensteile enthalten. Es wird dabei nicht protokolliert, ob ein Zugriff auf Datensätze stattgefunden hat, es wird nicht protokolliert, wer mit welchen Suchkriterien auf die Datenbank zugegriffen hat und es wird nicht protokolliert, aus welchem Anlass eine Abfrage stattfindet. Es gibt lediglich die Beschränkung, dass pro Nutzerin bzw. Nutzer maximal 20, 50 oder 150 Abfragen pro Tag vorgenommen werden können. Im Zuge der Prüfung wurde uns von der Fachlichen Leitstelle bestätigt, dass so auch Daten von Mitgliedern des Senats für diesen großen Nutzerkreis recherchierbar waren.

Die nahezu unbegrenzte Suchmöglichkeit für tausende von Beschäftigten der FHH ist sehr problematisch. Wir sehen darin einen Verstoß gegen das Hamburgische Datenschutzgesetz und die Einheitspersonenkontenverordnung. In deren gerade 2015 fortgeschriebenen Fassung (vgl. VIII 2.1) wird in § 2 Abs. 3 explizit ausgeführt, dass personenbezogene Daten nur „einzelfallbezogen im erforderlichen Umfang“ für den in Absatz 2 genannten Zweck verarbeitet werden dürfen. Bereits im März 2015 haben wir das Projekt deshalb aufgefordert, insbesondere die freie Suche und die Protokollierung so zu verändern, dass die datenschutzrechtlichen Anforderungen eingehalten werden. Es reicht nicht aus, nur einige wenige Datensätze, wie z.B. von Mitgliedern des Senats, von der freien Suche auszuschließen.

Nach zahlreichen Konsultationen hat die Fachliche Leitstelle HERAKLES nunmehr Ende November 2015 zugesagt, dass die freie und die unscharfe Suche für einen großen Teil der Nutzerinnen und Nutzer beschränkt wird, womit dem Mangel, dass bei einem Suchvorgang nicht benötigte personenbezogene Daten angezeigt werden, im Wesentlichen abgeholfen wird. Aber nach wie vor ist nicht vorgesehen, dass die Eingabe einer eindeutigen Kennung des behördlichen Vorgangs Voraussetzung für das Starten einer Suchanfrage ist. Damit ist es nicht möglich zu kontrollieren, ob einer Suchanfrage tatsächlich ein behördlicher Vorgang zugrunde lag und ob dieser Vorgang die Suchanfrage rechtfertigte. Das Ziel, mit einer derartigen Protokollierung die Gefahr des Missbrauchs ausreichend zu verhindern, kann somit nicht erreicht werden. Vor diesem Hintergrund bleibt festzustellen, dass die Fachliche Leitstelle mit den vorgeschlagenen Maßnahmen zwar einen Schritt in die richtige Richtung machen würde. Aber es werden damit noch nicht die erforderlichen Maßnahmen nach § 8 Abs. 1 HmbDSG getroffen, um eine ausreichende Schutzwirkung zu erzielen.

Daher haben wir die Finanzbehörde aufgefordert, dafür Sorge zu tragen, dass

- alle Suchanfragen im Verfahren HERAKLES protokolliert werden,
- insbesondere bei einer Suchanfrage mit den Eingangsparametern „Name, Vorname“, „Straße, Hausnummer“ und „Stadt“ auch eine eindeutige Kennung des behördlichen Vorgangs (z.B. ein Aktenzeichen oder eine Rechnungsnummer) als zwingend erforderliche Angaben von den Zugriffsberechtigten eingegeben werden müssen und dass diese Anfragedaten mit im Protokoll der Suchanfrage gespeichert werden,
- bei der Suche die Suchanfragen protokolliert werden und
- die Stichprobenprüfung in den Dienstanweisungen der Behörden und Ämter festgeschrieben wird.

Diese Anforderungen müssten in die Veränderungen einfließen, deren Umsetzung die Fachliche Leitstelle bis zum April 2016 plant. Damit wäre dann endlich, nach fast 1,5 Jahren, der gravierende Mangel in dem IT-Verfahren HERAKLES abgestellt. Wir werden das Ergebnis anschließend kritisch prüfen und uns ggf. weiter für Verbesserungen einsetzen. Das Beispiel zeigt, dass leider oft nur durch wiederholte und engagierte Diskussionen eine Verhaltensänderung gerade auch auf Seiten der öffentlichen Stellen zu verzeichnen ist. Das ist gerade vor dem Hintergrund der personellen Defizite unserer Behörde problematisch.

2.3 Automatischer Kirchensteuerabzug vom Kapitalertrag

Zu Irritationen bei einigen Betroffenen führten Informationen der Kreditinstitute über das neue automatische Kirchensteuerabzugsverfahren.

Uns erreichten Beschwerden von Bürgerinnen und Bürgern, die im Jahr 2014 ein obligatorisches Informationsschreiben von ihrem Finanzinstitut bekamen, wonach das Kreditinstitut eine Anfrage an das Bundeszentralamt für Steuern (BZSt) nach der Religionszugehörigkeit richten muss, wenn Abgeltungssteuer auf Kapitalerträge abgeführt wurde. Für ab dem 01.01.2015 anfallende Kapitalerträge werden nämlich die Kirchensteuern, die auf die Abgeltungssteuer entfallen (die ihrerseits seit Jahren von den Kreditinstituten automatisch an die Finanzämter abgeführt wird), ebenfalls automatisiert an die Finanzämter abgeführt. Dies beruht auf § 11a des Hamburgischen Kirchensteuergesetzes (HmbKiStG) und § 51a Einkommensteuergesetz (EStG).
Diese Kirchensteuer wird als Zuschlag zur Kapitalertragsteuer erhoben und betrifft die Steuerpflichtigen, die einer Religionsgemeinschaft angehören, die eine Kirchensteuer erhebt; und darunter berührt sie nur diejenigen, bei denen das kirchensteuerabzugsverpflichtete Institut tatsächlich eine Abgeltungsteuer abführt. Steuerpflichtige, die einen Freistellungsauftrag erteilt haben und unterhalb des Freibetrags liegen, sind also nicht betroffen.

Da die „Kirchensteuerabzugsverpflichteten" (das können Kreditinstitute sein, aber auch beispielsweise Versicherungen) nicht wissen, ob eine Kundin / ein Kunde einer Religionsgemeinschaft angehört und in welcher Höhe diese ggf. Steuern erhebt, sind sie verpflichtet, alle Kundinnen und Kunden über das neue Verfahren aufzuklären.

Betroffene Kirchensteuerpflichtige haben die Möglichkeit, die automatische Abführung des Zuschlags und den automatisierten Datenabruf über die Religionszugehörigkeit zu verhindern. Dazu müssen sie allerdings von sich aus aktiv werden. Auf einem vorgeschriebenen Formblatt, das an das BZSt gesendet werden muss, kann ein „Sperrvermerk" beantragt werden. Das BZSt benachrichtigt daraufhin das zuständige Finanzamt, das den Steuerpflichtigen dann zur Abgabe einer Steuererklärung zu den kirchensteuerpflichtigen Kapitalerträgen auffordert. Wenn das kirchensteuerabzugsverpflichtete Institut dann die vorgeschriebene Abfrage an das BZSt über die Religionszugehörigkeit des Steuerpflichtigen richtet, erhält es eine „Nullmeldung", genauso wie zu Steuerpflichtigen, die keiner Religionsgemeinschaft angehören.

Das BZSt hat unter dem Link *http://www.bzst.de/DE/Steuern_National/Kirchensteuer/Info_Buerger/Informationen_fuer_Buerger_node.html* Informationen zum Verfahren bereitgestellt. Gegen die neue Rechtslage und die von uns überprüften Informationsschreiben der Kirchensteuerabzugsverpflichteten haben wir keine datenschutzrechtlichen Bedenken.

3. Versicherungswirtschaft

3.1 Meldungen an das Hinweis- und Informationssystem – Sparte Kranken

Der Verband der Privaten Krankenversicherung (PKV) plant die Einführung einer Warndatei, in die Daten von Versicherten eingemeldet werden, von denen ein besonderes Betrugsrisiko ausgeht.

Das Hinweis- und Informationssystem der Versicherungswirtschaft (HIS) ist eine vom Gesamtverband der deutschen Versicherungswirtschaft e.V. (GDV) geführte Datei, mittels derer deutsche Versicherungen sich vor möglichen Versicherungsbetrugsfällen warnen (vgl. 23. TB, IV 5.3). Hat ein Versicherungsnehmer beispielsweise bei Vertragsabschluss bewusst relevante Daten verschwiegen, muss er damit rechnen, dass dieser Umstand an das HIS gemeldet wird. Andere Versicherungsunternehmen können auf diese Weise Kenntnis von dem Fall erhalten, wenn er dort später einen Vertrag abschließen möchte.

Die privaten Krankenversicherungen nehmen bislang am HIS weder einmeldend noch abrufend teil. Über ihren Verband PKV planen sie aktuell entweder eine Beteiligung am HIS oder den Aufbau einer eigenständigen, vergleichbaren Informationsplattform. Vorgesehen ist ein Punktesystem in der Art, dass vordefinierte Verdachtstatbestände unterschiedlich gewichtet werden. Jeder Verdachtsfall muss mehrere Tatbestände erfüllen, um die Schwelle zu überschreiten, ab der eine Meldung möglich ist. Zusätzlich zu diesem mathematischen Kriterium muss die einmeldende Versicherung eine Einzelfallabwägung vornehmen, in deren Rahmen die tatsächliche Gefahr eines künftigen Versicherungsbetrugs abzuschätzen ist.
Hinsichtlich der Ausgestaltung steht der PKV in enger Abstimmung mit der AG Versicherungswirtschaft des Düsseldorfer Kreises, an der auch unsere Behörde beteiligt ist. Dabei konnte die AG darauf hinwirken, dass die vorgesehenen Einmeldegründe deutlich reduziert und eingegrenzt werden und teilweise bestimmtere und damit transparentere Begriffsbestimmungen erhalten. Beispielsweise verzichtet der PKV auf Drängen der AG auf den unbestimmten und unverhältnismäßigen Tatbestand „Hartnäckiges Drängen auf Schadenregulierung“. In Fällen des vertragswidrigen Verschweigens einer Mehrfachversicherung bei verschiedenen Unternehmen oder eines Verwandtschaftsverhältnisses des Versicherten mit dem behandelnden Arzt konnte der PKV überzeugt werden, den Tatbestand auf vorsätzliche Fälle zu beschränken, weil vielen Versicherten nicht bekannt sein dürfte, dass sie derartigen Vertragspflichten unterliegen.

Nachdem der PKV der AG eine überarbeitete Fassung des Konzeptes zukommen lässt, ist eine abschließende Befassung des Düsseldorfer Kreises im Frühjahr 2016 vorgesehen.

3.2 Einwilligungserklärungen für die Dienste von Versicherungsmaklern

Die bisher wenig zufriedenstellende Datenverarbeitungspraxis der Versicherungsvermittlerinnen und -vermittler sowie Maklerinnen und Makler soll künftig auf eine rechtssichere Grundlage gestellt werden.

Die Tätigkeiten von Versicherungsvermittlerinnen und -vermittlern beziehungsweise Versicherungsmaklerinnen und -maklern setzen die Erhebung und Weitergabe umfangreicher persönlicher Daten ihrer Mandanten voraus. Dabei ist zu Beginn eines umfassenden Beratungsgesprächs vielfach noch nicht bekannt, welche Lebensbereiche mit welcher Art von Versicherungen abgedeckt werden sollen. Die Mandantinnen und Mandanten geben dem Vermittler in der Regel vollumfängliche Einsicht in ihre berufliche und private Situation. Diese in ihrer Gesamtheit sehr sensiblen Personenprofile gibt die Vermittlerin oder der Vermittler oftmals an eine Vielzahl von Unternehmen und Personen weiter, die diese Daten unter anderem nutzen, um Versicherungstarife zu berechnen und zurückzumelden. Nur so kann die Vermittlerin oder der Vermittler den optimalen Tarif ermitteln, der zu seinem Mandanten passt. Zu den Datenempfängerinnen und -empfängern gehört ein je nach Mandant und Vermittler stark divergierendes Netz aus Versicherern, Rückversicherern, Maklerpools, Untervermittlern, Tippgebern, Kreditinstituten, Bausparkassen und vielen weiteren Stellen.

Während das Verhältnis zwischen den Versicherten und ihren Versicherungen durch den Code of Conduct für die Versicherungsbranche umfassend geregelt ist, fehlt es bislang an branchenweiten einheitlichen Regelungen für die zwischengeschalteten Stellen. Teilweise erfolgen die betreffenden Datenübermittlungen auf der Grundlage verschiedener Einwilligungserklärungen, deren Muster einzelne Maklerinnen und Makler oder Versicherungspools entworfen haben. Diese Texte sind einzelfallbezogen und kaum dazu geeignet, das komplexe Geflecht aus Datenübermittlungen zu beschreiben, die eine Vermittlungstätigkeit nach sich zieht. Vielfach erfolgen in der Praxis auch Datenerhebungen und -übermittlungen ohne Rechtsgrund und damit unter Verletzung des § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG).
Der Verband Deutscher Versicherungsmakler (VDVM) hat diesen Missstand erkannt und ist mit dem Ziel einer branchenweiten Lösung an die AG Versicherungswirtschaft des Düsseldorfer Kreises herangetreten. In einem ersten Schritt sollen Mustertexte für Einwilligungserklärungen entworfen werden. Gegebenenfalls wird sich die Erarbeitung eines Code of Conduct anschließen. Die Beratung des VDVM erfolgt im Wesentlichen durch unsere Behörde sowie durch das Schleswig-Holsteinische Unabhängige Landeszentrum für Datenschutz (ULD), das den Vorsitz der AG innehat. Die Rolle des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit folgt aus seiner Zuständigkeit für den VDVM, der seinen Sitz in Hamburg hat. Eine eventuelle Prüfung der erarbeiteten Ergebnisse nach § 38a BDSG wird daher gegebenenfalls uns obliegen.

3.3 Geplante Datei zur Verhinderung von Tachomanipulationen

Zur geplanten Einführung einer Datei zur regelmäßigen Speicherung der Kilometerstände von Kraftfahrzeugen haben wir uns kritisch positioniert.

Die manipulative Herabsenkung des Tachostandes in Kraftfahrzeugen durch kriminelle Gruppen steigert den Wiederverkaufswert der Wagen und fügt Gebrauchtwagenkäufern dadurch hohe finanzielle Schäden zu. Betroffen sind auch Kfz-Versicherungen bei Verkehrsunfällen, weil die nach einem Verkehrsunfall fälligen Leistungen sich am Kilometerstand orientieren.

Zur Eindämmung des verbreiteten Delikts möchte ein baden-württembergisches Unternehmen eine Datei errichten, in die Fahrzeugverkäufer, Werkstätten, Versicherungen und andere Stellen die Kfz-Identifikationsnummer (FIN) und den aktuellen Kilometerstand der Fahrzeuge einspeisen, mit denen sie befasst sind. Auf die Weise kann nachvollzogen werden, ob der Wert zwischen zwei Einmeldungen irregulär gesunken ist. Als Rechtsgrundlage für die Datenübermittlungen sieht das Unternehmen vom Fahrzeughalter abzugebende Einwilligungen vor.

Wir haben uns sowohl in der AG Auskunfteien als auch in der AG Versicherungswirtschaft des Düsseldorfer Kreises gegenüber der Einwilligungslösung kritisch positioniert. Unserer Ansicht nach weist eine solche Einwilligung nicht das in § 4a Abs. 1 S. 1 Bundesdatenschutzgesetz Maß an Freiwilligkeit auf. Es ist zu erwarten, dass eine Weigerung des Betroffenen, bei Inspektionsterminen seines Fahrzeugs die Kilometerstände übermitteln zu lassen, zu erheblichen Nachteilen führen kann. Sobald es marktüblich geworden ist, dass zu einem Wagen in regelmäßigen Abständen aktuelle Werte in der Datei vermerkt werden, wird es schwieriger werden, einen Gebrauchtwagen zu verkaufen, zu dem solche Nachweise nicht verfügbar sind. Die Verweigerung der Einwilligung wird damit voraussichtlich sofort zur erheblichen Absenkung des Verkaufswerts oder sogar zur faktischen Unverkäuflichkeit des Wagens führen, weil potentielle Käufer mangels Nachweises eine Tachomanipulation für wahrscheinlich halten würden. In dieser Drucksituation ist eine freie Entscheidung des Fahrzeughalters nicht vorstellbar.

Die Thematik der Warndatei wirft ferner generelle Einwände unter dem Gesichtspunkt der Verhältnismäßigkeit und Datensparsamkeit auf. Mit ihrer Einrichtung und Etablierung verschiebt sich die faktische Darlegungslast zu Ungunsten der Betroffenen. Von ihnen wird dann ein regelmäßiger Nachweis erwartet, dass sie nicht betrügerisch handeln. Diese für die informationelle Selbstbestimmung des Einzelnen verheerende Entwicklung würde durch die Kfz-Warndatei auf einen weiteren Lebensbereich ausgeweitet werden.

4. Handel und Werbung

4.1 Werbeschreiben eines Versandhändlers

Ein Versandhändler hat wiederholt Werbeschreiben an Kunden verschickt, die der werblichen Nutzung ihrer Daten widersprochen haben.

Wir haben ein hohes Bußgeld gegen ein Hamburger Versandhaus wegen der unerlaubten Versendung von Katalogen und anderen Werbemitteln erlassen. Die Kundin, die sowohl bei dem Versandhaus direkt als auch bei dem Onlineshop einer weiteren Marke des Unternehmens Ware bestellt hatte, widersprach mehrfach der werblichen Nutzung ihrer Daten. Das Versandhaus unterließ es bis zu unserer Intervention, die Kundenverwaltung des weiteren Onlineshops über den Widerspruch zu informieren, sodass die Betroffene nach wie vor regelmäßig Werbeschreiben und -anrufe erhielt. Dass das Unternehmen in der Vergangenheit bereits wegen eines ähnlichen Falls aufgefallen war, fiel im Rahmen des Ordnungswidrigkeitenverfahrens nach § 43 Abs. 2 Nr. 5b Bundesdatenschutzgesetz (BDSG) besonders ins Gewicht.

Erschwerend kam in demselben Fall eine weitere Ordnungswidrigkeit nach § 43 Abs. 1 Nr. 3 BDSG hinzu. Eines der an die Betroffene gesendeten Werbeschreiben enthielt keinen Hinweis auf das Widerspruchsrecht des Empfängers, obwohl dies nach § 28 Abs. 4 S. 2 BDSG für solche Sendungen verpflichtend ist. Beide Rechtsverletzungen wurden gemeinsam empfindlich geahndet.

5. Unterlassungsklagengesetz

5.1 Änderung des Unterlassungsklagengesetzes

Der Vorschlag, die Datenschutzaufsichtsbehörden in die Verbandsklagebefugnis von Verbraucherschutzverbänden gegen Datenschutzverstöße einzubinden, fand im Gesetzgebungsverfahren Berücksichtigung.

Zum 1. Oktober 2016 soll eine Änderung des Unterlassungsklagengesetzes (UKlaG) in Kraft treten, die es insbesondere den Verbraucherschutzverbänden ermöglichen wird, gerichtlich gegen Verstöße von Unternehmen gegen datenschutzrechtliche Regelungen vorzugehen. Seit Mitte des Jahres 2014 wurde im Kreise der Datenschutzbeauftragten intensiv über die geplante Gesetzesänderung diskutiert. Die absehbare Verbesserung der Rechtsdurchsetzung auf dem Gebiet des Datenschutzes wurde dabei von der Mehrheit der Konferenz der Datenschutzbeauftragten begrüßt und unterstützt.

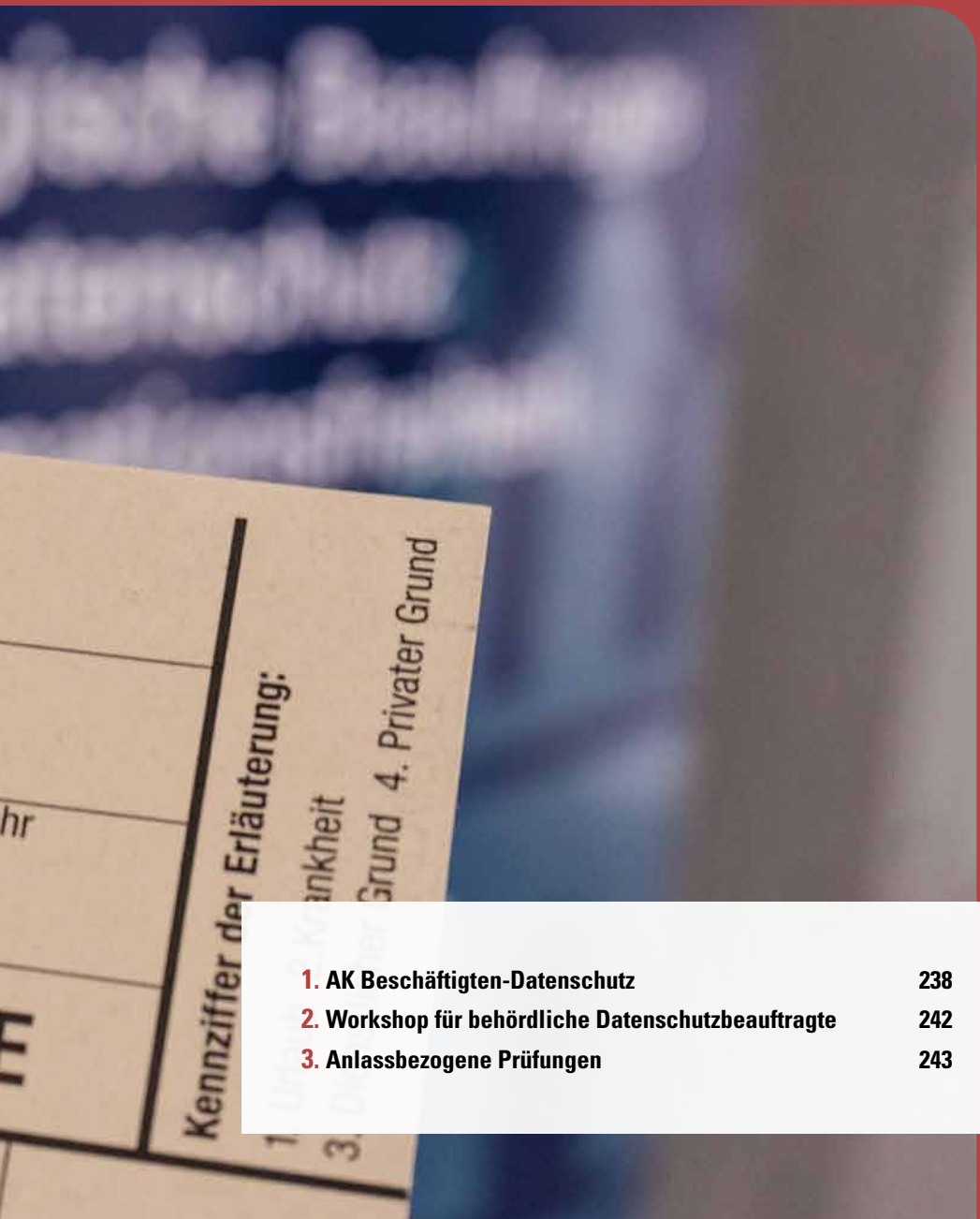
Bedenken bestanden allerdings dahingehend, dass durch die Neuregelung eine Parallelstruktur zu den Aufsichtsbehörden geschaffen werden könnte. Hierbei besteht die Gefahr von Abstimmungsproblemen, zumal der Rechtsweg jeweils zu unterschiedlichen Gerichten eröffnet ist.

Die Aufsichtsbehörden schlugen daher vor, eine frühzeitige Beteiligung der zuständigen Aufsichtsbehörden verpflichtend vorzusehen. Zumindest für das gerichtliche Verfahren wurde eine Anhörungspflicht der Aufsichtsbehörden gefordert, wie sie bereits in § 8 UKlaG für andere Fälle vorgesehen ist. Ein Schreiben unsererseits an das Bundesministerium der Justiz und für Verbraucherschutz unterstützte diese Position ebenso wie die Anhörung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit vor dem Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages. Die Anhörungspflicht wurde dann auch mit § 12 a UklaG in den Gesetzesentwurf (BT-Drucksache 18/4631) aufgenommen. Die Beschlussempfehlung des Ausschusses für Recht und Verbraucherschutz (BT-Drucksache 18/6916) hat den Gesetzentwurf einschließlich der Vorschrift über die Anhörungspflicht der Datenschutzaufsichtsbehörden angenommen und dabei nur Änderungen vorgeschlagen, die diese Thematik nicht betreffen.

Es bleibt abzuwarten, wie sich die Neuregelung auf die Praxis der Datenschutzaufsichtsbehörden auswirken wird. Wir werden die Zusammenarbeit mit den Verbraucherverbänden intensivieren, um auch auf diesem Wege die Durchsetzung der Rechte Betroffener zu stärken und einer Aufsplitterung des Rechts durch die unterschiedlichen Rechtswege entgegenzuwirken.


Name
ARBEITNEHMER
Dienststelle
DATENSCHUTZ
Monat
ZEITWERTKARTE
GLEITZEIT
Geht
Auswertung

BESCHÄFTIGTENDATENSCHUTZ IX.



1. AK Beschäftigten-Datenschutz 238
2. Workshop für behördliche Datenschutzbeauftragte 242
3. Anlassbezogene Prüfungen 243

1. AK Beschäftigten-Datenschutz

Nachdem wir den Vorsitz des Arbeitskreises Beschäftigten-Datenschutz übernommen hatten (vgl. 24. TB, IV 2), sind viele datenschutzrechtliche Fragestellungen in den Sitzungen im Jahr 2014 und 2015 behandelt worden. Über die wichtigsten Themen berichten wir in den folgenden Kapiteln.

1.1 Mitarbeiterüberwachung – Einsatz von Ortungssystemen

Der Einsatz von Ortungssystemen durch Arbeitgeber darf nicht zu permanenter Überwachung der Beschäftigten führen.

Uns erreichen häufig Anfragen zur Zulässigkeit der Ausrüstung von Firmenfahrzeugen mit GPS-Empfängern oder anderer Ortungsmöglichkeiten, beispielsweise über das dienstliche Smartphone. Dabei ist für die Beschäftigten von Interesse zu erfahren, ob der Arbeitgeber mit einem solchen System den Arbeitsplatz überwachen darf und ob Ortungsdaten beispielsweise bei privater Verwendung des Fahrzeugs erhoben, verarbeitet oder genutzt werden dürfen, wie etwa in Pausen oder nach Feierabend. Befürchtet wird eine mehr oder weniger lückenlose Überwachung.

Vielfach sind die Beschäftigten gar nicht oder unzureichend über den Einsatz solcher Ortungsmöglichkeiten und deren Einsatzzwecke informiert. Vorabkontrollen nach § 4 d Abs. 5 BDSG wurden oftmals mit dem Argument nicht durchgeführt, weil keine personenbezogenen Beschäftigtendaten verarbeitet würden. Mit der Zusammenführung beispielsweise der Personaleinsatzpläne und der Ortungsdaten der Fahrzeuge ist ein Personenbezug ohne besonderen Aufwand möglich.

Bei unseren Prüfungen stand für die Unternehmen üblicherweise die Personaleinsatzplanung der Außendienstmitarbeiter oder deren Zeiterfassung im Vordergrund.

Nach § 32 Abs. 1 S. 1 BDSG dürfen personenbezogene Beschäftigtendaten erhoben, verarbeitet oder genutzt werden, wenn sie für die Durchführung des Beschäftigungsverhältnisses erforderlich sind. Im Rahmen unserer Prüfungen stellen wir den Unternehmen folgende Fragen:

1. Sind alle Dienstfahrzeuge/Smartphones o.ä. mit GPS-Ortungssystemen ausgestattet? Wenn nicht alle Fahrzeuge/Geräte damit ausgerüstet bzw. die Systeme aktiviert wurden, um wie viele Fahrzeuge/Geräte handelt es sich?

2. Welche Daten werden mit den eingesetzten GPS-Ortungssystemen erhoben?

3. Werden neben Standort und Route bei Fahrzeugen weitere technische Angaben über die Fahrzeugnutzung erhoben (z. B. über den Betriebszustand des Motors, die Drehzahlbereiche oder das Bremsverhalten)?

4. Zu welchen konkreten Zwecken werden die Daten über die GPS-Ortungssysteme erhoben?

5. Werden die Daten beim Unternehmen gespeichert?
5.1. Wenn nein, welcher Dienstleister wurde damit beauftragt?
5.2. Werden die Anforderungen zur Auftragsdatenverarbeitung nach § 11 Abs. 2 BDSG eingehalten?

6. Über welchen Zeitraum werden die Daten gespeichert?

7. Gibt es ein Konzept zur Löschung der Daten?
7.1. Wenn ja, unter welchen Voraussetzungen werden die Daten gelöscht?
7.2. Wenn nein, wie lange bleiben die Daten personenbeziehbar gespeichert?

8. In welcher Form werden die Daten ausgewertet?

9. Findet über die Auswertung der GPS-Daten auch eine Leistungs- und Verhaltenskontrolle der Mitarbeiter statt?

10. Erfolgt eine langfristige Speicherung der Daten zu statistischen Zwecken? Werden die Daten vorab aggregiert?

11. Werden die mit GPS ausgestatteten Fahrzeuge/Geräte von den Mitarbeitern auch außerhalb der Dienstzeiten, etwa zum Zweck der An- und Abfahrt zum Arbeitsplatz oder für private Telefonate genutzt?

12. Besteht eine Möglichkeit, die GPS-Ortung im Falle einer privaten Nutzung auszuschalten bzw. zu deaktivieren?

13. Gibt es in Ihrem Betrieb einen Betriebsrat?
13.1. Wenn ja, ist der Einsatz der GPS-Systeme in einer Betriebsvereinbarung geregelt?
13.2. Wenn nein, existiert zum Einsatz der GPS-Ortung eine Arbeitsanweisung?

14. Wie wurden die Mitarbeiter über den Einsatz von Ortungssystemen informiert?

15. Auf welche Art und Weise werden Personaleinsätze geplant und dokumentiert?

Unter engen Voraussetzungen kann der Einsatz von GPS in Firmenwagen für die Personaleinsatzplanung und bei Smartphones für die Zeiterfassung erlaubt sein. Eine Überwachung in Pausen oder nach Feierabend ist unzulässig.

1.2 Mindestlohn

Zur Vermeidung von Haftungsrisiken nach dem „Mindestlohngesetz" ist es in der Regel weder erforderlich noch zulässig, Beschäftigtendaten von einem beauftragten Unternehmen an den Auftraggeber zu übermitteln.

Mit Einführung des gesetzlichen Mindestlohnes erreichten uns viele Anfragen von Auftragnehmern, weil sich Auftraggeber weit reichende Einsichtsrechte in Unterlagen mit personenbezogenen Daten der Beschäftigten einräumen lassen wollten oder die Übermittlung entsprechender Dokumente forderten. Hintergrund ist, dass Auftraggeber sich von einem Haftungsrisiko freihalten wollen. Nach § 13 des Mindestlohngesetzes (MiloG) haftet der jeweilige Auftraggeber dafür, dass die von ihm beauftragten Unternehmer sowie die von diesen beauftragten Subunternehmer ihren Beschäftigten den gesetzlich zustehenden Mindestlohn zahlen.

Der Gesetzgeber hat allerdings keine ausdrücklichen Regelungen dazu erlassen, wie sich der Auftraggeber davon überzeugen kann, ob der Auftragnehmer den Mindestlohn zahlt. Der Auftraggeber und auch die beauftragten Unternehmen sowie Subunternehmen müssen bei der Auswahl und dem Einsatz der Kontrollmittel die datenschutzrechtlichen Anforderungen einhalten. Aus Sicht des Auftraggebers ist zu prüfen, inwieweit die Erhebung und Speicherung der personenbezogenen Beschäftigtendaten als Mittel für die Erfüllung eigener Geschäftszwecke zur Wahrung berechtigter Auftraggeberinteressen erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG). Der beauftragte Unternehmer sowie die Subunternehmer müssen untersuchen, ob die Übermittlung personenbezogener Daten ihrer Beschäftigten für die Durchführung des Beschäftigungsverhältnisses erforderlich ist (§ 32 Abs. 1 Satz 1 BDSG). Dabei darf keine pauschale Bewertung erfolgen, es bedarf einer Prüfung im konkreten Einzelfall. Vor diesem Hintergrund ist es datenschutzrechtlich nicht zulässig, wenn der Auftraggeber auf Basis einer vertraglichen Abrede mit dem beauftragten Unternehmer bei diesem einen pauschalen Zugriff auf bestimmte arbeitsvertragliche Unterlagen möglicherweise aller Beschäftigten oder gar auf deren Personalakten erhält. Ebenso unzulässig ist die Übermittlung nichtanonymisierter Gehaltsbescheinigungen. Angaben z. B. zur Konfessionszugehörigkeit, zum Familienstand, zur gewählten Steuerklasse, zur Anzahl der Kinder, zum vollständigen Geburtsdatum und zur Privatanschrift des Beschäftigten stellen Angaben dar, deren

Erhebung zur Verringerung des Haftungsrisikos für den Auftraggeber nicht erforderlich sind (*https://www.datenschutzzentrum.de/artikel/871-.html*).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zu diesem Thema auch eine Entschließung verabschiedet: (*http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/89DSK-MindestlohngesetzUndDatenschutz.pdf?__blob=publicationFile&v=5*) .

1.3 Arbeitgeberzeitschrift AKTIV

Private Anschriften der Beschäftigten dürfen vom Arbeitgeber nicht genutzt werden, um eine von Arbeitgeber- und Unternehmensverbänden herausgegebene Zeitschrift zu versenden.

Die Zeitschrift AKTIV wird seit 1972 von der IW Medien bzw. ihren Vorgängerunternehmen herausgegeben und erscheint in der Regel 14-tägig bis monatlich. Die IW Medien betreut die redaktionellen und publizistischen Aktivitäten des Instituts der deutschen Wirtschaft Köln e.V. Hierbei handelt es sich um ein von Arbeitgeber- und Unternehmerverbänden finanzierte, beratend tätige Institution. Die Zeitschrift AKTIV ist ein Erzeugnis der IW Medien, welches dazu bestimmt ist, Arbeitnehmer in Unternehmen über branchenspezifisch relevante politische, wirtschaftliche und gesellschaftliche Entwicklungen zu informieren sowie insbesondere Verständnis für branchen- und betriebsrelevante sowie gestaltende, politische sowie wirtschaftliche Ansichten der Arbeitgeber bei den Arbeitnehmern hervorzurufen.
Arbeitgeber abonnieren die Zeitschrift und stellen der IW Medien die privaten Postanschriften ihrer Arbeitnehmer zur Verfügung, so dass ein Direktversand der Zeitschrift von IW Medien an die einzelnen Arbeitnehmer erfolgen kann. Bei der erstmaligen Zusendung eines Exemplars wird dem Empfänger unter Beilegung eines entsprechenden Vordrucks die Möglichkeit gegeben, der weiteren Zusendung von AKTIV unmittelbar gegenüber IW Medien zu widersprechen. Dort werden die Daten der widersprechenden Arbeitnehmer in einer „Robinsonliste" zusammengetragen und mit der entsprechenden vom jeweiligen Arbeitgeber überlassenen Auflistung der Arbeitnehmerdaten abgeglichen. Eine bloße Auslegung der AKTIV im Unternehmen im Gegensatz zur Versendung an die Privatadressen der Arbeitnehmer wird von Arbeitgeberseite als weniger geeignet betrachtet, da durch ein bloßes Auslegen der Zeitung nicht sämtliche Arbeitnehmer, wie etwa Außendienstler, erreicht werden könnten. Vor diesem Hintergrund wird die unmittelbare Versendung an die Privatanschriften der Arbeitnehmer für erforderlich erachtet. Die IW Medien handele im Hinblick auf die Versendungstätigkeit als Auftragsdatenverarbeiter i.S.d. § 11 BDSG, mithin als Dienstleister der Arbeitgeber.

Bereits 2007 haben die Aufsichtsbehörden für den Datenschutz mehrheitlich die Auffassung vertreten, dass die Nutzung der Privatadresse des Arbeitnehmers zum Zwecke der Versendung einer Zeitschrift eines Arbeitgeberverbandes unzulässig ist. Im Januar 2015 haben sich die Aufsichtsbehörden für den Datenschutz erneut mit diesem Thema beschäftigt, weil ein neues Gutachten vorgestellt wurde, das die Nutzung für zulässig erachtet.

Eine Rechtfertigung der Datennutzung durch § 32 Abs. 1 S. 1 BDSG scheidet aus. Zutreffend ist, dass den Arbeitgeber eine Vielzahl an Informations- und Aufklärungspflichten im Verhältnis gegenüber den Arbeitnehmern trifft. Zur Erfüllung dieser Pflichten kann er sich Informationsmaterials aus fremden Quellen bedienen. Zutreffend ist ebenfalls, dass der Arbeitgeber für die Erfüllung ihn treffender Verpflichtungen aus dem Arbeitsverhältnis hierfür grundsätzlich die personenbezogenen Daten der Arbeitnehmer verwenden kann. Eine Datennutzung ist jedoch lediglich dann zulässig, sofern sie für die Erfüllung der Pflicht erforderlich ist. Insofern ist zu prüfen, ob der verfolgte Zweck auch ohne die jeweils intendierte Datennutzung zu erreichen ist.

Ein Direktversand unter Verwendung der Privatanschriften der Arbeitnehmer ist zur Erfüllung der hier in Rede stehenden Pflichten nicht erforderlich. Die Zeitschrift AKTIV enthält lediglich allgemeine, abstrakte Informationen, die nicht für die Erfüllung der Aufklärungspflichten des Arbeitgebers gegenüber den jeweiligen Arbeitnehmern in seinem Betrieb relevant sind. Insbesondere lässt sich hieraus nicht die Erforderlichkeit ableiten, die Zeitschrift durch Verwendung der Privatadressen der Arbeitnehmer zu versenden. Das Auslegen der Zeitschrift reicht hier völlig aus und ist möglich, ohne dass die Anschriftendaten der Arbeitnehmer genutzt werden.

Diese Auffassung wird mehrheitlich von den Aufsichtsbehörden für den Datenschutz vertreten.

2. Workshop für behördliche Datenschutzbeauftragte

Seit einigen Jahren bieten wir Informationsveranstaltungen für behördliche Datenschutzbeauftragte mit dem Schwerpunkt Personaldaten an. In diesen zweistündigen Workshops berichten wir auch über aktuelle IT-Themen (s. dazu VI 1.1, 1.8) und erörtern die von den behördlichen Datenschutzbeauftragten eingebrachten Fragestellungen. Neben der aktuellen Rechtsprechung des EuGH zu Safe Harbor und einem Kurzbericht über die Entwicklung der DSGVO standen im Vordergrund die Informationen über das Projekt KoPers.

2.1 KoPers - Sachstand

Die datenschutzrechtliche Abstimmung für den Bereich Versorgungsempfänger wurde erfolgreich abgeschlossen.

Das Projekt KoPers ist mit der Verarbeitung der Daten der Versorgungsempfänger im September 2014 im Echtbetrieb gestartet (vgl. 24. TB, IV 4). Daten verarbeitende Stelle ist ausschließlich das Zentrum für Personaldienste (ZPD). Durch die frühzeitige Einbindung konnten wir mit dem Projekt die datenschutzrechtlichen Fragestellungen klären.

Die Planungen sehen bisher vor, dass zwei kleinere Anstalten des Öffentlichen Rechts zum 01.03. bzw. 01.04.2016 beginnen, um Erfahrungen sammeln zu können. Für alle anderen Behörden, Landesbetriebe und die am Projekt teilnehmenden Anstalten des öffentlichen Rechts sollte der Wechsel zum 01.01.2017 erfolgen. Zum Redaktionsschluss stand der genaue Zeitplan allerdings noch nicht fest. Gleichwohl haben wir mit dem Projekt eine Risikoanalyse und Verfahrensbeschreibung für die zwei startenden Betriebe abgestimmt und die Vorlage an die Daten verarbeitenden Stellen vorbereitet. Ihnen obliegt die Beteiligung ihrer behördlichen Datenschutzbeauftragten.

Mit dem Projekt KoPers stehen wir nach wie vor im engen Kontakt. Datenschutzrechtliche Probleme können somit zeitnah benannt und vom Projekt gelöst werden.

3. Anlassbezogene Prüfungen

Strukturelle Defizite verursachen datenschutzrechtliche Probleme.

Ein Hinweis über unbefugte Datenspeicherung und Zugriffe von Beschäftigtendaten veranlasste uns, eine umfangreiche Prüfung bei einem Unternehmen durchzuführen. Dabei offenbarten sich erhebliche strukturelle Defizite, die zu einigen Forderungen führten:

1. Das Unternehmen muss die Zuständigkeiten für die Bearbeitung von Personalangelegenheiten insbesondere im Bereich der Betriebsgruppenleiter präzise regeln, die Prozesse dokumentieren sowie die Regelungen den Betriebsgruppenleitern in geeigneter Weise bekannt geben. Festzulegen sind dabei auch die zum Zwecke der Aufgabenwahrnehmung erforderlichen personenbezogenen Datenarten der der jeweiligen Betriebsgruppe zugeordneten Beschäftigten, deren Daten an die Betriebsgruppenleiter weiter gegeben werden dürfen, sowie die Art und Weise der Datenhaltung bei den Betriebsgruppenleitern.

2. Die im Ordner des Betriebsgruppenleiters gespeicherten Dokumente sind nach Abschluss der Prüfung zu löschen.

3. Für die Aufgabenwahrnehmung der Betriebsgruppenleiter wird dringend empfohlen, unterstützende Arbeitsmittel einzuführen. Dabei könnte beispielweise für die Personaleinsatzplanung das bereits in einigen Tochterunternehmen eingesetzte Programm hilfreich sein.

4. Der betriebliche Datenschutzbeauftragte hat für die Beschäftigten ein Schulungskonzept zu erstellen.

5. Das Unternehmen hat dafür Sorge zu tragen, dass der Prozess für die Vergabe und das Einrichten von Nutzern dokumentiert wird, insbesondere im Hinblick auf die Zuständigkeiten für diese Aufgaben. Dabei ist darauf zu achten, dass revisionssicher festgestellt werden kann, wer wann mit welchen Rechten einen Nutzer eingerichtet hat.

6. Für die Kontrolle solcher Protokollierungen ist ein Konzept zu erstellen.

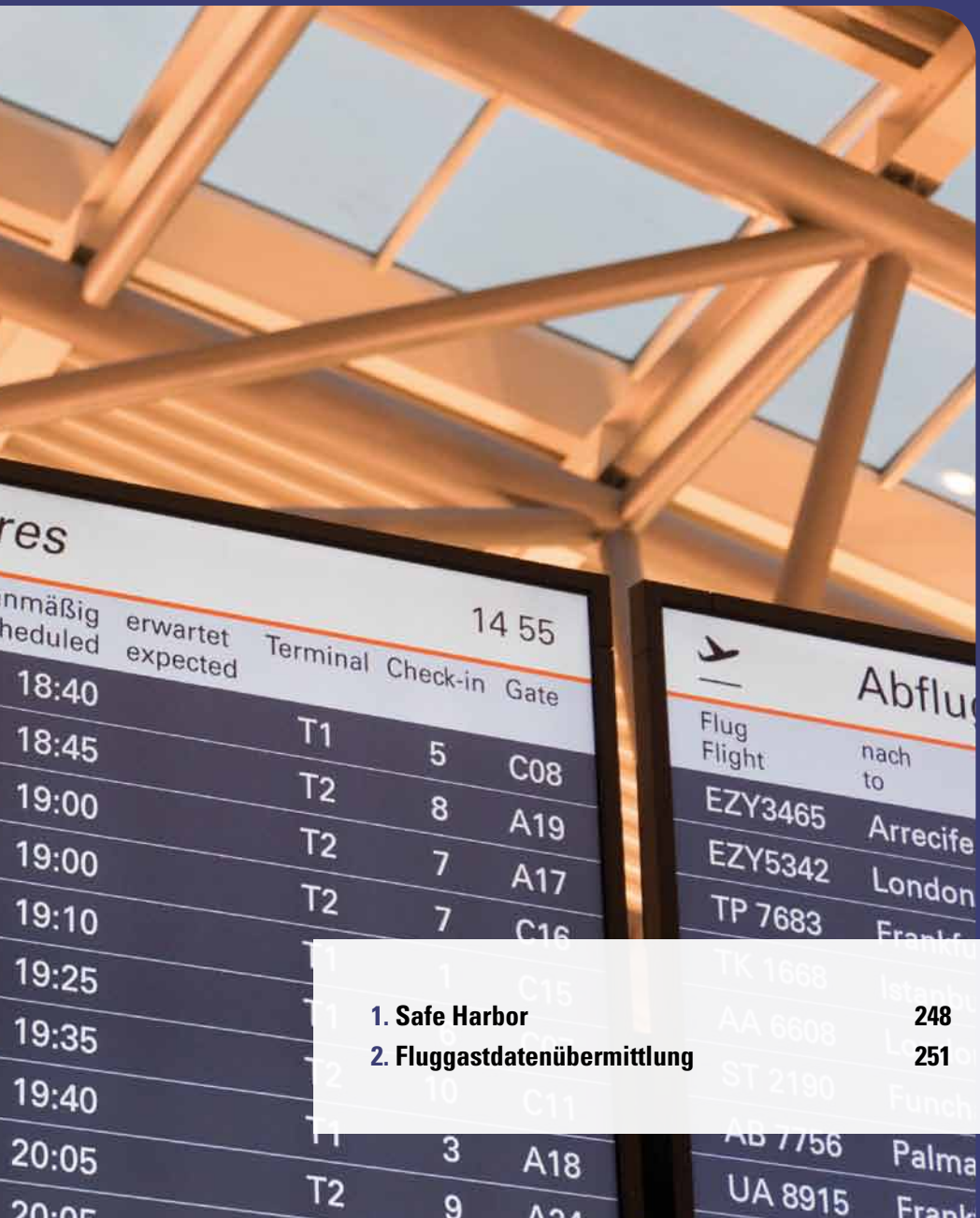
7. Das Unternehmen muss durch geeignete Maßnahmen gewährleisten, dass personenbezogene Daten nicht unbefugt gelesen oder verwendet werden können. Zu vermeiden ist der unverschlüsselte Mailverkehr, insbesondere zwischen Betriebsarzt und dem Arbeitgeber. Es kommt nicht darauf an, ob es sich dabei nur um das interne Kommunikationsnetz handelt.

Das Unternehmen hatte daraufhin insbesondere für die Mitarbeiter mit Führungsaufgaben eine umfangreiche Leitlinie für die Verarbeitung und Nutzung personenbezogener Beschäftigtendaten erstellt. Das vom betrieblichen Datenschutzbeauftragten des Unternehmens erarbeitete Schulungskonzept wurde umgehend für die datenschutzrechtliche Fortbildung der Führungskräfte genutzt.

Ein weiterer Prüfungsfall betraf Unterlagen über Lebensläufe von Bewerbern, die in einem allgemein offen zugänglichen Altpapiercontainer gefunden wurden. Der Inhaber des Unternehmens, der als Existenzgründer noch keine festangestellten Mitarbeiter beschäftigte, hatte nach seiner Darstellung Vorkehrungen getroffen, dass Bewerbungsunterlagen datenschutzgerecht gelagert und vernichtet werden. Dennoch wurden einige nicht mehr benötigte Bewerberunterlagen von einer Aushilfe versehentlich im Altpapiercontainer entsorgt. Der Unternehmer sagte zu, zukünftig auf eine datenschutzrechte Entsorgung von Unterlagen mit personenbezogenen Daten zu achten.


14:55
Check-in Gate
2 B20
2 C08
2 A38
3 A19
8 A32
7 C16
7 A17
6 C06
B31
A37
Abflug · Departu
Flug Flight
nach to
über via
D8 5187 Barcelona
LX 2751 Zürich
SQ 2047 Frankfurt
CA 6122 München
AY 856 Helsinki
KM 369 Malta
LO 394 Warschau
FR 4026 Alicante
EW 1037 Düsseldorf
FR 9205 Porto

INTERNATIONALES X.



1. **Safe Harbor** **248**
2. **Fluggastdatenübermittlung** **251**

1. Safe Harbor

Die Entscheidung des Europäischen Gerichtshofs zur Zulässigkeit von Übermittlungen personenbezogener Daten in die USA auf der Grundlage von Safe Harbor stellt in datenschutzrechtlicher Hinsicht einen Meilenstein dar.

Im 24. TB (VI. 2.1.1) haben wir zuletzt über dieses Thema berichtet. Dort wurde noch einmal dargestellt, dass die EU-Kommission schon im Jahre 2000 eine Entscheidung dahingehend getroffen hat, dass Unternehmen in den USA, die dem Safe-Harbor-System beigetreten sind, ein angemessenes Datenschutzniveau aufweisen. Die Folge war, dass europäische Unternehmen bei Übermittlungen personenbezogener Daten an diese Unternehmen keine darüber hinausgehenden Schutzvorkehrungen treffen mussten, wenn die Übermittlungen auch innerhalb Europas zulässig gewesen wären.

Schon 2010 gab es die ersten Hinweise darauf, dass die Safe-Harbor-Zertifizierungen nicht in allen Fällen dem erwarteten Standard entsprechen, verstärkt wurde die Problematik unter Berücksichtigung der Prism-Vorwürfe im Jahre 2013. Das führte im Ergebnis zu einem 13-Punkte-Katalog der EU-Kommission mit dem Ziel, das Safe-Harbor-Abkommen zu erneuern (Einzelheiten und Nachweise hierzu im 24. TB, VI. 2.1.1).

Angesichts der Tatsache, dass die Verhandlungen der EU-Kommission mit den USA sich deutlich verzögerten und bisher immer noch nicht abgeschlossen sind, haben sich die Datenschutzaufsichtsbehörden verstärkt seit Ende 2014 mit der Frage befasst, ob die Übermittlungen personenbezogener Daten allein auf der Grundlage von Safe Harbor ausgesetzt werden können oder sogar müssten. Im März 2015 erließ die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Entschließung, die sich außerordentlich kritisch mit dem Thema auseinandersetzte (im Wortlaut abrufbar unter: *https://www.datenschutz.hessen.de/k89.htm#entry4319*).

Mit Spannung erwartet wurde ein Urteil des Europäischen Gerichtshofs (EuGH), das sich mit der EU-Kommissionsentscheidung unter dem Eindruck der Enthüllungen von Edward Snowden im sogenannten Schrems-Verfahren auseinandersetzte. Dieses Urteil erging am 6. Oktober 2015 und fand enorme Aufmerksamkeit in der Öffentlichkeit (abrufbar unter *http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62014CJ0362*) und insbesondere bei allen Datenschutzaufsichtsbehörden Europas. Wir betrachten diese Entscheidung als historisch im Sinne unserer europäischen Werteordnung und gehen davon aus, dass sie einen Wendepunkt im Datenverkehr zwischen der EU und den USA markiert (vgl. unsere Presseerklärung unter *https://www.datenschutz-hamburg.de/news/detail/article/eugh-kippt-transatlantisches-safe-harbor-abkommen.html?tx_ttnews%5BbackPid%5D=170&cHash=4d11fb012149f1a2faf43033f19fce5f*).

Ohne das ausführliche Urteil an dieser Stelle in Einzelheiten wiedergeben zu wol-

len, ist es doch erwähnenswert, dass sich der EuGH gerade zu den Spähangriffen der US-Behörden und den fehlenden Datenschutzrechten der Betroffenen deutlich positioniert hat:

„Insbesondere verletzt eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des durch Art. 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens.
Desgleichen verletzt eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des in Art. 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz. Nach Art. 47 Abs. 1 der Charta hat nämlich jede Person, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, das Recht, nach Maßgabe der in diesem Artikel vorgesehenen Bedingungen bei einem Gericht einen wirksamen Rechtsbehelf einzulegen. Insoweit ist schon das Vorhandensein einer wirksamen, zur Gewährleistung der Einhaltung des Unionsrechts dienenden gerichtlichen Kontrolle dem Wesen eines Rechtsstaats inhärent." (Rdnr. 94 und 95 des Urteils).

Schon 2 Tage nach Veröffentlichung des Urteils fand eine Sondersitzung der Subgroup International Transfers der Artikel 29-Gruppe der EU-Kommission statt, die sich ausführlich mit den Folgen der Entscheidung für die Praxis auseinandersetzte und eine Sondersitzung der Artikel 29-Gruppe selbst vorbereitete. Das Ergebnis dieser Sitzung ist in einem Statement vom 15. Oktober 2015 niedergelegt, das unter *https://www.datenschutz-hamburg.de/uploads/media/Statement_der_Art.29-Gruppe_zu_Safe-Harbor_2015-10-16.pdf* abgerufen werden kann. Daraus wird die Forderung an die europäischen und mitgliedstaatlichen Institutionen deutlich, im Zusammenwirken mit den US-amerikanischen Behörden politische und technische Lösungen zu finden, um die Grundrechte bei Datenübermittlungen zu wahren. Übermittlungen auf der Grundlage von Safe Harbor, die nach dem EuGH-Urteil erfolgen, werden als rechtswidrig eingestuft. Als ein Instrument zur Lösung der Problematik spricht die Art. 29-Gruppe die noch laufenden Verhandlungen über das Safe-Harbor-Abkommen an. Gefordert werden Verpflichtungen in Bezug auf die nötige Kontrolle des staatlichen Zugriffs, Transparenz, Verhältnismäßigkeit, Rechtsmittel und Datenschutzrechte. Angekündigt wird in diesem Statement insbesondere auch, dass weiter untersucht werden wird, wie sich das Urteil auf weitere Übermittlungsinstrumente wie Standardvertragsklauseln oder verbindliche Unternehmensrichtlinien auswirken. Gleichzeitig nennt das Statement Ende Januar 2016 als Termin, nach dem die EU-Datenschutzaufsichtsbehörden verpflichtet seien, alle notwendigen und angemessenen Maßnahmen zu ergreifen.

Die Datenschutzkonferenz des Bundes und der Länder hat sich wenige Tage danach zum zweiten Mal nach der Entscheidung zu einer Sondersitzung getroffen und eine gemeinsame Position für die deutschen Datenschutzaufsichtsbehörden festgelegt. Diese orientiert sich im Wesentlichen an den Aussagen der Art. 29-Gruppe der EU-

Kommission (veröffentlicht unter *https://www.datenschutz.hessen.de/ft-europa.htm#entry4521*). Wesentlich dafür ist, dass Datenübermittlungen, die sich auf Safe Harbor stützen, nicht mehr als zulässig angesehen werden und auch die Zulässigkeit von Übermittlungen aufgrund von Standardvertragsklauseln oder verbindlichen Unternehmensregelungen in Frage gestellt werden. Die Datenschutzbehörden haben sich darauf verständigt, Datenübermittlungen in die USA, die bisher ausschließlich auf Safe Harbor gestützt waren, zu untersagen und keine neuen Genehmigungen auf der Grundlage von verbindlichen Unternehmensregelungen zu erteilen. Gleichzeitig wird die Kommission in dem Papier aufgefordert, in ihren Verhandlungen mit den USA auf die Schaffung ausreichend weitreichender Garantien zum Schutz der Privatsphäre zu drängen, wobei insoweit die Frist bis zum 31. Januar 2016 begrüßt wird.

Alle denkbaren Datenschutzinstitutionen auf europäischer (Art. 29-Gruppe und mehrere Unterarbeitsgruppen) und deutscher (Datenschutzkonferenz, alle Aufsichtsbehörden, Düsseldorfer Kreis, AG Internationaler Datenverkehr) sowie die Kommission selbst arbeiten seit dem 6. Oktober 2015 mit Hochdruck an der Lösung verschiedener Fragen, die diese Entscheidung aufgeworfen hat. Gleichzeitig findet über die verschiedenen Arbeitsgremien auch ein reger Austausch über die Verfahrensweisen der jeweiligen Aufsichtsbehörden statt. Zunächst ist es zwar wichtig, unmittelbar festzustellen, dass Datenübermittlungen auf der Grundlage von Safe Harbor nicht mehr zulässig sind. Darüber hinaus ist jedoch möglichst umgehend zu klären, ob Übermittlungen auf der Grundlage von Standardvertragsklausen und verbindlichen Unternehmensregelungen und wenn ja, unter welchen Umständen, überhaupt noch von den Aufsichtsbehörden akzeptiert werden können. Vor dem Hintergrund der Interessen derjenigen Unternehmen, die Datenübermittlungen in die USA vornehmen, erscheint es dringlich, Lösungen zu finden, die die Betroffeneninteressen im Sinne des EuGH-Urteils berücksichtigen.

Wir haben unsere konkrete Vorgehensweise über eine Information kommuniziert, die der Orientierung der Unternehmen dient und unsere schrittweise Umsetzung – auch in Abhängigkeit zu möglichen Erfolgen der EU-Kommission – der Entscheidung verdeutlicht (vgl. *https://www.datenschutz-hamburg.de/uploads/media/Information_zum_Safe-Harbor-Urteil_des_Europaeischen_Gerichtshofs.pdf)*. Noch im November 2015 haben wir eine Anzahl von Unternehmen angeschrieben und diese Information direkt übersandt. Dabei handelte es sich solche, von denen nach kursorischer Durchsicht der Safe-Harbor-Liste angenommen werden kann, dass sie Datenübermittlungen auf dieser Grundlage durchführen. Geplant ist, im Januar 2016 dann den nächsten Schritt zu gehen und diese Unternehmen im Rahmen von Prüfungen um Auskunft zu ersuchen, ob Übermittlungen personenbezogener Daten in die USA vorgenommen werden und auf welcher Rechtsgrundlage dies geschieht. Erst in einem dritten Schritt sind ab Februar – abhängig von den Ergebnissen und den Fortschritten der EU-Kommission – rechtliche Maßnahmen geplant. Diese Vorgehensweise ermöglicht es den betroffenen Unternehmen, ihre Datenübermittlungen in die USA vor etwaigen Maßnahmen

auf rechtlich sichere Grundlagen zu stellen. Eine Möglichkeit hierzu ist in bestimmten Fällen, in denen die Übermittlungen nicht unbedingt in die USA erfolgen müssen, die Daten in Europa zu verarbeiten.

2. Fluggastdatenübermittlung

Die vorgesehenen Regelungen zur Fluggastdatenübermittlung sind weiterhin kritisch zu begleiten. Als Rückschlag für den Datenschutz ist die EU-Richtlinie zu den Flugpassagierdaten anzusehen.

Wie bereits im letzten Tätigkeitsbericht angedeutet (vgl. 24.TB, VI. 2.3) und nicht anders zu erwarten, hat sich das Thema einer EU-Richtlinie zur Fluggastdatenspeicherung nicht von allein erledigt, sondern wurde wieder mit Nachdruck betrieben. Nachdem das Europäische Parlament noch im Jahre 2013 einen Vorschlag wegen der Befürchtung von Grundrechtsverletzungen abgelehnt hatte, hat der Innenausschuss des EU-Parlaments die Richtlinie im Dezember 2015 unter dem Eindruck der Pariser Anschläge abgesegnet. Bereits im Februar 2015 wurde ein entsprechender Bericht im Innenausschuss des Parlaments präsentiert und im Juli 2015 mehrheitlich angenommen. Vor dem Hintergrund, dass damit erneut eine Rechtsgrundlage für die Vorratsdatenspeicherung – vorgesehen sind derzeit insgesamt 5 Jahre – geschaffen werden soll, ist diese Entwicklung Besorgnis erregend. Dabei verständigte sich der EU-Rat auch darauf, dass alle Mitgliedsstaaten die Option zur Einbeziehung innerstaatlicher Strecken nutzen werden. Das bedeutet, dass diese Art der kritischen Vorratsdatenspeicherung auch auf die innerdeutschen Strecken ausgedehnt werden wird. Angesichts der Rechtsprechung des Europäischen Gerichtshofs zur Vorratsdatenspeicherung besteht jedoch die Erwartung, dass die Regelung wegen Verstoßes gegen die Grundrechte des Datenschutzes und des Privatlebens keinen Bestand haben wird.

Die bereits angekündigte Regelung zur Übermittlung von Passagierdaten an Kanada (vgl. 24.TB, VI. 2.3) ist bisher nicht verabschiedet. Das Europäische Parlament hat das Abkommen vielmehr im November 2014 dem Europäischen Gerichtshof zur Erstellung eines Gutachtens vorgelegt.

Das Ergebnis dieses Gutachten wird voraussichtlich auch unmittelbare Auswirkungen auf den Abschluss eines Passagierdatenabkommens mit Mexiko haben. Nachdem Mexiko einigen Fluggesellschaften für den Fall unterbliebener Übermittlungen von Fluggastdaten empfindliche Zwangsgelder angedroht hatte, hat die Europäische Kommission Verhandlungen mit Mexiko über ein entsprechendes Abkommen aufgenommen. Ohne eine solche Rechtsgrundlage, die insbesondere auch dem zu erwartenden Gutachten des Europäischen Gerichtshofs gerecht werden muss, sind die Datenübermittlungen rechtswidrig. Sie können dann auch durch Bußgelder der Datenschutzauf-

sichtsbehörden sanktioniert werden. Bisher gibt es keine Erkenntnisse über einen konkreten Zeitplan der Europäischen Kommission in dieser Angelegenheit.

Angesichts der von immer mehr Ländern geforderten Fluggastdatenübermittlungen sind Bestrebungen der EU zu begrüßen, ein Modellabkommen zu entwickeln, das anschließend zur Vertragsgrundlage mit verschiedenen Staaten gemacht werden kann. Dabei ist allerdings die Aufmerksamkeit auf die Inhalte eines solchen Modells zu richten, die sich an datenschutzrechtlichen Anforderungen zu orientieren haben. Durch die Absegnung der oben erwähnten Richtlinie auch für den europäischen Raum wird besonders zu beobachten sein, in welcher Weise ein derartiges Modellabkommen auch den Datenschutz der Betroffenen berücksichtigt.

INFORMATIONEN ZUR DIENSTSTELLE XI.

1. Eingabenstatistik 256
2. Bußgeldfälle und Anordnungen 258
3. Meldepflicht nach § 42a BDSG 260
4. Register 261
5. Presse- und Öffentlichkeitsarbeit 262
6. Aufgabenverteilung (Stand: 1. Januar 2016) 264

1. Eingabenstatistik

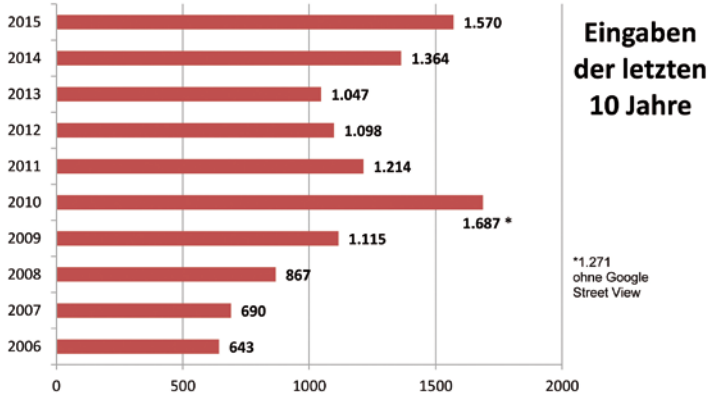
Die Eingaben beim Hamburger Datenschutzbeauftragten sind im Vergleich zum letzten Tätigkeitsbericht deutlich angestiegen. Dieser Anstieg hing nicht nur mit dem Urteil des Europäischen Gerichtshofs zum „Recht auf Vergessenwerden" zusammen.

Bürgerinnen und Bürger, die meinen, von staatlichen oder privaten Stellen in ihrem Recht auf informationelle Selbstbestimmung verletzt worden zu sein, können sich auf Grundlage der Datenschutzgesetze an die oder den örtlich zuständige/n Datenschutzbeauftragte/n wenden. Aufgabe der Datenschutzbeauftragten ist es dann, im Falle der Rechtsverletzung der Bürgerin oder dem Bürger zu ihrem bzw. seinem Recht zu verhelfen und eventuell auch schwerwiegende Rechtsverstöße zu ahnden (vgl. XI.2 Bußgelder und Anordnungen). Diese schriftlichen Beschwerden von Bürgerinnen und Bürgern werden als Eingaben bezeichnet. Die Eingaben von Bürgerinnen und Bürgern sind dabei in der Regel der Anlass für sogenannte anlassbezogene (Über-) Prüfungen von verantwortlichen Stellen. Ihnen kommt, besonders wenn wegen fehlender personeller Kapazitäten kaum noch anlassfreie Prüfungen durchgeführt werden können, eine hohe Bedeutung zu. Dabei sind sie die wohl wichtigste Kennzahl für die Tätigkeit der Datenschutzbeauftragten und ihrer Mitarbeiter und Mitarbeiterinnen sowie ein Indikator für die datenschutzrechtlichen Befindlichkeiten der Bürgerinnen und Bürger.

Im Berichtszeitraum 2014/2015 haben uns insgesamt **2.934 Eingaben** von Bürgerinnen und Bürgern erreicht (2014: 1.364 und 2015: 1.570). Damit sind in den Jahren 2014 und 2015 insgesamt 789 Eingaben mehr eingegangen, als im Berichtszeitraum 2012/2013 (vgl. 24. TB, VII 1: 2.145 Eingaben). Im Verhältnis zu den 1.047 Eingaben des Jahres 2013 haben sich die Eingaben 2014 um 30 Prozent und 2015 sogar um 50 Prozent erhöht.

Mit 448 Eingaben (15%) machen die Eingaben auf Grundlage des EuGH-Urteils zum sogenannten „Recht auf Vergessenwerden" (siehe hierzu V 1.1) dabei einen großen Teil im Berichtszeitraum aus. Dieser Anlass ist neu (am 14.07.2014 haben uns die ersten Eingaben dazu erreicht), es handelt sich dabei aber nicht, wie es beispielsweise bei den Eingaben zu Google Street View im Jahr 2010 der Fall war (vgl. 23. TB, IV 3.4), um ein einmaliges Phänomen, sondern um eine dauerhafte Aufgabe der Hamburgischen Datenschutzaufsicht. Hinzu kommt, dass die Eingaben zu Google Street View einfach dadurch gelöst werden konnten, dass sie an die verantwortliche Stelle weitergeleitet wurden. Auch das ist bei den Eingaben zum „Recht auf Vergessenwerden" anders, denn hier muss jeder Einzelfall geprüft und rechtlich beurteilt werden, was erhebliche Ressourcen bindet.

Auch deshalb, aber nicht ausschließlich aufgrund der Eingaben zum „Recht auf Vergessenwerden“, sind bei uns im Berichtszeitraum 2014/2015 die bisher meisten datenschutzrechtlichen Beschwerden innerhalb eines 2-Jahres-Zyklus eingegangen. Dabei ist das Jahr 2015 besonders herausragend, denn wenn man die 416 Beschwerden, die uns 2010 zu Google Street View erreicht haben, als einmaliges und weitgehend durch automatisierte Löschung zu lösendes Problem herausrechnet, haben uns 2015 die mit Abstand meisten Eingaben von Bürgerinnen und Bürgern erreicht, seit es die Institution des Hamburgischen Datenschutzbeauftragten gibt bzw. seit die Eingaben statistisch erfasst werden.



Das Verhältnis der datenschutzrechtlichen Beschwerden über nicht-öffentliche Stellen (also beispielsweise private Firmen und Unternehmen) zu den Beschwerden über öffentliche Stelle (Behörden) beträgt im Berichtszeitraum etwa 6:1. Das bestätigt den Trend der vergangenen Jahre, wobei wohl nicht mehr nur von einem Trend die Rede sein kann. Es ist (digitale) Realität, dass die „Datenkraken“, trotz NSA und Snowden, nicht in erster Linie in den Amtsstuben sitzen. Wenig überraschend ist dabei auch, dass sich weit mehr als ein Drittel (39%) aller im Berichtszeitraum eingegangen Eingaben gegen Unternehmen im Bereich der Medien, Telemedien und der Telekommunikation, zu denen die Internetriesen Facebook und Google gehören, richteten.

Eingaben 2014/2015 nach Themen*	2014	2015
Bauen und Wohnen	39	48
Finanzwesen und Versicherungen	173	139
Gesundheitswesen	48	82
Inneres	41	57
Justiz (einschl. Strafvollzug)	13	15
Medien, Telemedien und Telekommunikation	**486**	**664**
Meinungsforschung, Statistik	10	14
Schulen und Hochschule	26	36
Soziales	53	75
Transport und Verkehr	26	17
Wirtschaft	205	192
* nur bei mehr als 9 Eingaben im jeweiligen Themenbereich		

Da die bundesweite Zuständigkeit für Google und Facebook beim Hamburgischen Datenschutzbeauftragten liegt, wird sich diese Entwicklung der Eingabenzahlen in Zukunft voraussichtlich fortsetzen oder sogar noch verstärken.

2. Bußgeldfälle und Anordnungen

Das Verhängen von Bußgeldern ist nach wie vor nicht überflüssig geworden.

Im Vordergrund unserer aufsichtsbehördlichen Tätigkeit steht zwar nicht, Bußgelder zu verhängen. Dennoch musste die Aufsichtsbehörde auch in diesem Berichtszeitraum 14 Verfahren einleiten, um Datenschutzverstöße mit Bußgeldern zu ahnden:

Tatbestand § 43 Abs. 1 Nr.	Tatbestand § 43 Abs. 2 Nr.	Sachverhalt	Bußgeld in €	E = Einspruch N = Kein Einspruch	Verfahrens-ausgang vor dem Amtsgericht
10			1.800	N	gezahlt
	1	unbefugte Übermittlung personenbezogener Daten auf der Internetseite des Unternehmens wg. mangelnder technischer/ organisatorischer Maßnahmen	1.500	N	§ 59 Landeshaushaltsordnung (LHO) niedergeschlagen wg. Uneinbringlichkeit
	1	unbefugte Übermittlung (Bonitätsanfrage)	2.000	N	gezahlt
	1	unbefugte Übermittlung personenbezogener Daten auf der Internetseite des Unternehmens wg. mangelnder technisch-organisatorischer Maßnahmen	1.800	E	Verfahren eingestellt nach § 47 Abs. 2 OwiG mit Zustimmung der Staatsanwaltschaft
	1 und 2	personenbezogene Daten unbefugt gespeichert und zum Abruf bereit gehalten trotz vorliegendem schutzwürdigen Interesse des Betroffenen	5.000	E	Reduzierung auf € 3.500 durch Verwaltungsbehörde; gezahlt
10			1.000	N	gezahlt
10			1.500	N	gezahlt
10			1.000	N	Vollstreckung
	3	unbefugter Abruf von Kontodaten aus dem Verwandtenkreis der abrufenden Person	200	N	gezahlt
4a			1.900	N	gezahlt
	7	Mitteilungspflicht gem. § 42a BDSG nicht sowie nicht vollständig erfüllt	350	N	gezahlt
	5b	Versand von Werbemails trotz Widerspruch	500	N	gezahlt
10			1.000	N	Vollstreckung
3	5b	Versand von Werbung trotz Widerspruch + fehlender Hinweis nach § 28 Abs. 4 BDSG	2.000	N	gezahlt

Interessant dabei ist, dass Rechtsmittel nur in zwei Verfahren eingelegt wurden, die restlichen Bescheide wurden akzeptiert. In nur einem Fall konnte das Bußgeld bisher nicht eingetrieben werden, zwei Verfahren befinden sich noch in der Vollstreckung. Dadurch wird deutlich, dass die Einleitung der Bußgeldverfahren gerechtfertigt war. Allerdings ist auch festzustellen, dass Personalengpässe die Verfolgung von Bußgeldtatbeständen einschränken. Dies gilt insbesondere für Verfahren mit komplexen Sachverhalten und schwieriger rechtlicher Würdigung.

Im Berichtszeitraum wurden keine Strafanträge gestellt.

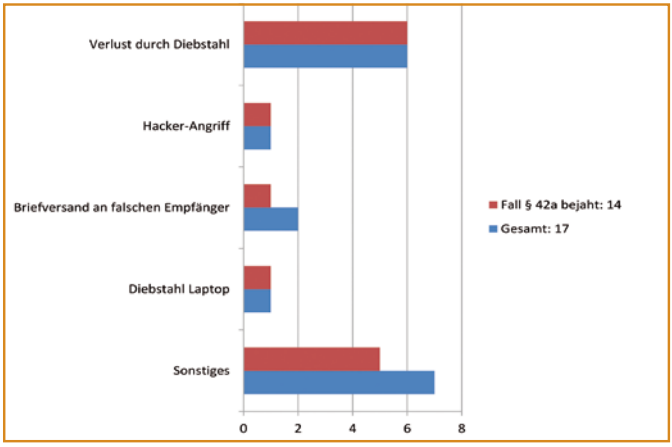
Die Aufsichtsbehörde hat gegenüber drei Unternehmen Anordnungen nach § 38 Abs. 5 BDSG erlassen. Ein Fall betraf Kundendaten, die im Internet öffentlich zugänglich waren, bedingt durch unzureichende technische und organisatorische Maßnahmen nach § 9 BDSG. Jeweils eine Anordnung wurde gegenüber Google (vgl. V 1.2) und Facebook (vgl. V 2.2) erlassen.

3. Meldepflicht nach § 42a BDSG

Die Zahl der angezeigten Datenpannen hat sich verringert.

Im Berichtszeitraum erreichten uns wieder zahlreiche Meldungen über Datenschutzvorfälle. Allerdings sind wesentlich weniger Datenpannen angezeigt worden als im letzten Berichtszeitraum (vgl. 24. TB, IV 12.2).

Die nachstehende Übersicht stellt die wichtigsten Sachverhalte der 17 eingegangenen Meldungen dar:



4. 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.

57 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 IV 11.1; 23. TB, IV 12.2; 24. TB, VI 12.3). Unterteilt nach der Art der meldepflichtigen Verfahren ergibt sich folgendes Bild:

Speicherung zum Zwecke der Übermittlung	
Auskunfteien/Warndienste	10
Informationsdienste	5
Adresshändler	15
Speicherung zum Zwecke der anonymisierten Übermittlung oder für Zwecke der Markt- und Meinungsforschung	27

5. Presse- und Öffentlichkeitsarbeit

Die Pressearbeit beim HmbBfDI ist im Vergleich zum letzten Berichtszeitraum nochmal deutlich angestiegen. Die Presseanfragen aus dem In- und Ausland folgen dabei nicht nur sensationellen Neuerungen oder Ereignissen, sondern es ist ein mediales Grundinteresse an datenschutzrechtlichen Themen erkennbar.

Das mediale Interesse an datenschutzrechtlichen Themen reißt nicht ab und ist weiterhin ein Indikator für den immer höheren Stellenwert des Datenschutzes in der digitalisierten Gesellschaft. Denn obwohl nach wie vor besondere Ereignisse – beispielsweise der Erlass eines Verwaltungsakts gegen einen globalen Internetdienst oder ein bahnbrechendes Urteil des Europäischen Gerichtshofs – eine Welle von Presseanfragen auslösen, gibt es auch eine Vielzahl von Anfragen, die sich mit vielleicht eher alltäglichen Themen beschäftigen. GPS-Tracking bei Versicherungen, Smart-TV, Körperscanner an Flughäfen, Videoüberwachung im Parkhaus oder der Umgang mit Patientendaten sind nur einige Bespiele für die Themen, nach denen bei uns recherchiert wurde oder zu denen wir um ein Statement oder ein Interview gebeten wurden. Gerade auch durch diese Anfragen bleibt die Anzahl der Presseanfragen Monat für Monat auf einem weitgehend gleichbleibend hohen Niveau, der Datenschutz kennt kein Sommerloch.

Im Berichtszeitraum haben uns insgesamt 626 Presseanfragen erreicht, also fast 80 mehr als in den Jahren 2012 und 2013 (549). Von diesen 626 Anfragen konnten 98% abschließend von uns bearbeitet werden, nur bei 13 Anfragen mussten wir aufgrund fehlender Kapazitäten oder Unzuständigkeit absagen oder auf andere Stellen verweisen. Im Durchschnitt wurden also rund 26 Anfragen pro Monat von uns bearbeitet.

Abb. 1: **Presseanfragen 2014** pro Monat mit Kennzeichnung „besonderer Ereignisse"

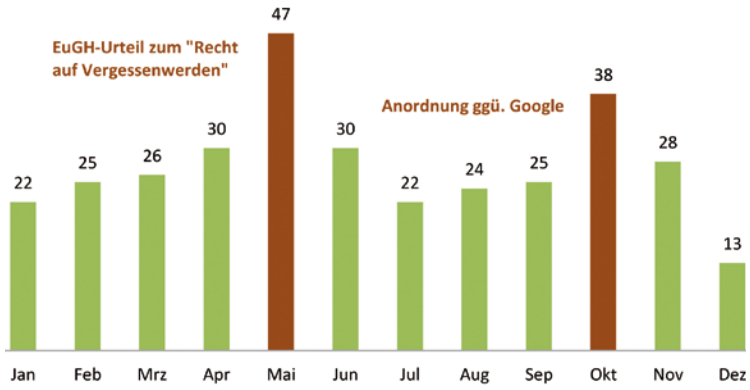
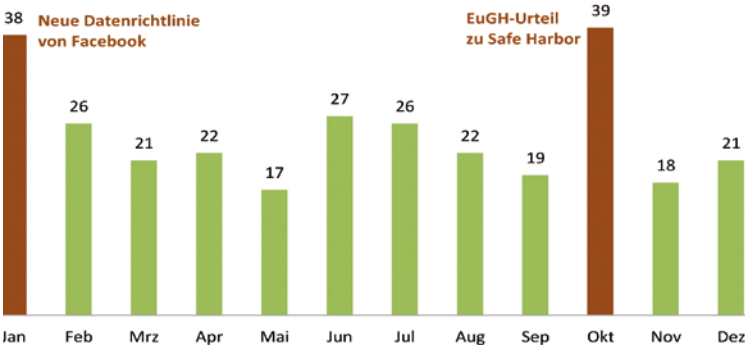


Abb. 2: **Presseanfragen 2015** pro Monat mit Kennzeichnung „besonderer Ereignisse“



Wie aus den vorstehenden Grafiken deutlich wird, liegt die hohe Zahl der Presseanfragen im Berichtszeitraum insbesondere an dem mit 330 Anfragen herausragenden Jahr 2014. Ein Drittel der gesamten Anfragen dieses Jahres (110) bezogen sich dabei allein auf Google, sei es wegen der bereits genannten Ereignisse oder sei es in anderen Zusammenhängen (zum Beispiel Nest Labs, Google Glass oder Street View). Diese auf Google bezogenen Anfragen sind dann aber im Jahr 2015 mit nur 39 stark zurückgegangen. Die Anfragen zu Facebook liegen mit insgesamt 97 auch deutlich unter den 127 Anfragen im Berichtszeitraum 2012/2013. Die Presseanfragen zu diesen beiden Internetgrößen sind insgesamt im Berichtszeitraum etwas zurückgegangen, machen aber noch 39% der Gesamtanfragen aus (41% in den Jahren 2012/2013).

Interessanterweise hatte dieser Umstand aber keinen Einfluss auf die Anzahl der Presseanfragen, die uns von ausländischen Medien erreicht haben, wie die folgende Tabelle verdeutlicht:

Presseanfragen…	2014 (2012)	2015 (2013)	Gesamt (2012/2013)
regionaler Medien	111 (88)	73 (80)	184 (168)
überregionaler Medien	169 (191)	164 (131)	333 (322)
ausländischer Medien	50 (24)	59 (35)	109 (59)
Gesamt:	330 (303)	296 (246)	626 (549)

Tabelle 1: Presseanfragen beim HmbBfDI 2014/2015, Klammerzusätze: Presseanfragen 2012/ 2013 zum Vergleich

Das stark gestiegene Interesse ausländischer Medien ist vermutlich – zumindest teilweise – auf den Europäischen Gerichtshof zurückzuführen, der im Berichtszeitraum mit mehreren Entscheidungen zu einem gestiegenen Interesse der europäischen aber auch der außereuropäischen Presse an datenschutzrechtlichen Themen beigetragen hat.

Mit der Organisation und Durchführung der 87. und der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) im Frühjahr und Herbst 2014, mit denen wir turnusgemäß an der Reihe waren, sind wir dann auch an die Grenzen unserer diesbezüglichen Leistungsfähigkeit gekommen. Nur aufgrund einer gemeinsamen Kraftanstrengung der gesamten Dienststelle sind diese beiden Veranstaltungen, wie auch die Organisation der zentralen Veranstaltung der DSK zum Europäischen Datenschutztag 2015, die traditionell auf den Vorsitz der DSK folgt, dennoch mit großem Erfolg durchgeführt worden.

Neben den Tätigkeitsberichten des vergangenen Berichtszeitraums und des Flyers „Europa: Sicher Hafen des Datenschutzes" anlässlich der Veranstaltung zum 9. Europäischen Datenschutztag gab es in den Jahren 2014 und 2015 keine weiteren Veröffentlichungen im Printbereich. Veröffentlichungen, insbesondere von allgemeinen Informationen oder Orientierungshilfen, wurden ausschließlich im Internet vorgenommen. Daneben haben wir im Berichtszeitraum 25 Pressemitteilungen veröffentlicht und, insbesondere aufgrund unseres Vorsitzes der DSK, 4 Pressekonferenzen durchgeführt.

Neben der schon traditionellen Teilnahme an der Dataport-Hausmesse haben wir an einer Veranstaltung zum Safer Internet Day der Bücherhallen Hamburg teilgenommen. Außerdem haben der Hamburgische Datenschutzbeauftragte und ein Teil seiner Mitarbeiter und Mitarbeiterinnen auch in den vergangenen 2 Jahren eine Vielzahl von Vorträgen zu datenschutzrechtlichen Themen bei diversen Veranstaltungen gehalten und an Diskussionsrunden teilgenommen.

6. Aufgabenverteilung (Stand: 1. Januar 2016)

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:	Ulrich Kühn	-4054
Vorzimmer:	Heidi Niemann	-4040

Verwaltungsleiter, Presse- und Medienreferent
Arne Gerhards -4153

Haushalt und Personalwesen
Rolf Nentwig -4043

IT-Leitung, Internetangebot des HmbBfDI, Öffentlichkeitsarbeit
Martin Schemm -4044

Vorzimmer, Geschäftsstelle
Heidi Niemann -4040

Registratur, Geschäftsstelle
Katharina Schmidt -4042

Übergreifende Infrastrukturprojekte, Hamburg Gateway, technisch-organisatorische Beratung und Prüfung
Dr. Sebastian Wirth -4053

Technisch-organisatorische Beratung und Prüfung
Jutta Nadler -4055

Netzwerke und mobile Geräte, technisch-organisatorische Beratung und Prüfung
Thomas Morische -4048

Technisch-organisatorische Beratung und Prüfung
Frank Grebe -4142

Informationsfreiheit/Transparenz, Videoüberwachung, Auskunftsanspruch nach Presserecht
Dr. Christoph Schnabel -4047

Informationsfreiheit/Transparenz, Videoüberwachung
Cornelia Goecke -4141

Grundsatzfragen des HmbDSG, Gesundheitswesen und medizinische Forschung, Schule und Bildungswesen, Sozialwesen, Pass- und Ausweisangelegenheiten, Personenstands- und Archivwesen
Matthias Jaster -4062

Verkehr, Wirtschaftsverwaltung, Bezirks- und Parlamentsangelegenheiten, Wahlen und Volksabstimmungen, Hochschul- und Bibliothekswesen, behördliche Datenschutzbeauftragte, Landwirtschaft
Eva-Verena Scheffler -4064

Sicherheit und Justiz, Waffenrecht, private Sicherheitsdienste und Detekteien, Rechtsanwälte und Notare, Ausländerwesen, Friedhöfe
Okşan Karakuş -4049

Statistik, Bearbeitung von abgelehnten Anträgen auf Löschung aus den Ergebnissen der Google-Suchmaschine
Uta Kranold -4046

Grundsatzfragen des BDSG, Grundsatzfragen Internationales, Auskunfteien
Helga Naujok -4058

Beschäftigtendatenschutz, Bauen und Wohnen, Vereine und Gewerkschaften
Evelyn Seiffert -4060

Finanz-, Steuer- und Rechnungswesen, Handel und Industrie, Steuerberater und Wirtschaftsprüfer, Geodaten
Heike Wolters -4052

Versicherungen, Kreditwirtschaft, Versand- und Onlinehandel, Werbung- und Adresshandel, Markt- und Meinungsforschung
Dr. Jens Ambrock -4059

Gewerbliche Dienstleistungen, Bearbeitung von abgelehnten Anträgen auf Löschung aus den Ergebnissen der Google-Suchmaschine, juristische Sachbearbeitung bei Medien und Telemedien
Herr Schröder -4144

Technische Grundsatzfragen bei Medien, Telemedien, Telekommunikation und E-Government, Netzwerke, Biometrie, technisch-organisatorische Beratung und Prüfung bei Informationsfreiheit und Kultur
Ulrich Kühn -4054

Juristische Grundsatzfragen der Medien, Telemedien, Telekommunikation und E-Government, elektronischer Rechtsverkehr, Kultur
Dr. Moritz Karg -4051

Beratung und Prüfung bei Medien, Telemedien, Telekommunikation, E-Government, soziale Netzwerke und Bewertungsportale, technisch-organisatorische Beratung und Prüfung bei Videoüberwachung
Herr Schneider -4061

Zahlen - Fakten - Defizite - Lösungen

Die Informationsschrift „Zahlen-Fakten-Defizite-Lösungen" wurde dem Ausschuss für Justiz und Datenschutz der Hamburgischen Bürgerschaft im Rahmen einer Expertenanhörung zur Stärkung der Unabhängigkeit des Datenschutzbeauftragten am 1. Dezember 2015 vorgelegt. Die hier abgedruckte Fassung ist leicht gekürzt und aktualisiert.

Bericht zur Ausstattungssituation beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit

1. Einleitung

Die Analyse der Ausstattung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) ist gerade im Zusammenhang mit der gegenwärtigen Diskussion um eine rechtliche Stärkung der Unabhängigkeit dieses Amtes von großer Bedeutung. Die Selbstständigkeit, mit der das Amt des Datenschutzbeauftragten wahrgenommen werden kann, hängt nicht nur von den rechtlichen Vorgaben ab, die die Unabhängigkeit des Datenschutzbeauftragten vor äußerer Einflussnahme schützen. Daneben gibt es eine materielle Dimension der Unabhängigkeit, die in § 22 Absatz 2 Satz 1 Hamburgisches Datenschutzgesetz (HmbDSG) gesetzlich festgeschrieben ist. Danach ist dem HmbBfDI die zur Aufgabenerfüllung notwendige Personal- und Sachausstattung zur Verfügung zu stellen. Diese Vorschrift trägt der Tatsache Rechnung, dass ohne eine angemessene Ausstattung eine freie Entscheidung über die Art und Weise der Aufgabenerfüllung der Datenschutzbehörde zum Schutz der Grundrechte von Bürgerinnen und Bürgern nicht möglich ist. Fachliche Zwänge im Personal- und Verwaltungshaushalt können dazu führen, dass die Unabhängigkeit bei der Wahrnehmung des Amtes nicht mehr besteht. Dies ist insbesondere dann der Fall, wenn die Durchführung insbesondere anlassfreier Prüfungen und Kontrollen durch mangelnde Ressourcen massiv eingeschränkt wird.

Insoweit gilt es im Folgenden, die Ausstattungssituation des HmbBfDI kritisch zu analysieren. Hierbei werden sowohl qualitative als auch quantitative Aspekte in den Blick genommen. Veranschaulicht wird der folgende Bericht durch konkrete Fallbeispiele aus Sicht der zuständigen Referate der Behörde. Sie zeigen, wie langwierig und komplex die durch die Dienststelle zu bearbeitenden Verfahren sind.

2. Das Personal

Die Dienststelle des HmbBfDI wurde zum Januar 2014 neu organisiert und besteht

seitdem aus 6 Referaten. Die vorherige Gliederung in „Verwaltung", „Technik", „Öffentlich" und „Nicht-Öffentlich" wurde zugunsten einer realitätsnäheren und effektiveren Organisation aufgegeben. Viele datenschutzrechtliche Fragestellungen stellen sich sowohl im öffentlichen als auch im nicht-öffentlichen Bereich, sodass eine organisatorische Zusammenfassung Synergien schafft. Beispielhaft seinen hier die Videoüberwachung oder staatliche und private Krankenhäuser genannt.

Diese 6 Referate sind momentan (Stand 31.Dezember 2015) mit 22 Mitarbeiterinnen und Mitarbeitern besetzt, die sich auf 18,4 Vollzeitäquivalente (VZÄ) verteilen. Von diesen 18,4 VZÄ sind aber nur 15,4 VZÄ tatsächliche Planstellen beim HmbBfDI, also im Stellenplan aufgeführt und in den Personalkosten berücksichtigt. Im Zuge der Planaufstellung des Doppelhaushalts 2013/2014 wurde dem HmbBfDI auferlegt, jährlich eine Summe von 15.000,- Euro einzusparen. Diese Sparquote wurde dadurch erreicht, dass 0,3 VZÄ aus dem bisherigen Stellenbestand gestrichen wurden. Da aber in diesem Zuge keine 0,3 Mitarbeiter eingespart werden konnten, sind die tatsächlichen Personalkosten gleich geblieben, sodass der HmbBfDI diese 15.000,- Euro jährlich aus anderen Quellen (Einnahmen, Reste) aufbringen muss.

1,2 VZÄ (2 Beschäftigte) sind von anderen Dienststellen gegen Personalkostenerstattung zum HmbBfDI abgeordnet. Dafür muss der HmbBfDI jährlich 70% der Kosten einer A12-Stelle und 7,5% der Kosten einer A14-Stelle erstatten (zusammen rund 58.290,- Euro nach Personalkostenverrechnungssatz 2016 - PKV), was in den vergangenen Jahren aus übertragenen Resten möglich war. Darüber hinaus hat der HmbBfDI seit Januar 2015 1,5 auf zunächst 1 Jahr befristete Stellen mit der Wertigkeit E13 TV-L besetzt, von denen eine (1 VZÄ) nun um ein Jahr verlängert werden soll. Diese Stellen werden ebenfalls aus übertragenen Resten finanziert (99.969 Euro für 2015, 71.769 Euro für 2016 nach den PKV 2015 und 2016).

Bei unveränderter Einnahmensituation und bei Übertragung der prognostizierten Reste sind die Deckung der Personalkosten der befristeten Arbeitsverhältnisse noch für das Haushaltsjahr 2016 und die Deckung der Personalkostenerstattungen noch bis einschließlich 2017 gegeben. Danach müsste sich der HmbBfDI von diesen Mitarbeitern trennen bzw. müsste die Abordnungen beenden, da eine Finanzierung nicht mehr möglich sein wird. Die Mitarbeiter sind jedoch mit Aufgaben betraut, die mit großer Gewissheit über das Jahr 2016 hinaus bestehen bleiben, wie etwa die Videoüberwachung oder die Bearbeitung von Eingaben im Zusammenhang mit Löschanträgen bei der Google-Suche.

Von den 22 Mitarbeiterinnen und Mitarbeitern sind 5 (4,75 VZÄ) im „Verwaltungsreferat" beschäftigt (siehe 4.1), sodass für die tatsächliche datenschutz- und informationsfreiheitsrechtliche Aufsicht und Beratung nur 17 Mitarbeiter und Mitarbeiterinnen (13,65 VZÄ) zu Verfügung stehen.

3. Die Zuständigkeiten

Diese 17 Mitarbeiterinnen und Mitarbeiter sind hinsichtlich datenschutzrechtlicher Fragen für die gesamte Wirtschaft und für die gesamte Infrastruktur der Freien und Hansestadt Hamburg zuständig. Sie bilden unter anderem die datenschutz- und informationsfreiheitsrechtliche Aufsichtsbehörde für alle Hamburger Fachbehörden, für die Bezirksämter, die Finanzämter, die Schulen, die Universitäten sowie für die Körperschaften, insb. die Kammern der freien Berufe, Anstalten und Stiftungen der FHH. Sie sind für alle Landesbetriebe, für die gesamte Polizei, für die Feuerwehr, die Gerichte, die Staatsanwaltschaft und für das Landesamt für Verfassungsschutz zuständig. Sie sind die datenschutzrechtliche Aufsichtsbehörde für etwa 150.000 Hamburger Unternehmen und rund 15.000 Handwerksbetriebe (vgl. Internetauftritte der Handels- und der Handwerkskammer Hamburg).

Aus diesen Unternehmen stechen die globalen Internetfirmen Google und Facebook hinsichtlich des Arbeitsaufwands wie auch der Außenwirkung hervor. Dabei sollte aber nicht aus den Augen verloren werden, dass Hamburg eine Medienstadt ist und dass noch über 9.000 (Quelle: „Digitaler Aufbruch", Welt am Sonntag (Hamburg) vom 2. Februar 2014, Ausgabe 5, Seite 1) weitere Internetfirmen hier ihren Sitz haben, darunter weitere „Schwergewichte" wie Xing oder Parship. Datenschutz findet aber auch nicht nur im Internet statt. Die Mitarbeiterinnen und Mitarbeiter des HmbBfDI beaufsichtigen außerdem die in Hamburg niedergelassenen Ärzte und Zahnärzte, die Krankenhäuser und Apotheken, Banken, Versicherungen, Restaurants, Hotels, Gaststätten, Einkaufszentren etc..

Dabei bedeutet Datenschutzaufsicht aber nicht, dass der HmbBfDI nur solche Unternehmen und Behörden im Visier haben muss, die im Rahmen ihrer Aufgaben oder ihres Geschäftsmodells Bürger-, Kunden- oder Patientendaten verarbeiten. Auch Behörden und Unternehmen, die die Daten ihrer Mitarbeiterinnen und Mitarbeiter verarbeiten oder durch Dritte verarbeiten lassen, müssen dabei die Datenschutzgesetze beachten. Es dürfte daher kaum ein in Hamburg ansässiges Unternehmen und eine Hamburgische Behörde geben, mit denen die 17 Mitarbeiterinnen und Mitarbeiter des HmbBfDI keine dienstlichen Berührungspunkte haben.

Nicht zuletzt deshalb sind im Jahr 2014 insgesamt 1.364 datenschutzrechtliche Eingaben von Bürgerinnen und Bürgern beim HmbBfDI eingegangen. Umgelegt auf die damals vorhandenen 16,9 VZÄ des HmbBfDI (einschl. Verwaltungsreferat aber ohne die befristeten 1,5 VZÄ, die erst 2015 eingerichtet wurden) wurden also im vergangenen Jahr etwa 80 Eingaben pro VZÄ bearbeitet. Zum Vergleich: Im Jahr 2014 sind beim Berliner Beauftragten für Datenschutz und Informationsfreiheit (BInBDI) ca. 1.200 datenschutzrechtliche Eingaben eingegangen. Bei einem Stellenbestand von 38 VZÄ (nach Auskunft des BInBDI im Rahmen einer Presseauskunft am 18. August 2015, hier ohne die Stelle des Datenschutzbeauftragten selber) bedeutet das, dass dort rund 32

Eingaben pro VZÄ bearbeitet wurden.

Beim HmbBfDI wurden 2014 also deutlich mehr als doppelt so viele Eingaben pro VZÄ bearbeitet, als es beim Berliner Datenschutzbeauftragten der Fall war.

Im Jahr 2015 haben den HmbBfDI 1.570 datenschutzrechtliche Eingaben von Bürgerinnen und Bürgern erreicht. Dadurch erhöht sich die Quote auf 85 Eingaben pro VZÄ, obwohl der HmbBfDI in diesem Jahr 1,5 VZÄ zusätzlich zur Verfügung hat und die Eingaben nach dem Hamburgischen Transparenzgesetz nicht einmal einberechnet sind.

4. Die Referate

4.1 Referat D1: Interner Service, Presse- und Öffentlichkeitsarbeit

Das Referat D1 ist das Verwaltungsreferat beim HmbBfDI, wobei diese Bezeichnung die Aufgaben des Referats nur unzureichend beschreibt. Ein Großteil der tatsächlichen internen Verwaltungstätigkeit, wie z.B. Haushaltsplanführung, Berichterstattung, Personalbearbeitung und Betreuung des Stellenplans wird von Mitarbeiterinnen und Mitarbeitern der Justizbehörde (JB) durchgeführt. Das Referat D1 ist dabei das Bindeglied zu diesen Stellen der JB. Sämtliche personalrechtlichen Planungen, Entscheidungen und Anträge laufen über das Referat D1, Stellenbeschreibungen werden ebenso von D1 erstellt wie Stellenausschreibungen. Bewerbungsverfahren werden vom Referat D1 organisiert und durchgeführt. Das Referat D1 ist für die Budget- und Stellenplanung des HmbBfDI sowie deren Verwaltung zuständig, prüft die Berichte der JB und ermittelt und kommentiert im Bedarfsfall die Kennzahlen. Die kleinen alltäglichen Erledigungen, wie Vorzimmertätigkeit, Post, Verwaltung der Eingaben und Registratur, Miet- und Gebäudeangelegenheiten, Beschaffung von Büromaterial, Technik sowie die Durchführung von Veranstaltungen des HmbBfDI obliegen dem Referat D1. D1 ist außerdem auch die Pressestelle des Datenschutzbeauftragten, koordiniert und beantwortet die über 300 Presse- und Interviewanfragen, die den HmbBfDI pro Jahr aus dem In- und Ausland erreichen. Dazu erstellt D1 die Pressemitteilungen und organisiert die Pressekonferenz, die regelmäßig anlässlich der Veröffentlichung des Tätigkeitsberichts Datenschutz durchgeführt wird.

Die Gestaltung sowie die Pflege des Internetauftritts des HmbBfDI, der nicht im Rahmen von hamburg.de gelauncht ist, obliegen dem Referat D1 ebenso wie die Entwicklung, Gestaltung und Verteilung der Druckerzeugnisse des HmbBfDI (Tätigkeitsberichte, Broschüren, Flyer). Die Antwortbeiträge zu parlamentarischen Anfragen werden von D1 erstellt oder ihre Erstellung wird, ebenso wie die Beiträge zu Drucksachenabstimmungen, vom Referat D1 überwacht und koordiniert.

Dadurch, dass die Landesdatenschutzbeauftragten Deutschlands den HmbBfDI zu Ihrem Vertreter auf europäischer Ebene – in der sogenannten Art. 29-Gruppe – bestimmt haben, sind dem Referat D1 zudem umfangreiche und anspruchsvolle Aufgaben im

Rahmen der Koordinierung und Abstimmung datenschutzrechtlicher Fragen und Aufgabenstellungen zwischen der nationalen und der europäischer Ebene zugefallen. Insbesondere sind die turnusgemäßen Sitzungen in Brüssel vorzubereiten und anschließend auszuwerten.

Zusätzlich obliegt D1 die Organisation der Referendariate beim HmbBfDI sowie die weitere Aus- und Fortbildung. Das Referat D1 stellt darüber hinaus den Beauftragten für Arbeitssicherheit, zwei Ersthelfer sowie den stellvertretenden Geheimschutzbeauftragten.

Das Referat D1 besteht momentan aus 5 Personen (4,75 VZÄ), was bei gleichbleibenden Aufgaben auskömmlich ist.

Bei einer Stärkung der Unabhängigkeit des HmbBfDI werden absehbar mehr Aufgaben auf das Referat D1 zukommen. Selbst wenn, wie es gegenwärtig geplant ist, das Personalamt die Aufgaben im Bereich der Personalverwaltung übernimmt, die bisher von der JB wahrgenommen werden, sind die großen Bereiche Haushalt und Organisation, die zur Herstellung der Unabhängig in den Händen des HmbBfDI bleiben müssen, eigenständig zu bearbeiten. Planaufstellung, -bewirtschaftung, Stellenplan, Haushalts-, VZÄ- und Kennzahlenberichte sind die zzt. absehbaren Hauptherausforderungen, die an die interne Verwaltung des HmbBfDI gestellt werden.

Nach hiesiger Einschätzung muss das Referat D1 mit 1,5 zusätzlichen VZÄ ausgestattet werden, um diese neuen Aufgaben bewältigen zu können, ohne dass die bisherigen Aufgabengebiete maßgeblich vernachlässigt werden. Eine volle Stelle wäre dann für die Haushaltssachbearbeitung und die stellvertretende Referatsleitung vorgesehen, die weitere halbe Stelle wäre insbesondere für Organisationsaufgaben zuständig und wäre Stellvertreter/-in des/der Haushaltssachbearbeiter/in.

4.2 Referat D2: Technik

Das Technikreferat ist für die technischen Fragen des Datenschutzes, also insbesondere für die Prüfung und Begleitung von IT-Verfahren zuständig. Im öffentlichen Bereich ist dabei ausdrücklich geregelt, dass der HmbBfDI zu den Auswirkungen der Nutzung neuer Informations- und Kommunikationstechniken in Bezug auf den Datenschutz Stellung nehmen sowie Behörden, Unternehmen und weitere Stellen in diesen Fragen beraten soll. Diese Aufgaben obliegen in erster Linie dem Referat D2.

Derzeit verfügt das Referat D2 über 3 Mitarbeiter und eine Mitarbeiterin bei 2,4 VZÄ. Von diesen VZÄ fallen ab 2017 0,5 weg, da es sich um die oben genannte befristete Stelle handelt, deren Befristung nicht verlängert wird (siehe 2.) Das Referat D2 stellt als Zusatzaufgaben die behördliche Datenschutzbeauftragte, einen der IT-Beauftragten des HmbBfDI und den IT-Sicherheitsbeauftragten.

Die Aufgaben des Referats D2 sind in der Regel technisch komplex und oft auch durch länderübergreifende Abstimmungs-verfahren geprägt. Ein typisches Beispiel dafür ist das Verfahren zum „Zentralen Meldebestand“:

Im Juni 2014 wird der HmbBfDI darüber informiert, dass die Bundesländer Hamburg, Schleswig-Holstein und Sachsen-Anhalt beabsichtigen, die Anforderungen aus dem neuen Meldegesetz (speziell für Suchanfragen von bzw. Auskünften an die Polizei und anderen Sicherheitsbehörden, den Melde- und weitere Behörden sowie Bürgerinnen, Bürger und Unternehmen) auf der Basis einer sog. Spiegeldatenbank innerhalb einer gemeinsamen IT-Infrastruktur umzusetzen. In einer ersten Information werden das Zielbild der geplanten IT-Architektur, die Darstellung von Gemeinsamkeiten und Unterschieden der Länder sowie der Terminplan übermittelt.

Eine erhöhte Schwierigkeit in diesem Projekt ergab sich dadurch, dass die Rechtsgrundlagen noch nicht vollständig vorlagen, in denen technische Maßnahmen zum Schutz der sensiblen personenbezogenen Daten festgeschrieben werden sollten. Diese gesetzlichen Vorgaben galt es mit den juristischen Kollegen des Referats D4 abzustimmen und gegenüber dem Projekt zu verdeutlichen, durch welche technischen und organisatorischen Maßnahmen sie realisiert werden könnten. Zusätzlich war – neben den notwendigen Abstimmungen mit der datenverarbeitenden Stelle – der stetige Informations- und Meinungsaustausch unter den drei beteiligten Landesdatenschutzbeauftragten erforderlich, da das Ziel ist, bei länderübergreifenden Projekten zu einheitlichen datenschutzrechtlichen Anforderungen und zu einer einheitlichen Bewertung des Verfahrens zu kommen.

Ein weiterer zentraler Punkt bei länderübergreifenden Projekten ist es, bereits im Rahmen der Vorabkontrolle zu klären, durch welche technischen und organisatorischen Maßnahmen die strikte Trennung der Daten der beteiligten Länder gewährleistet wird. Die Anforderungen dafür haben die Datenschutzbeauftragten des Bundes und der Länder zwar in einer Orientierungshilfe beschrieben, bei den datenverarbeitenden Stellen liegen aber bisher noch zu wenige Erfahrungen damit vor, so dass es regelmäßig zu Abstimmungen und Nachfragen kommt. Trotz vorliegender Orientierungshilfe bedurfte es also auch beim Projekt Zentraler Meldebestand mehrerer Gesprächstermine, bis die datenschutzrechtlichen Anforderungen in die Realisierungskonzepte eingeflossen sind. Dabei waren die zugrundeliegenden Unterlagen, die vom Referat D2 studiert werden mussten, sehr umfangreich. Allein das wichtigste technische Dokument, das dem HmbBfDI als Gesprächsgrundlage vom Projekt vorab zur Verfügung gestellt wurde, umfasst mehr als 250 Seiten. Dazu wurden dem HmbBfDI weitere 140 Dateien mit einem Datenvolumen von über 35 MB Dokumente übermittelt, in denen die technischen Details beschrieben sind.

Nach erfolgreicher Vorabkontrolle und Produktivsetzung des Verfahrens werden in der Einführungsphase regelhaft weitere im Rahmen der vorlaufenden Tests und der Freiga-

be nicht erkannte Schwierigkeiten offenbar, die zu Rückfragen und Klärungsprozessen mit dem Projekt führen. Diese Aspekte werden sowohl von den datenverarbeitenden Stellen, von Mitarbeitern der Anwender oder auch von betroffenen Bürgerinnen und Bürgern an das Referat D2 herangetragen und müssen kurzfristig aufbereitet werden. Gerade bei komplexen Verfahren ist es erklärtes Ziel, das IT-Verfahren im Echtbetrieb einer technischen Prüfung zu unterziehen. Beim IT-Verfahren Zentraler Meldebestand ist verabredet, diese Prüfung gemeinsam mit den anderen beteiligten Datenschutzbeauftragten durchzuführen.

Bereits im Frühjahr 2013 wurde eine Defizitliste der Tätigkeiten erstellt, die bereits im (damaligen) Referat D2 aufgrund der zu geringen personellen Kapazitäten nicht oder nicht ausreichend wahrgenommen werden können. Diese Tätigkeiten sind bei der Umstrukturierung nicht ebenso aufgeteilt worden wie das Personal, sondern sind fast vollständig beim neuen Referat D2 verblieben.

So werden dem Referat D2 beispielsweise umfangreiche technische Unterlagen (Leistungsbeschreibungen bei Ausschreibung, Realisierungskonzepte usw.) zur Beratung und Beurteilung von Großprojekten, wie z.B. JUS-IT oder eJustiz, übersandt. Aufgrund des hohen Zeitdrucks, unter dem die Projekte stehen, ergeht regelmäßig die Bitte um kurzfristige Rückäußerung. Um dieser berechtigten Bitte nachzugehen und da die dafür zur Verfügung stehenden Kapazitäten gering sind, unterbleibt häufig die intensive Durchdringung der jeweiligen Materie. Insbesondere bei länderübergreifenden Verfahren wie z.B. „Zentraler Meldebestand", „Community Cloud Mail Service", „TKÜ-Zentrum Nord" wäre eine intensivere Abstimmung mit den Beteiligten erforderlich, um Datenschutzanforderungen rechtzeitig in den Projektablauf einbringen zu können. Um auch dem Anspruch des HmbBfDI gerecht zu werden, nicht nur Probleme aufzuzeigen und vorgelegte Konzepte aus datenschutzrechtlicher Sicht zu kritisieren, sondern vielmehr Wege aufzuzeigen, wie eine datenschutzfreundliche Lösung aussehen könnte, müssten die Mitarbeiterinnen und Mitarbeiter die Möglichkeit zur Entwicklung von projekt-spezifischen datenschutzfreundlichen Lösungsmöglichkeiten haben. Die Rolle des Gestalters würde jedoch deutlich mehr Kapazität erfordern als zur Verfügung steht. Eine kontinuierliche Nutzung und Weiterentwicklung des eigenen Datenschutz-IT-Labors zur Bewertung und Prüfung von IT-Lösungen (Hardware und Software) unterbleibt. In diesem Zusammenhang macht sich die mangelnde Möglichkeit zur technischen Fortbildung bemerkbar, die aufgrund der Arbeitsbelastung faktisch nicht besteht. Dabei wäre sie zur kenntnisreichen Beratung bzw. zur effektiven Aufsicht von IT-Projekten zwingend erforderlich. Monolithische Lösungen wie früher gibt es nicht mehr, heute sind alle Ebenen vernetzt. Anwendungen sind für alle Plattformen erreichbar, damit muss das Wissen zur Einschätzung der Wirkung von technischen Maßnahmen sehr breit angelegt sein. Aber auch eine rechtliche Fortbildung wäre, gerade vor dem Hintergrund neuer datenschutzrechtlicher Regelungen, auch für den technischen Bereich notwendig. Ohne Kenntnis der rechtlichen Grundlagen, Hintergründe und Zusammenhänge können fundierte Bewertungen nur schwer vorgenommen werden.

Die Aufgabe der Vorabkontrolle ist mit Bestellung der behördlichen Datenschutzbeauftragten (behDSB) weitgehend auf diese übertragen. Die behDSB sind aber fast ausschließlich rechtlich vorgebildet. Technischer Sachverstand ist regelhaft kaum vorhanden. Aus diesem Grund wenden sie sich mit Risikoanalysen, die von den Daten verarbeitenden Stellen bei der Vorabkontrolle zu erstellen sind, an das Referat D2 und bitten um Unterstützung und Stellungnahme zu den technischen Ausführungen. Da wir in solche Projekte dann nur punktuell und nicht kontinuierlich eingebunden sind, erhöht sich der Aufwand für die einzelne Beantwortung der an uns herangetragenen Fragestellungen. Abhilfe würde ggf. die Erstellung von Arbeitshilfen für datenverarbeitende Stellen und für behördliche Datenschutzbeauftragte schaffen, die bereits seit geraumer Zeit geplant ist. Nach der flächendeckenden Bestellung der behDSB hatte das Referat D2 das Ziel, die behDSB durch die Erarbeitung von Arbeitshilfen (Checklisten etc.), die die spezifischen Gegebenheiten der IT in der Hamburgischen Verwaltung berücksichtigen, zu unterstützen. Dafür sollten Arbeitsergebnisse, Stellungnahmen etc., die für Einzelfälle erstellt wurden, so aufbereitet werden, dass die verallgemeinerbare Information allen behDSB zur Verfügung gestellt werden könnte. Trotz mehrfacher Anläufe mussten wir dieses Vorhaben abbrechen, da die Zeit für die erforderliche Aufbereitung der Informationen fehlt. Dadurch unterbleibt die Informationsweitergabe an behDSB hinsichtlich technisch-organisatorischer Themen, obwohl gerade in diesem Bereich ein hoher Bedarf besteht. Dies gilt leider auch für unsere Mitwirkung bei der Erstellung von gemeinsamen Arbeitshilfen der Datenschutzbeauftragten des Bundes und der Länder. Der Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder hat bereits zahlreiche Orientierungshilfen erstellt und sich dabei auch auf einheitliche Bewertungsmaßstäbe verständigt. Auch wenn dabei arbeitsteilig vorgegangen wird, setzt dieser Ansatz voraus, dass auch wir uns an den Arbeitsgruppen beteiligen. Die Mitarbeit bei der Erstellung solcher Orientierungshilfen bindet aber so viele Kapazitäten, dass wir in den letzten Jahren immer signalisieren mussten, dass sich der HmbBfDI nicht einbringen kann.

Auch kommt es zu einer Vernachlässigung von Infrastrukturthemen, da die personelle Unterbesetzung im technischen Bereich ausschließlich zu einer anlassbezogenen Reaktion in Datenschutzfragen führt, die dann auch nur noch oberflächlich geklärt werden können. Grundsätzliche Infrastrukturthemen mit Auswirkungen für alle Bereiche werden wegen des damit verbundenen Aufwandes nicht in ausreichendem Maße angegangen. Gleiches gilt für anlassfreie Prüfungen im öffentlichen und nichtöffentlichen Bereich, die nur in einem sehr geringen Umfang bzw. im nicht-öffentlichen Bereich quasi gar nicht mehr stattfinden. Damit entfällt die präventive Wirkung solcher Prüfungen für andere Daten verarbeitende Stellen.

Die Aufgabenwahrnehmung ist nur durch die zusätzliche Bewilligung von 2 VZÄ gewährleistet.

4.3 Referat D3: Informationsfreiheit und Videoüberwachung

Das Referat D3 besteht aus 1,7 VZÄ. Der Referatsleiter ist gleichzeitig der Geheimschutzbeauftrage des HmbBfDI.

Das Referat übt die informationsfreiheitsrechtliche Aufsicht über alle Hamburgischen Behörden im Sinne des § 2 Abs. 3 Hamburgisches Transparenzgesetz aus. Dabei ist zu beobachten, dass das relativ neue Institut der Informationsfreiheit mehr und mehr ins Bewusstsein der Bürgerinnen und Bürger rückt. So ist die Zahl der Beschwerden beim Hamburgischen Datenschutzbeauftragten darüber, dass Behörden ihrer Auskunftspflicht nicht oder nicht ausreichend nachgekommen sind, in den vergangenen Jahren stetig gestiegen (haben uns z.B. im Jahre 2011 insgesamt 23 solcher Beschwerden erreicht, sind es in diesem Jahr bis Mitte November bereits knapp 80 Beschwerden und 37 Auskunftsersuchen an den HmbBfDI).

Zusätzlich ist das Referat D3 für die datenschutzrechtlichen Belange bei der Videoüberwachung zuständig, die man mittlerweile überall finden kann. Im Folgenden wird zur Veranschaulichung ein konkretes Verfahren beschrieben, das (leider) typisch ist. Die darin aufgezeigten Probleme der Sachverhaltsaufklärung zeigen sich so oder so ähnlich in nahezu jedem Verfahren zur Videoüberwachung im nicht-öffentlichen Bereich:

Am 9. April 2014 geht eine Anzeige/Anfrage wegen der Videoüberwachung in einem Restaurant beim HmbBfDI ein. Videoüberwachung in der Gastronomie ist einer unserer Tätigkeitsschwerpunkte aufgrund der Vielzahl von Beschwerden. Wir beantworten die Eingabe am 15. April 2014 kurz und verweisen auf die nun anstehende Sachverhaltsaufklärung, wobei wir bei Videoüberwachungen immer vor dem gleichen Problem stehen: Für eine fundierte rechtliche Beurteilung ist die Frage entscheidend, was die Kameras zeigen. Dies können wir ohne Zugriff auf das System nicht klären. Kündigen wir unseren Besuch vor Ort an, geben wir der datenverarbeitenden Stelle die Möglichkeit, die Verhältnisse schnell (im schlimmsten Fall sogar nur für die Zeit unseres Besuchs) gesetzeskonform zu machen. Die Verfolgung von Ordnungswidrigkeiten ist so praktisch nie möglich. Erscheinen wir hingegen ohne Ankündigung, so erhalten wir nahezu ausnahmslos die Antwort, dass die einzige Person mit Zugriffsberechtigung auf das System (in der Regel: Geschäftsführer) momentan nicht anwesend ist und auch nicht geholt werden kann. Den zeitlichen Aufwand ergebnisloser Anreisen können wir uns nicht leisten, weshalb wir praktisch immer auf Fragebögen zurückgreifen müssen, in denen die verantwortliche Stelle ihr Fehlverhalten selbst angeben müsste. Die Nichtbeantwortung unserer Fragen stellt eine Ordnungswidrigkeit dar, die Verhängung eines Bußgeldes ist jedoch zeitintensiv und führt vor allem nicht zur Beantwortung der offenen Fragen. Dadurch wird der datenschutzrechtswidrige Zustand nicht beseitigt. Wir geben daher in aller Regel mehrere Möglichkeiten, bevor wir ein Owi-Verfahren einleiten.

In diesem Fall verschickten wir unseren Fragebogen am 16. April 2014 an den Betreiber des Restaurants. Es erfolgt keine Reaktion. Am 19. Mai 2014 versendeten wir den Fragebogen erneut. Es erfolgt wieder keine Reaktion. Daraufhin leiteten wir ein Owi-Verfahren wegen unterbliebener Auskunft ein und verschickten am 23. Juni 2014 ein Anhörungsschreiben wegen des Vorwurfs einer Ordnungswidrigkeit. Die Zustellung des Anhörungsschreibens scheiterte. Auf telefonische Nachfrage erfuhren wir am 8. Juli 2014 von einem Betreiberwechsel.

Am 8. Juli 2014 versendeten wir den ursprünglichen Fragebogen an die neue Inhaberin. Es erfolgte keine Reaktion. Am 7. August 2014 versendeten wir den Fragebogen erneut. Es erfolgte wieder keine Reaktion. Am 1. September 2014 leiteten wir ein erneutes Owi-Verfahren ein und verschickten dazu das Anhörungsschreiben. Gleichzeitig unterrichteten wir den Petenten davon, dass wir nach fünf Monaten noch nichts erreicht hatten. Am 22. September 2014 konnte die Beschuldigte telefonisch erreicht werden. Sie zeigte sich uneinsichtig und argumentierte außerhalb rechtlicher Erwägungen. Ihr konnte aber die Zusage abgerungen werden, sich schriftlich zu den Fragen zu äußern, dazu verwies sie allerdings auf ihre Geschäftsführerin. Am 23. September 2014 meldete sich die Geschäftsführerin und bat um Nachsicht. Sie wolle den Fragebogen beantworten, habe ihn aber im Rahmen eines Umzugs verloren. Sie versicherte nachdrücklich, dass sie die Fragen sehr zeitnah beantworten werde. Am 25. September 2014 wurden die Fragen erneut übersandt. Es erfolgte keine Antwort.

Am 29. Oktober 2014 wurde ein weiteres Owi-Verfahren gegen die Inhaberin eingeleitet und ein entsprechendes Anhörungsschreiben übersandt. Es erfolgte keine Reaktion, von der Möglichkeit der Anhörung wurde kein Gebrauch gemacht. Im Rahmen des Owi-Verfahrens wurde am 4. Dezember 2014 ein (verhältnismäßig hohes) Bußgeld von 1.500,- € für die Nichtbeantwortung der Fragebögen verhängt. Die Einspruchsfrist verstrich, die Geldbuße wurde eingetrieben, es wurde aber weiter keine Auskunft erteilt. Daher musste nun ein Auskunftsheranziehungsbescheid erlassen werden.

Am 9. April 2015 meldete sich der Petent erneut und gratulierte ironisch zur bisherigen Ergebnislosigkeit. Er verlangte eine Antwort auf die Frage, warum wir bislang noch nichts erreicht hatten. Am 20. April 2015 wurde dem Petenten ausführlich geantwortet. Am 22. April 2015 wurde die Verantwortliche mit einem Verwaltungsakt zur Auskunft herangezogen. Am 4. Juni 2015 ging eine lückenhafte Auskunft ohne Datumsangabe oder Unterschrift beim HmbBfDI ein. Auf der Grundlage dieser Informationen teilten wir der Verantwortlichen mit Schreiben vom 2. Juli 2015 mit, dass die VÜ in dieser Form rechtswidrig sei und erklärten, welche Änderungen wir für erforderlich halten. Darauf erfolgte keine Reaktion. Mit Schreiben vom 19. August 2015 wiederholten wir unseren Vorhalt und gaben eine letzte Möglichkeit zur Vermeidung des Erlasses einer verwaltungsrechtlichen Anordnung. Bis zum Ablauf der Frist am 4. September 2015 erfolgte keine Reaktion. 17 Monate nach Eingang der Eingabe konnten nun endlich aufsichtsbehördliche Maßnahmen ergriffen werden. Die Verzögerung ist das Resultat

einer strategischen Zurückhaltung bei der Einleitung förmlicher Verfahren, weil diese zeitintensiv sind und dies vom Referat nicht geleistet werden kann. Bei einer angemessenen personellen Ausstattung des Referats wären derartige Schritte bereits sehr viel früher eingeleitet worden und die Verzögerungstaktik der Beschuldigten hätte sich nicht ausgezahlt.

Aus dem personellen Mangel ergibt sich bei der Videoüberwachung auch ein erheblicher Mangel an Verfolgungsgerechtigkeit. Bei praktisch jeder anlassbezogenen Kontrolle werden dem HmbBfDI Dutzende andere Stellen mit dem Hinweis „Die machen das doch auch!" genannt. Diese Hinweise treffen in aller Regel auch zu. Bürgerinnen und Bürger sind über den Mangel an Schutz ihrer Grundrechte empört, von einer Kontrolle betroffene Unternehmen sind darüber empört, dass ausgerechnet sie kontrolliert werden, der Großteil ihrer Konkurrenz hingegen nicht. Diese Beschwerden sind berechtigt, der HmbBfDI kann ihnen aber nicht abhelfen. Dem Wildwuchs an Kameras kann mit dem jetzigen Personal nicht entgegengetreten werden und es fehlen auch die Möglichkeiten, mit technischer Unterstützung ein System zu analysieren und die Aussagen der verantwortlichen Stelle kritisch zu hinterfragen. Dies könnte nur in Ausnahmefällen erfolgen. Eine regelmäßige Kontrolle von Aussagen, die eine klare Entlastungsmotivation haben, kann im Gegensatz zu Aufsichtsbehörden in anderen Bereichen nicht erfolgen.

Die Situation würde sich eventuell schon dadurch entspannen, wenn Beratungen im Bereich Videoüberwachung für Unternehmen angeboten werden könnten. Immer wieder wenden sich Unternehmen mit der Bitte um Beratung an den HmbBfDI. Dabei handelt es sich in erster Linie um Unternehmen aus dem Bereich „Sicherheitstechnik", aber nicht ausschließlich. Sie haben sowohl Fragen zu konkreten Systemen als auch Bitten um eine generelle Fortbildung, damit sie ihre Kunden technisch und rechtlich beraten können und keine Produkte erwerben, die sie hinterher nicht einsetzen können. Die abschlägigen Antworten des HmbBfDI, die ausschließlich wegen fehlender personeller Ressourcen erfolgen, sorgen vor allem dann für Ärger, wenn die Unternehmen in der Folge aufgrund von Beschwerden geprüft und ggf. sogar beanstandet werden. Beratungen im Vorfeld könnten helfen, das Beschwerdeaufkommen zu senken und würden die Zufriedenheit der Betroffenen stärken.

Beobachtungen geben beispielsweise Anlass für eine gründliche Prüfung des gesamten Bereichs der Videoüberwachung in Apotheken. Daten über den Einkauf von Medikamenten, insbesondere deren Art, Häufigkeit des Einkaufs, Veränderungen in der Medikation usw. stellen sensible Gesundheitsdaten dar. Gleichzeitig werden zahlreiche Apotheken videoüberwacht und die Beratung findet häufig am Tresen in direkter Anwesenheit anderer Kunden statt. Eine grundlegende Überprüfung am besten in Kooperation mit der Apothekerkammer wäre dringend angezeigt, ist aber momentan nicht umzusetzen. Gleiches gilt für die Auswertung der öffentlichen Videoüberwachung. Im Zuge des Neuerlasses von § 30 HmbDSG (VÜ durch öffentliche Stellen)

hat der HmbBfDI alle öffentlichen Stellen, also Polizei, Schulen, JVAs usw., abgefragt und sich Informationen zu sämtlichen Videoüberwachungsanlagen zusenden lassen. Leider reichen die personellen Kapazitäten nicht für eine Überprüfung. Die Unterlagen werden zum Teil ungesichtet gelagert.

Die Kapazitätsprobleme des Referats wirken sich dabei nicht nur auf den Bereich der Videoüberwachung aus, sondern führen auch zu Mängeln im Bereich der Informationsfreiheit.

Beim Transparenzportal wäre beispielsweise, auch unabhängig von konkreten Bürgerbeschwerden, eine gründliche Überprüfung sämtlicher Unternehmen und ihrer Veröffentlichungspraxis angezeigt. Schon eine oberflächliche Sichtung zeigt auf den ersten Blick, dass die nach § 2 Abs. 3 HmbTG zur Veröffentlichung verpflichteten Unternehmen nur verhältnismäßig wenige Unterlagen veröffentlichen. Eine Überprüfung wurde vom HmbBfDI bislang nur bei der Hamburger Hochbahn AG unternommen. Die Besprechung war für alle Beteiligten hilfreich, Vor- und Nachbereitung waren jedoch zu zeitintensiv, als dass man dies regelmäßig wiederholen könnte, geschweige denn für alle betroffenen Unternehmen durchführen könnte. Auch im Bereich des Transparenzgesetzes wären Beratungen, Informationen und Schulungen sicherlich hilfreich. Zwar hat das Umsetzungsprojekt zahlreiche Schulungen durchgeführt, aber diese bezogen sich ausschließlich auf den Workflow und die Veröffentlichungsgegenstände. Es gibt daneben in den Behörden auch zahlreiche Fragen zum Auskunftsverfahren. Aufgrund der gestiegenen Eingabenzahlen im Bereich der „Informationsfreiheit" können Fortbildungsveranstaltungen im ZAF zum HmbTG aber leider nicht mehr angeboten werden. Dies ist besonders bedauerlich, da dadurch zahlreiche Probleme aus den Behörden an den HmbBfDI herangetragen wurden und gleichzeitig die Hemmschwelle für die Behörden abgesenkt wurde, sich an den HmbBfDI zu wenden und sich beraten zu lassen. Vor diesem Hintergrund ist es zwingend erforderlich, dass die bisherige Abordnung fest in den Stellenbestand des HmbBfDI überführt wird. Zusätzlich müsste das Referat mit einer weiteren Stelle ausgestattet werden.

4.4 Referat D4: Sicherheit, Demokratie und Daseinsvorsorge

Das Referat D4 ist aus dem ehemaligen „Referat Datenschutzrecht" hervorgegangen und ist daher noch immer das Fachreferat beim HmbBfDI, das hauptsächlich im öffentlichen Bereich tätig ist und in erster Linie die datenschutzrechtliche Aufsicht über die Hamburger Behörden nach dem Hamburgischen Datenschutzgesetz ausübt. Dabei ist das Referat für so unterschiedliche Bereiche wie Gesundheit, Soziales, Schulen und Hochschulen, Verkehr („Smart City"), Innere Sicherheit und Justiz zuständig. Das Referat D4 spiegelt mit seinen 4 Mitarbeiterinnen und Mitarbeitern (bei 3,1 VZÄ, eine Mitarbeiterin ist nur noch mit 0,1 VZÄ im Referat D4 tätig, ansonsten im Referat D6) also fast die gesamte Hamburger Verwaltung einschl. der Polizei wider. Nur bestimmte übergreifende Themen, wie z.B. der Arbeitnehmer-datenschutz und die Videoüberwachung, sind in andere Referate verlagert worden.

Ein großes „Überwachungsobjekt" des Referats D4 ist das Universitätsklinikums Hamburg-Eppendorf (UKE), mit dem der HmbBfDI allein schon für ein einziges Forschungsvorhaben über einen Zeitraum von mehr als zwei Jahren in Kontakt stand, um die datenschutzrechtliche Planung der Hamburg City Health Studie zu begleiten. Bei dieser Studie handelt es sich um eine Beobachtungsstudie, durch die ein besseres Verständnis über Häufigkeiten, Ursachen und Verlauf von Erkrankungen erlangt werden soll. Zu diesem Zweck sollen rund 45.000 Hamburgerinnen und Hamburger im Alter von 45 bis 74 Jahren untersucht werden, um Risikofaktoren für die häufigsten Volksleiden (Herz-Kreislauf-Erkrankungen, Schlaganfall, Demenz und Krebserkrankungen) und Todesursachen zu identifizieren. Die Studie wird umfassend von fast 30 Kliniken und Instituten des UKE einschließlich des Universitären Herzzentrums und der Martini-Klinik durchgeführt. Neben einer Vielzahl von medizinischen Untersuchungen gehören zu diesem Forschungsvorhaben auch die genetischen Untersuchungen von Blut bzw. sonstigem Biomaterial sowie deren Sammlung in einer Biomaterialbank. Über mehrere Jahre und Jahrzehnte hinweg sollen hier personenbezogene Daten verarbeitet werden. Hinzu kommt die Erweiterung des auszuwertenden Datenmaterials dadurch, dass Informationen auch von dritter Seite hinzugezogen werden sollen, z.B. von Hausärzten, Fachärzten, Krankenhäusern, aber auch von der Krankenversicherung, Rentenversicherung und dem Krebsregister. In diesem Zusammenhang kooperiert das UKE auch mit weiteren Partnern, sodass die Daten ggf. auch international verarbeitet werden. Die datenschutzrechtliche Begleitung beinhaltet eine detaillierte Betrachtung der einzelnen Datenverarbeitungsschritte von der Datenerhebung über die Speicherung bis hin zur Nutzung bzw. Übermittlung an andere Stellen. Kern der datenschutzrechtlichen Sicherung personenbezogener Daten ist ein umfangreiches und weit verzweigtes Pseudonymisierungsverfahren, das seinerseits technisch unterstützt ist. Hier muss sichergestellt sein, dass die Forscher auf der Grundlage einer wirksamen Einwilligung zwar die erforderlichen Daten nutzen können; die jeweilige konkrete Person des Studienteilnehmers ist jedoch für die Forschungstätigkeit nicht von Bedeutung, so dass hier mittels Pseudonymisierung die Kenntnis von Namen und sonstigen direkt identifizierenden Informationen der Studienteilnehmer ausgeschlossen sein muss. Nach über zwei Jahren intensiver Auseinandersetzung mit dem UKE konnte letztlich ein Studiendesign entwickelt werden, das einerseits datenschutzrechtlichen Anforderungen genügt und andererseits auch die Forschungsinteressen hinreichend berücksichtigt.

Durch solche nicht ungewöhnlichen Verfahren werden über lange Zeiträume Arbeitskräfte gebunden, die naturgemäß an anderer Stelle fehlen. So plant beispielsweise das UKE bereits seit einigen Monaten ein sogenanntes Zuweiserportal, mit dessen Hilfe medizinische Daten der Patienten dem Zuweiser zur Verfügung gestellt sollen. Die dem HmbBfDI bereits längere Zeit vorliegenden Unterlagen konnten aber aus Kapazitätsgründen bisher nicht weiter geprüft werden.

Auch die Überprüfung der in Hamburg bestehenden Bio-/Datenbanken, also die in

Bio-/Datenbanken in Krankenhäusern gesammelten Gesundheitsdaten, wurde wegen fehlender Kapazitäten bereits seit Jahren stetig vertagt. Bio-/Datenbanken bilden oftmals über Jahre hinweg ein gesundheitliches Profil des Betroffenen ab. Hinzu kommt, dass die gesammelten Bioproben meistens dazu geeignet sind, das gesamte Genom des Betroffenen und damit einen unveränderlichen Teil seiner Identität zu entschlüsseln. Kommt es bei dem Betrieb einer Bio-/Datenbank zu Datenschutzverletzungen, z.B. durch den Zugriff Unbefugter auf die Daten und das genetische Material, dürfte es für den Forschungsstandort Hamburg extrem negative Auswirkungen haben.

Die (erste) Prüfung der Antiterrordatei, die laut Urteil des Bundesverfassungsgerichts vom 24. April 2013 in angemessenen Abständen – deren Dauer ein gewisses Höchstmaß, etwa zwei Jahre, nicht überschreiten darf – zu wiederholen ist, dauert weiterhin an und geht bereits jetzt weit über April 2015 hinaus. Es müsste also bereits eine Wiederholungsprüfung stattfinden, obwohl die erste Prüfung noch gar nicht abgeschlossen ist.

Auch eine Prüfung des Statistikamtes Nord ist schon lange dringend geboten. Grund hierfür ist die enorm große Datenmenge, die dort verarbeitet wird. Damit der HmbBfDI von der Einhaltung der speziellen statistikrechtlichen Datenschutzvorschriften überzeugt ist, bedarf es insoweit dringend einer entsprechenden Kontrollprüfung, was jedoch derzeit nicht durchführbar ist.

Diese und weitere Defizite müssen behoben werden, indem das Referat mit 1,5 zusätzlichen VZÄ ausgestattet wird.

4.5 Referat D5: Wirtschaft und Finanzen

Das Referat D5 war bis zur Umstrukturierung die „Aufsichtsbehörde nach § 38 BDSG" und weitestgehend allein verantwortlich für den nicht-öffentlichen Bereich. Viele Aufgabenbereiche aus dieser Zeit sind erhalten geblieben, sodass D5 u.a. für Banken, Versicherungen, Werbung, Handel (einschl. Onlinehandel), Industrie, Gewerkschaften und Vereine zuständig ist. Dafür stehen dem Referat gegenwärtig 5 Mitarbeiterinnen und Mitarbeiter mit zusammen 3,3 VZÄ zur Verfügung.

Das Referat D5 ist u.a. für einen großen Hamburger Versandhandelskonzern zuständig. Mitte 2013 erreichten den HmbBfDI Beschwerden über die Übermittlung von Kundendaten innerhalb dieses Konzerns. Aus diesem Anlass begannen wir eine Prüfung des konzerninternen Austauschs von Neukundendaten und stellten fest, dass daran 11 Unternehmen mit insgesamt 33 Dateien beteiligt waren. Die jeweiligen Übermittlungen entsprachen zwar einem von den Unternehmen festgelegten Muster, dieses war jedoch nicht datenschutzgerecht und ließ insbesondere die in derartigen Fällen maßgeblichen Auskunfteienvorschriften außer Acht. In der Folge wurden insgesamt 13 Schreiben an das Unternehmen und deren Anwälte verfasst, auf die wir ebenso viele, teilweise 20-30seitige Antworten mit ausführlichen rechtlichen Erörterungen

erhielten. Das Unternehmen weigerte sich lange Zeit, die datenschutzrechtlich notwendigen Veränderungen an dem System einzuführen und versuchte, durch intensive Rechtsausführungen den Status Quo zu sichern.

Intern wurden die rechtlich schwierigen Fragen insgesamt in 8 Sitzungen mit mindestens 2, oft aber 4 Teilnehmern (einschließlich des HmbBfDI), intensiv erörtert. Hinzu kamen zahlreiche Telefonate mit den Unternehmensvertretern. Ein erster persönlicher Gesprächstermin unserer Dienststelle mit den Unternehmensvertretern fand dann Anfang 2014 statt. Das von uns dabei gefertigte Protokoll musste anschließend eingehend zwischen allen Beteiligten abgestimmt werden. Erst nach dieser Sitzung konnte angesichts der komplizierten Ausgestaltung der gegenseitigen Datenübermittlungen ein umfassender Sachverhalt erarbeitet werden, woran 4 Bearbeiter beteiligt waren und der innerhalb der Dienststelle mehrfach besprochen werden musste. Im Anschluss daran erfolgte eine nicht ganz konfliktfreie Abstimmung mit den Unternehmensvertretern. Nach Feststellung des Sachverhalts folgte eine 29-seitige rechtliche Bewertung der einzelnen Datenübermittlungen in diesem recht undurchschaubaren System, an der wiederum 4 Bearbeiter beteiligt waren. Nachdem diese dem Unternehmen zur Verfügung gestellt worden war, folgten wieder wechselseitige rechtliche Erörterungen. Anschließend wurden 5 weitere Aufsichtsbehörden eingebunden, die unmittelbar beteiligt waren, weil an dem System angeschlossene Unternehmen auch in den Bundesländern dieser Aufsichtsbehörden und in Österreich ansässig sind. Der Sachverhalt und unsere rechtliche Bewertung wurden zur Verfügung gestellt und ein 2-tägiger Termin vereinbart, in dem zunächst die Aufsichtsbehörden an einem Tag ihre Auffassung abstimmten und am nächsten Tag mit den Unternehmensvertretern erörterten. Allein die schriftliche Vorabstimmung dieses Termins erforderte weiteren umfangreichen Schriftwechsel über die Inhalte der von uns vorgenommenen rechtlichen Bewertung. Die genannten Arbeiten nahmen einige Monate von 2013 sowie das ganze Jahr 2014 in Anspruch. Nachdem im Januar 2015 der oben erwähnte Termin stattgefunden hatte, gab es einen „Durchbruch“, der sich sowohl in dem wiederum mehrfach abzustimmenden Protokoll ausdrückte, als auch in Ergebnisabsprachen mit dem Unternehmen mündete. Diese Ergebnisse wurden dann im März 2015 zum Düsseldorfer Kreis angemeldet und führten zu einem Beschluss, der unsere Arbeit unterstützte. Mittlerweile hat es weiteren Schriftwechsel mit dem Unternehmen, verteilt über das Jahr 2015, gegeben, weil die Ergebnisabsprachen einen Zeitplan für die Umsetzung der Änderungen enthalten, die von uns überprüft werden. Voraussichtlich wird sich dies bis Anfang 2016 hinziehen. Dieser Fall war schon Thema im Tätigkeitsbericht 2012/2013 und wird auch im Tätigkeitsbericht 2014/2015 eingehend geschildert. Er zeigt, dass es in komplexen Verfahren außerordentlich schwierig ist, die Unternehmen zu datenschutzgerechtem Verhalten zu veranlassen. Immer wieder wurde zwischenzeitlich auch über die Möglichkeit einer Anordnung oder eines Bußgeldes unsererseits diskutiert. Das wurde jedoch verworfen, weil zwar vieles unzulässig war, die rechtliche Diskussion aber zeigte, dass es an Eindeutigkeit fehlte und ein hohes Prozessrisiko allein wegen der Schwierigkeit bestand, einzelnes Fehlverhalten anhand konkreter Punkte festzumachen.

Angesichts solcher langwierigen und komplexen Fällen, die, wie schon beim Referat D4 angemerkt, unverhältnismäßig viel Arbeitskraft binden, wird deutlich, warum auch im Referat D5 andere wichtige Tätigkeiten „auf der Strecke bleiben". So ist es zum Beispiel in fast keinem Arbeitsfeld möglich, dem Beratungsbedarf von behördlichen und betrieblichen Datenschutzbeauftragten, Unternehmen oder Behörden gerecht zu werden. Rechtsfragen können nicht mit der erforderlichen Sorgfalt bearbeitet werden, und es fehlt die Zeit für die teilweise notwendige intensive Recherchen in Literatur und Rechtsprechung. Auch kann Zweifeln an der Recht- und sogar Verfassungsmäßigkeit von Vorschriften nicht in wünschenswertem Umfang nachgegangen werden; bei Beteiligungen in laufenden Gesetzgebungsverfahren wird dies soweit wie möglich gewährleistet. Bei bereits bestehenden Rechtsvorschriften über Spezialgebiete (z. B. Steuer- oder Geodatenrecht) jedoch überhaupt nicht mehr. Ausreichende Sachverhaltsaufklärung bei Prüfungen und Beweiserhebung bei Zweifeln an Stellungnahmen von Unternehmen sind kaum möglich. Hält der HmbBfDI infolge einer Bürgerbeschwerde einen Datenschutzverstoß in einem Unternehmen für wahrscheinlich, fordert er das Unternehmen in der Regel zunächst zu einer Stellungnahme auf. Oftmals weist das Unternehmen die Vorwürfe zurück, indem es schon den Sachverhalt bestreitet. Eine mögliche Vor-Ort-Prüfung mit Einsichtnahme in die EDV oder die Unterlagen des Unternehmens ist der Behörde aufgrund der begrenzten Kapazitäten nur in Ausnahmefällen bei überragendem öffentlichem Interesse oder in vermuteten eingriffsintensiven Fällen möglich. Die Angaben der Unternehmen müssen deshalb häufig als wahr hingenommen werden und Beschwerden kann dann nicht weiter nachgegangen werden. Dabei ist es auch schon angesichts der vielen Beschwerden, in denen bereits aus diesen Anlässen heraus Kontrollen vorgenommen werden, so gut wie gar nicht mehr möglich, Unternehmen auch ohne Anlass zu prüfen. Das ist umso bedauerlicher, weil dadurch der Eindruck entstehen kann, dass die Nichtbeachtung der Datenschutzregeln unentdeckt und folgenlos bleiben kann.

Die Aufstockung des Personalbestands bei D5 um 2 VZÄ (davon 1 x zur Versetzung des bisher nur abgeordneten Personals und als Ersatz für die zeitlich befristeten 0,3 VZÄ) wird als notwendig betrachtet.

4.6 Referat D6: Medien, Telemedien und Telekommunikation, E-Government

Das Referat D6 wurde im Zuge der Neustrukturierung des HmbBfDI neu geschaffen und ist das einzige Referat beim HmbBfDI, in dem Informatiker und Juristen gemeinsam tätig sind. Der Schwerpunkt dieses Referats liegt bei der Aufsicht und der Beratung von Internetdiensten, was sowohl globale Internetunternehmen als auch kleine Startups umfasst. Das Referat bestand ursprünglich aus 3 Mitarbeitern mit zusammen 1,95 VZÄ. Im Laufe dieses Jahres wurde das Referat um 2 Mitarbeiter und Mitarbeiterinnen (1,2 VZÄ) verstärkt, die ausschließlich die Eingaben von Bürgerinnen und Bürgern bearbeiten, die sich wegen abgelehnter Anträge zur Löschung bei der Google-Suche an den HmbBfDI wenden. 0,5 VZÄ davon wurden beim Referat D4 abgezogen, und 0,7 VZÄ werden durch eine u.a. zu diesem Zweck geschaffene befristete Stelle

(weitere 0,3 VZÄ dieser befristeten Stelle kommen bei D5 zum Einsatz) eingebracht.
Beispielhaft gerade für die datenschutzrechtliche Aufsicht über die großen Internetkonzerne ist der folgende Vorgang. Bereits 2012 hatte die Google Inc. ihre sogenannten Privatsphärebestimmungen durchgreifend geändert. Wo bislang unterschiedliche Regelungen für die einzelnen Google-Produkte (Suche, Youtube etc.) galten, wurde nun eine gemeinsame Basis für alle Produkte geschaffen. Diese erklärte einseitig die kombinierte, gemeinsame Verwendung aller von Google gesammelten Daten produktübergreifend für zulässig.Hiergegen wurde vom HmbBfDI und einer Reihe anderer europäischer Datenschutzbehörden massive Kritik geäußert. Dies führte zur Bildung einer europaweiten „Task Force", an der für Deutschland der HmbBfDI teilnimmt. Da Google seinen Deutschlandsitz in Hamburg hat, ist der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit die national zuständige Aufsichtsbehörde.

Die ersten Reaktionen von Google auf die geäußerte Kritik machten deutlich, dass es in diesem Fall der gemeinsamen und koordinierten Anstrengung verschiedener Aufsichtsbehörden in Europa bedarf, um Google zu relevanten Zugeständnissen zu bewegen. Um diesen Schulterschluss zu praktizieren und auf der Arbeitsebene zu verwertbaren Ergebnissen zu kommen, waren ein intensiver Austausch von Dokumenten und eine Reihe von Treffen erforderlich. Diese fanden überwiegend in Paris statt, da die Federführung der Task Force bei der französischen Datenschutzbehörde CNIL liegt, aber auch Hamburg war als Gastgeber aktiv. Um den Aktivitäten auf gesamteuropäischer Ebene den nötigen Nachdruck zu verleihen, haben die Aufsichtsbehörden die ihnen jeweils zur Verfügung stehenden rechtlichen Instrumente genutzt, die Anforderungen durchzusetzen. In unserem Fall geschah dies im September 2014 durch eine Anordnung, mit der Google verpflichtet wird, die Kombination der Nutzerdaten auf eine zulässige Basis zu stellen oder diese zu unterlassen. Zusätzliche Komplexität erhält dieser Verwaltungsakt dadurch, dass Google Klage dagegen erhoben hat, so dass wir uns nun auch verwaltungsgerichtlich damit befassen müssen.Unabhängig davon zeigt die von den Aufsichtsbehörden eingeschlagene Strategie mittlerweile deutliche Erfolge. Das Unternehmen Google hat wesentliche Änderungen an seinen Produkten vorgenommen, die durch eine Einwilligungslösung die rechtskonforme Verarbeitung der erhobenen Daten sicherstellen sollen. Zugleich können die Nutzer in erweitertem Umfang Kontrollrechte wahrnehmen und damit die Datensammelei von Google einschränken. Ob das Gesamtpaket eine Umsetzung unserer Anordnung darstellt, ist noch Gegenstand weiterer Prüfungen, zu der auch erweiterte Dokumentationen gehören, die Google bis spätestens Anfang März 2016 vorlegen muss.

Nicht immer, aber immer öfter bedürfen die Verfahren gegen große Unternehmen bundesweiter und auch europäischer Abstimmungen, was neben den Sachmitteln (insb. Reisekosten) auch in hohem Maße Personal bindet. Das ist mit ein Grund dafür, dass das Referat bestimmte Tätigkeiten nicht oder nur mit (in Bezug auf die Komplexität und den Umfang der Dinge) deutlich zu geringem Einsatz durchführen kann bzw. konnte. Ein Dauerbrenner in dieser Hinsicht sind beispielsweise die Beschwerden im Zusammen-

hang mit Löschanträgen an Google, von denen dem HmbBfDI mittlerweile knapp 400 vorliegen. Die Betroffenen sehen darin ihre Ansprüche auf Löschung von Links in der Suchmaschine von Google durch das Unternehmen nicht ausreichend berücksichtigt. Ständig kommen neue Beschwerden hinzu und in vielen bearbeiteten Fällen kommen neue Vorträge bzw. weitere Eingaben. Aufgrund zu geringer Kapazitäten konnten bislang ca. 150 dieser Beschwerden nicht abgearbeitet werden. Es entstehen dadurch erhebliche Reaktionszeiten für die Betroffenen, bis es überhaupt zu einer ersten Befassung durch die Dienststelle kommt. Gleiches gilt für weitere Bürgerbeschwerden, bei denen aufgrund hoher Fallzahlen bei geringer Personalstärke selten eine angemessene Bearbeitungszeit gewährleistet werden kann. Bürger müssen vielmehr häufig zeitlich vertröstet werden, bevor eine inhaltliche Befassung möglich ist.
Weitere Defizite ergeben sich bei der Begleitung von Social Media in der hamburgischen Verwaltung (z.B. Facebook und Twitter), die von verschiedenen Behörden und Dienststellen der FHH eingesetzt werden. Der HmbBfDI konnte hier in wenigen Einzelfällen beratend tätig sein oder im Beteiligungsweg datenschutzrechtliche Vorgaben durchsetzen. Allerdings fehlen die Kapazitäten, um allgemein geltende Vorgaben im Sinne eines Social Media Guide zu erstellen und diesen anschließend durchzusetzen. Es ist daher damit zu rechnen, dass in der FHH soziale Medien nicht datenschutzgerecht eingesetzt werden. Ähnliches gilt für die Begleitung von Wissenschaft und Forschung, also die Begleitung der technischen und rechtlichen Entwicklung moderner Datenschutzkonzepte. Solche Initiativen seitens des HmbBfDI sind nicht möglich, wodurch die wertvollen Praxiserfahrungen der Dienststelle nicht in die Fortentwicklung des Datenschutzes eingebracht werden können. Den entwickelten Konzepten fehlt daher häufig der Praxisbezug. Zudem ist eine systematische rechtliche und technische Fortbildung der Mitarbeiterinnen und Mitarbeiter derzeit kaum möglich. Die beschriebene Arbeitslast erlaubt es nicht, dass Beschäftigte der Dienststelle sich systematisch fortbilden können. In dem hochdynamischen Bereich der IT-Entwicklung und der Rechtsfortbildung im Datenschutzrecht bedroht diese Situation die fachliche Qualität der Arbeitsergebnisse der Behörde.

Wie in allen anderen Referaten werden auch im Referat D6 kaum anlassfreie Prüfungen durchgeführt. Dabei wären zum Beispiel Prüfungen von Unternehmen aus der Computerspielebranche dringend geboten. In Hamburg sitzen bedeutende Anbieter von Onlinespielen, deren Kunden dort mit umfänglichen personenbezogenen Daten – nicht zuletzt Kontodaten und ähnliches zur Bezahlung der Spiele – gespeichert sind. Welches Datenschutzniveau die Anbieter dabei einhalten, liegt für uns völlig im Dunkeln.

Die Dringlichkeit der Prüfungen gilt genauso für Prüfungen von Apps, Webseiten oder Telemediendiensten, die aufgrund des Zeitaufwandes nur aus konkretem Anlass stattfinden. Für Spontan- oder Initiativprüfungen ist keine Zeit. Unternehmen oder öffentliche Stellen in Hamburg müssen kaum befürchten, dass Datenschutzmissstände in ihren Apps, Webseiten oder Dienstangeboten durch uns aufgedeckt werden. Aktuell

wird eine länderübergreifende Prüfung von Partnerschaftsbörsen durchgeführt, an der auch der HmbBfDI teilnimmt. Dabei können von uns jedoch lediglich die drei größten Anbieter geprüft werden; für die Prüfung der anderen Anbieter mit Sitz in Hamburg fehlen die Kapazitäten. Insgesamt hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit nicht die Kapazitäten, sich an deutschland- oder europaweiten Branchenprüfungen zu beteiligen.

Auch die Beratung von Unternehmen, eine der gesetzlich festgelegten Aufgaben des HmbBfDI, kann durch das Referat D6 nur sehr rudimentär durchgeführt werden. Über eine kurze Orientierung oder die Beantwortung sehr spezifischer Einzelfragen hinaus müssen Unternehmen, die sich mit Beratungsbedarf an uns wenden, abgewiesen werden. Dies betrifft auch solche Unternehmen, die sich rechtzeitig um datenschutzgerechte oder datenschutzfreundliche Produkte bzw. Dienstleistungen bemühen möchten, um von vornherein Datenschutzprobleme zu vermeiden. Zudem sind die Beratungszeiten zu lang, um den teilweise zeitsensiblen Entwicklungen gerecht zu werden. Letzteres ist auch das große Problem beim Monitoring bzw. Dokumentieren von Facebook oder Google. Das breite Dienstangebot und die Funktionalitäten von Facebook und Google oder des von Google konzipierten Betriebssystems Android verändern sich nahezu täglich. Aus Kapazitätsgründen kann dies nicht regelmäßig dokumentiert oder überhaupt angemessen verfolgt werden. Es wird daher häufig an Themen (weiter-)gearbeitet, die durch Schaffung neuer Fakten durch die Anbieter in der datenschutzrechtlichen Konstellation verändert wurden. Oftmals kann der ursprüngliche Zustand bzw. die Problemlage dann nicht mehr geahndet werden.

Um die Aufgaben wahrnehmen zu können, ist es erforderlich, dass die bisher befristete Stelle für das Referat D 6 auf 100% aufgestockt und entfristet wird. Zusätzlich benötigt das Referat einen weiteren juristischen Referenten bzw. Referentin und eine halbe Stelle für eine weitere technische Referentin bzw. Referenten.

5. Personalforderung und Kosten

Die Forderungen nach mehr Personal beim HmbBfDI und die sich daraus ergebenden zusätzlichen Personalkosten nach Personalkostenverrechnungstabelle 2016 stellen sich zusammengefasst wie folgt dar:

Referat	VZÄ 2015	davon abgeordnet o. befristet	gefordert VZÄ	zusätzliche Personalkosten	VZÄ nach bewilligter Forderung
D1	4,75	-	1,5	121.821,50 €	6,25
D2	2,4	0,5	2	158.010,- €	3,9
D3	1,7	0,7	2	152.860,- €	3
D4	3,1	-	1,5	115.932,50 €	4,6
D5	3,3	0,8	2	167.027,- €	4,5
D6	3,15	0,7	2,5	190.276,- €	4,95
Gesamt	18,4	2,7	11,5	905.927,- €	27,2

Dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit ist bewusst, dass angesichts der gegenwärtigen Situation der öffentlichen Haushalte eine einmalige hohe Aufstockung des Personals um 11,5 Stellen aller Voraussicht nach nicht umgesetzt werden kann. Zudem lassen sich vor der Umsetzung der Europäischen Datenschutzgrundverordnung Aussagen über künftige Personalmehrbedarfe, die in diesem Zusammenhang entstehen werden, nicht abschließend treffen. Der HmbBfDI ist daher bereit, die erforderliche Personalaufstockung von 11,5 VZÄ um jeweils 0,5 VZÄ pro Referat zu kürzen und zunächst zurückzustellen.

Es bleibt somit bei einer Forderung nach Verstärkung des Personals beim HmbBfDI um 8,5 VZÄ.

Diese personelle Verstärkung würde Personalkosten in Höhe von 672.682 Euro verursachen.

Durch diese Erhöhung des Personalbestands ergeben sich aber auch Folgekosten, die hier nur angedeutet werden können:

Durch den geplanten Verkauf der Cityhochhäuser ist der HmbBfDI gezwungen, spätestens Mitte 2017 neue Büroräume zu beziehen. Das Immobilien Service Zentrum der Sprinkenhof GmbH ist nach Vermittlung durch das LIG bereits auf der Suche nach adäquaten Immobilien. Die derzeitigen Räumlichkeiten der Dienststelle des HmbBfDI verursachen Kosten in Höhe von rund 65.000 Euro pro Jahr. Nach Auskunft der Sprinkenhof sind Büroräume in Hamburg zu diesem Preis nicht zu finden. Nach einer entsprechenden Analyse geht die Sprinkenhof GmbH von einem Raumbedarf von etwa 800 m2 für den HmbBfDI aus, der nach dortiger Schätzung 175.000,- Euro Kosten pro Jahr verursachen würde. Diesen Mehrbedarf hat der HmbBfDI, insbesondere zur Berücksichtigung bei

den sog. Eckwerten, der JB bereits mitgeteilt.

Bei einer Erhöhung des Personalbestands würde sich der Raumbedarf entsprechend erhöhen, schätzungsweise um rund 100 m². Es muss also davon ausgegangen werden, dass sich die Kosten für Büroraum dann auf etwa 200.000,- Euro im Jahr erhöhen werden. Hinzu kommen Anschaffungskosten für (PC-) Arbeitsplätze und die sich daraus ergebenden laufenden Folgekosten.

6. Weitere Informationen

Würde sich das VZÄ-Soll des HmbBfDI von derzeit 16,4 auf 24,9 VZÄ erhöhen, würde der HmbBfDI im Vergleich der Datenschutzbeauftragten der Länder von seinem bisherigen 13. Rang (nur Mecklenburg-Vorpommern, Saarland und Bremen haben weniger Personal) auf den 8. Rang verbessern.

1.	NRW (53 VZÄ)	5.	NI (33,6 VZÄ)	9.	BB (23 VZÄ)	13.	TH (19 VZÄ)
2.	BY (50 VZÄ)	6.	BW (32,5 VZÄ)	10.	SN (22 VZÄ)	14.	MV (14 VZÄ)
3.	HE (44,5 VZÄ)	7.	SH (28 VZÄ)	11.	ST (22 VZÄ)	15.	SL (13 VZÄ)
4.	BE (39 VZÄ)	**8.**	***HH (24,9 VZÄ)***	12.	RP (20 VZÄ)	16.	HB (12,8 VZÄ)

(Quelle: Länderumfrage des BlnBDI 2014, DSB und LDA Bayern zusammengefasst, Zahlen jeweils einschließlich der Stelle des/der Datenschutzbeauftragten)

A

Abrufverfahren aus dem Melderegister IV 5.2
Abschottung III 1.1
Android VI 1.2
Anlage B zu den Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) IV 1.6
Anonymität V 9
Anordnungen nach § 38 Abs. 5 BDSG VI 11.1, XI 2
Anti-Terror-Datei I 1
Antiterrordatei (ATD) IV 1.4
Apple VI 1.2
Apps V 17, V 4
Arbeitgeberzeitschrift IX 1.3
Artikel 29-Gruppe X 1, V 1
Auditierung I 4.1
Auftragsdatenverarbeitung VIII 1.6, VI 2.7, V. 16.
Auskunft IV 1.9
Auskunfteien VIII. 1.
Auskunftssperre IV 5.2
Ausschuss für Justiz und Datenschutz I 1
Ausweiskopie IV 1.9
Authentisierungsverfahren IV 5.2
AutiSta IV 6.2
Automatisiertes Verfahren VII 2.5

B

Beanstandung I 3
Behörde für Inneres und Sport VI 1.4, IV 1.9
Beobachter/in zur Lagebeurteilung (BfL) IV 1.5
Berichtswesen II 2.3
Berufsgeheimnisträger IV 1.1
Berufsordnung für Rechtsanwältinnen und Rechtsanwälte (BORA) IV 4.2
Beschäftigte VII 2.4
Beschäftigtendaten IX 3.
Betrugsprävention VIII. 1.2
Bewerberunterlagen IX 3.
Bezahlkarten VIII 1.7
Bezirksamt Harburg – Amt für Zentrale Meldeangelegenheiten IV 5.2
Bezirksversammlung IV 8.1
Bildung und Teilhabe II 2.6
Bluetooth V 9
Bodycams IV 1.3
Bücherhalle VII 2.2
Bundeskriminalamt (BKA) IV 1.11, iV 1.4

Bundesliga VIII 1.7
Bundesmeldegesetz IV 5.1
Bundesrechtsanwaltsordnung (BRAO) IV 4.2
Bundesverfassungsgericht (BVerfG) I 1, IV 1.4
Bußgeld XI 2
BYOD VI 1.3, VI 1.2

C

CCMS VI 1.5
Cisco VI 2.4, VI 2.1, VI 1.7
Cloud Computing V 6
Clouddienste V 1. 3
Community Cloud Mail Service VI 1.5
Compliance I 4.1
Cookie-Richtlinie V 12
Cookies V 17

D

Dashcam VII 1.1
Data Center Polizei IV 1.12
Datenabgleich IV 5.1
Datenabrufe aus dem Melderegister IV 5.1
Datenerhebung IV 1.10
Datenpannen XI 3
Datenschutz-Kodex für Geodatendienste V. 14
Datenschutzverstöße XI 2
Datenschutzvorfälle XI 3
Datenträgervernichtung VI 1.8
Datentrennung III 1.1
Demokratische Legitimation I 2.2
Dienstaufsicht I 2.1
Digitale Revolution Vorwort
Digitale Stadt VI 2.1
DIN 66399 VI 1.8
Direkterhebungsgebot II 2.1
DME Excitor VI 1.3, VI 1.2
DSK XI 5

E

Eingaben XI 1
Eingabenstatistik XI 1
Einheitspersonenkontenverordnung VIII 2.2, VIII 2.1
Einsatz von verdeckt ermittelnden Polizeibeamtinnen und -beamten IV 1.5

Einwilligung	IV 8.1
Einwilligungserklärung	III 1.4
Elektronische Patientenakte	II 1.7
E-Mail-Kommunikation	II 2.4, II 1.5
Ende-zu-Ende-Verschlüsselung	VI 1.4
Energieversorger	VI 2.6
Energieversorgungsunternehmen	VI 2.6
EPKVO Siehe	VIII 2.1
E-Privacy Richtlinie	V 12
Errichtungsanordnung	IV 1.10
eTicketing	VI 2.3
EU-Datenschutzgrundverordnung	I 3, I 1, Vorwort
EuGH	V 1. 1.1, IV 1.1
EU-Kommission	I 3
Europäischer Datenschutztag 2015	XI 5
Europäischer Gerichtshof	IV 1.1, I 1, Vorwort
Europäisches Parlament	I 3
Exchange	VI 1.4
Exchange 2013	VI 1.5

F

Facebook	IV 1.6
Anordnung	V 2.2
Anwendbares Recht	V 2
Ausweiskopie	V 2.2
Datenrichtlinie	V 2
Klarnamenpflicht	V 2.2, V 2.2
Nutzungsbedingungen	V 2
Pseudonyme Nutzung	V 2.2
Fachaufsichtliche Kontrolle	I 2.1
Fahndungsdaten	IV 1.6
Fax over IP	VI 1.1
Faxen	VI 1.1
Fernmeldegeheimnis	III 1.4
FHHportal	VI 1.6
Finanzbehörde	VIII 2.2, VI 1.6, VI 1.5, VI 1.4, VI 1.2, VI 1.1, III 2.1
Flüchtlinge	IV 3.1
Fluggastdatenübermittlung	X. 3.
Formular	II 2.6
Forschung	II 1.2
Freiwilligkeit	IV 3.1, III 1.4
Fremdsprachige Betroffene	IV 3.1

Funkbasierte Ablesegeräte VI 2.5

G

Gefahrengebiete IV 1.2
Geheimdienste VI 1.2
Geldbußen I 3
Gemeinsame Datei II 1.1
Generalregisterverfahren IV 6.1
Genetische Untersuchung II 1.3
Geobusiness Code of Conduct V. 15
Geodaten V. 15, V. 14
Geoinformationen V. 15.
Google VI 1.2, V 1. 1.1
  Apps V 1. 3
  Datenschutzerklärung \t 116
  Datenschutzniveau V 1. 3
  Google Task Force \t 116
  Privatsphärebestimmung V 1. 2
  Suchmaschine I 1
GPS IX 1.1
Grundrechtecharta I 2.3
Grundversorger VI 2.6
Gütesiegel I 4.1

H

Hamburg Port Authority (HPA) VI 2.4
Hamburger Medienpass III 1.5
Hamburger Schreib-Probe III 1.3
Hamburgisches Ausführungsgesetz zum Bundesmeldegesetz IV 5.1
Hamburgisches Verfassungsschutzgesetz (HmbVerfSchG) IV 2.1
Hanseatische Rechtsanwaltskammer Hamburg (RAK Hamburg) IV 4.2
HbbTV V 17
Heartbleed V 13
HERAKLES VIII 2.2, VIII 2.2
Hilfsmerkmale IV 7.1
Hinweis- und Informationssystem VIII 3.1
HIS VIII 3.1
Hotspot V 7
HVV-Card VI 2.3

I

Identifizierung IV 1.9
Identitätsfeststellung IV 1.10
Indoor-Tracking V 9

Informationelles Selbstbestimmungsrecht	IV 1.10
Informationspflicht	IV 5.1, II 1.4
Integration	IV 3.1
Integrierte Hilfe	II 2.1
Intelligenter Bürgerservice	VI 1.7
Internet der Dinge	VI 2.1
Internet of Things, IoT	VI 2.1
Internetforen	V 8
Pressefreiheit	V 8
Internetsuchmaschine	V 1. 1.1
iOS	VI 1.2
IP-Adressen	IV 1.1
IP-Kommunikation	VI 1.1
iTunes	VI 1.2

J

JI-Richtlinie	I 3
Jugendhilfeplanung	II 2.3
JUS-IT	II 2.2, II 2.1
Justizvollzugsanstalten	IV 4.2

K

Kameradrohnen	VII 1.2
Kennzeichenerkennungssystem	VII 2.1
Kilometerstand	VIII 3.3
Kindertagesstätte	VII 2.4
Kirchensteuerabzugsverfahren	VIII. 2.3
Kirchensteuergesetz	VIII. 2.3
Kita-Gutschein	VI 1.7
Konferenz der Datenschutzbeauftragten des Bundes und der Länder	XI 5
Kontoabrufverfahren	II 2.5
KoPers	IX 2.1
Kraftfahrzeug	VIII 3.3
Krankenversicherung	VIII 3.1
Kreditinstitut	VIII 1.8
Kreditwesen	VIII. 1.

L

Landesamt für Verfassungsschutz (LfV)	IV 2.2, IV 2.1
Landesbetrieb Verkehr	VI 1.4
Landesinformationssystem	IV 7.2
Landeskriminalamt Hamburg (LKA)	IV 1.8, IV 1.4
Landesverfassung	I 2.3

Längsschnittuntersuchungen III 1.1
Lernplattform III 1.4
Lichtbilder IV 1.10
Löschfristen für die Hilfsmerkmale IV 7.1

M

MAC-Adresse VI 2.2, V 9
Mandantenfähiges Verfahren IV 5.1
Mandantenfähigkeit VI 1.6, VI 1.5
Marktortprinzip I 3
MDK Nord II 1.5, II 1.4
Medienkompetenztage III 1.5
Medienprivileg V 10, V 8
Meldebehörde IV 5.2, IV 5.1
Meldedatenübermittlungsverordnung IV 5.1
Meldepflicht XI 4
Meldepflicht nach § 42a BDSG XI 3
Melderegister IV 5.2
Memorandum of Understanding (MoU) VI 2.4, VI 2.1
Mieterdaten VI 2.6
Mieterdatenverarbeitung VI 2.7
Mindestlohn IX 1.2
Mitarbeiterüberwachung IX 1.1

N

N/ITB IV 6.1
Nachrichtendienstliches Informationssystem (NADIS) IV 2.1
National Single Window II 1.6
Neukundenkreditprüfung VIII. 1.4
NFC-Chips VIII 1.7
NGN VI 1.1
Notare IV 1.4

O

Obachtverfahren – Gewalt unter 21 Jahren VI 1.6, VI 1.4
Offenlegung des Leistungsbezuges II 2.6
Öffentlicher Gesundheitsdienst II 1.1
Öffentlicher Raum V 9
Öffentlichkeitsarbeit XI 5
Öffentlichkeitsfahndung IV 1.6
One-Stop-Shop I 3
Online-Auswertung III 1.3
Online-Dating V 11

Online-Lernplattform	III 1.4
Online-Übertragungen	IV 8.1
Open Library	VII 2.2
OpenSSL	V 13
Ordnungswidrigkeit	IV 1.10
Orientierungshilfe Apps	V 4
Orientierungshilfe Smart-TV	V 17
Ortung	V 9
Ortungssysteme	IX 1.1

P

Panoramaaufnahmen	V. 16.
Pariser Anschläge	X 2
Parkhäuser	VII 2.1
Partnerbörsen	V 11
Partnerschaftsvermittlung	V 11
Personalausweis	IV 1.9
Personelle Ressourcen	I 4.2
Personenstandswesen	IV 6.1
Play-Store	VI 1.2
Polizei	VII 2.5, VI 1.6, VI 1.4, IV 1.11, IV 1.8, IV 1.4, IV 1.2
Polizei Hamburg	IV 1.10, IV 1.6
Polizeidatenverarbeitungsgesetz (PolDVG)	IV 1.10
Polizeidienststellen	IV 1.6
Polizeilicher Informations- und Analyseverbund (PIAV)	IV 1.11
Polizeiliches Auskunftssystem (POLAS)	IV 1.10
Predictive policing	IV 1.13
Presseanfragen	XI 5
Pressearchiv	V 7
Privacy Impact Assessment	VIII 1.7
Profilbildung	V 11
Profile	V 10
Projekt smartPORT	VI 2.4
Protokollauswertung	II 1.7
Protokolldaten	VIII 1.8
Prüfung des Abrufverfahrens aus dem Melderegister	IV 5.2

R

Realofferte	VI 2.6
Rechen- und Dienstleistungszentrum zur Telekommunikationsüberwachung (RDZ -TKÜ Nord)	IV 1.8

Recht auf Vergessen V 6
Recht auf Vergessenwerden V 1. 1.1
Rechtsanwältinnen und Rechtsanwälte IV 4.2
Rechtsaufsichtliche Kontrolle I 2.1
Reisepass IV 1.9
Reisezeitermittlung VI 2.2, V 2.2
Religionszugehörigkeit IV 5.1
Richtlinie 95/46 I 2.1
Rights Management System (RMS) VI 1.4, VI 1.1
RMS (Rights Management System) VI 1.4, VI 1.1

S

Safe Harbor X. 1., V 5
Safe Harbor-Entscheidung I 1
SAP VIII 2.1
Schülerdaten III 1.2
Schutzbedarf bei melderechtlichen Auskunftssperren IV 5.1
Scoring VIII 1.6, VIII. 1.1
Sharepoint VI 1.6
Smart City VI 2.1, VI 1.7
Smartbox VI 1.7
Smartphones III 1.4
smartPORT energy VI 2.4
smartPORT logistics VI 2.4
Smart-TV V 17, V 4
Sozialdaten II 2.4, II 1.4
Soziale Netzwerke IV 1.6
Sozialräumliche Hilfen und Angebote II 2.3
Sperrvermerk VIII. 2.3
Spiegelmelderegister IV 5.1
Sportinformationen V 10
Sportler V 10
Staatsangehörigkeit IV 5.1
Stadien VIII 1.7
Stammdatensicht II 2.2
Standesamt IV 6.2
Standortdaten V 9
Statistik IV 7.1
Statistikamt Nord IV 7.1
Statistisches Amt für Hamburg und Schleswig-Holstein IV 7.2
Strafprozessordnung (StPO) IV 1.4
Strafrechtsausschuss der Konferenz der Justizministerinnen und Justizministerinnen sowie Justizsenatorinnen und

Justizsenatoren (JuMiKo) IV 1.6
Straftäterinnen und Straftäter IV 1.6
Strafverfolgungsbehörden IV 1.6
Straßenpanoramaaufnahmen V. 16.
Straßenpanoramadienste V. 14
Suchmaschine V 6, V 1. 1.1

T

Tachostand VIII 3.3
Telekommunikationsdaten IV 1.1
Telekommunikationsgesetz (TKG). IV 1.1
Telekommunikationsüberwachung IV 1.8
TLS V 3
Tracking V 17, V 9
Transport Layer Security (TLS) VI 1.4
Transportverschlüsselung VI 1.4
Trilog I 3, Vorwort

U

Übermittlung von Passagierdaten X. 3.
Überwachung V 9
Überwachungskapitalismus Vorwort
UKE II 1.7, II 1.3, II 1.2
Umkleidebereiche VII 2.3
Universität III 2.1
Unterarbeitsgruppe Geodaten V. 14
Unterlassungsklagengesetz VIII 5.
Unterrichtsmaterial III 1.5

V

VDV-Kernappplikation VI 2.3
Verdeckte Datenerhebung IV 1.5
Verdeckte/r Ermittler/in IV 1.5
Verfassungsfeindliche Bestrebungen IV 2.1
Verfassungsgemäßheit des ZensG2011 IV 7.1
Verfassungsschutz IV 2.2
Verhältnismäßigkeitsgrundsatz IV 1.6
Verkehrsdaten IV 1.1
Verkehrsmittel VII 1.2
Verkehrsordnungswidrigkeitenverfahren IV 1.10
Verkehrsunfall VIII 3.3
Vermieter VI 2.6
Veröffentlichung im Internet III 1.2
Versandhändler VIII. 1.4

Versandhaus	VIII 4.1
Verschlüsselung	VI 1.1, V 13, III 1.3, II 2.4, II 1.5
Versicherungsbetrug	VIII 3.1
Versicherungsmakler	VIII 3.2
Versorgungsvertrag	VI 2.6
Vertragsverletzungsverfahren	I 2.1
Videokonferenzsystem	VI 1.1
Videoüberwachung	VII 2.5, VII 2.4, VII 2.3, VII 2.2, VII 1.2, VII 1.1
Voice over IP	VI 1.1
Volkszählung Zensus 2011	IV 7.1
Völlige Unabhängigkeit	I 2.1
Vorabwiderspruchsrecht	V. 14
Vorratsdatenspeicherung	VDS IV 1.1

W

Warndatei Elektronisches Lastschriftverfahren	VIII. 1.5
Warndatei im Versandhandel	VIII. 1.4
Webcam	VII 1.1
Wellnessanlagen	VII 2.3
Weltweiter Jahresumsatz	I 3
Werbeschreiben	VIII 4.1
Wettkampfdaten	III 1.2
WhatsApp	VI 1.2, V 2.3, I 3
WLAN	V 9, V 7

X

Xing	
Nutzungsdaten	V 3
TLS	V 3

Z

Zahlen - Fakten - Defizite - Lösungen	Anhang
Zensus 2011	IV 7.1
Zentraler Meldebestand	IV 5.1
Zertifizierung	I 4

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: Axel Caro
Layout: Kameko Design, Inga Below
Druck: print74