Landtag von Sachsen-Anhalt

Drucksache 6/3512
15.10.2014

Unterrichtung

Chef der Staatskanzlei Magdeburg, 1. Oktober 2014

Stellungnahme der Landesregierung zum XI. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz für die Zeit vom 1. April 2011 bis 31. März 2013 (Drs. 6/2602)

Sehr geehrter Herr Präsident,

als Anlage übersende ich gemäß § 22 Abs. 4a Satz 2 des Gesetzes zum Schutz personenbezogener Daten der Bürger (DSG-LSA) die

> Stellungnahme der Landesregierung zum XI. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz für die Zeit vom 1. April 2011 bis 31. März 2013 (Drs. 6/2602)

mit der Bitte um Kenntnisnahme.

Mit freundlichen Grüßen

In Vertretung

Olmes

Verfügung des Präsidenten des Landtages von Sachsen-Anhalt:

Die Unterrichtung des Landtages erfolgt gemäß § 54 Abs. 1 der Geschäftsordnung des Landtages (GO.LT).

Gemäß § 40 Abs. 1 überweise ich den Tätigkeitsbericht zur Beratung und zur Berichterstattung an die Ausschüsse für Inneres und Sport (federführend), für Recht, Verfassung und Gleichstellung, für Bundes- und Europaangelegenheiten sowie Medien, für Wissenschaft und Wirtschaft, für Bildung und Kultur, für Arbeit und Soziales, für Landesentwicklung und Verkehr, für Finanzen, für Petitionen sowie an den Ältestenrat.

Hinweis: *Die Drucksache steht vollständig digital im Internet/Intranet zur Verfügung. Die Anlage ist in Word als Objekt beigefügt und öffnet durch Doppelklick den Acrobat Reader.*
Bei Bedarf kann Einsichtnahme in der Bibliothek des Landtages von Sachsen-Anhalt erfolgen oder die gedruckte Form abgefordert werden.

(Ausgegeben am 15.10.2014)

Stellungnahme der Landesregierung zum XI. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz für die Zeit vom 1. April 2011 bis 31. März 2013 (Drs. 6/2602)

Gliederung

Abkürzungsverzeichnis

AK	Arbeitskreis
AO	Abgabenordnung
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BR-Drs.	Bundesrats-Drucksache
BMG	Bundesmeldegesetz
BSI	Bundesamt für die Sicherheit in der Informationstechnik
BT-Drs.	Bundestags-Drucksache
BVA	Bundesverwaltungsamt
BYOD	bring your own device
bzw.	beziehungsweise
CIO	Chief Information Officer
Drs.	Drucksache
DSG LSA	Datenschutzgesetz Sachsen-Anhalt
eID	Elektronische Identifizierung
EU	Europäische Union
EuGH	Europäischer Gerichtshof
ff.	fortfolgende
FFOG	Feld- und Forstordnungsgesetz
FIM	Föderales Informationsmanagement
GG	Grundgesetz für die Bundesrepublik Deutschland
GIAZ ……..	Gemeinsames Informations- und Auswertungszentrum islamistischer Terrorismus
GO LSA	Gemeindeordnung Sachsen-Anhalt
GVBl. LSA	Gesetz- und Verordnungsblatt des Landes Sachsen-Anhalt
Hrsg.	Herausgeber
HVAG	Hallesche Verkehrs-AG
IKT	Informations- und Kommunikationstechnologie
IP	Internet Protocol
IPv6	Internet Protocol Version 6
IT…….....	Informationstechnik
IT-PLR	IT-Planungsrat
ITN-LSA	Informationstechnisches Netz Sachsen-Anhalt
ITN-XT ……..	Informationstechnisches Netz Sachsen-Anhalt - XT
JVA	Justizvollzugsanstalt
KOM	Europäische Kommission (Drucksache)

LBG LSA	Beamtengesetz des Landes Sachsen -Anhalt
Leika	Leistungskatalog der öffentlichen Verwaltung
LISA	Landesinstitut für Schulqualität und Lehrerbildung
LKO LSA	Landkreisordnung für das Land Sachsen-Anhalt
LL IS	Leitlinie Informationssicherheit
LJagdG	Landesjagdgesetz für Sachsen-Anhalt
LPSA	Landesportal Sachsen-Anhalt
LT-Drs.	Landtagsdrucksache
MBl. LSA	Ministerialblatt des Landes Sachsen-Anhalt
MG LSA	Meldegesetz des Landes Sachsen-Anhalt
MVB	Magdeburger Verkehrsbetriebe
NASA	Nahverkehrsservice Sachsen-Anhalt GmbH
nPA	neuer Personalausweis
Nr.	Nummer
NWR	Nationales Waffenregister
NWRG-DV	Verordnung zur Durchführung des Nationalen-Waffenregister-Gesetzes
ÖPNV	Öffentlicher Personennahverkehr
PPP	Private Public Partnership
PVS	Personalvermittlungsstelle
RdErl.	Runderlass
Rn.	Randnummer
S.	Seite
SALSA	Secure Access - Land Sachsen-Anhalt
StGB	Strafgesetzbuch
SOG LSA	Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt
TB	Tätigkeitsbericht
u.a.	unter anderem
vgl.	vergleiche
z.B.	zum Beispiel
ZensAG LSA .	Ausführungsgesetz des Landes Sachsen-Anhalt zum Zensusgesetz 2011
ZMDB	Zentraler Meldebestand auf Landesebene

Vorbemerkung

Die Landesregierung nimmt zum XI. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz (im Folgenden: Landesbeauftragter) gemäß § 22 Abs. 4a Satz 2 des Gesetzes zum Schutz personenbezogener Daten der Bürger (Datenschutzgesetz Sachsen-Anhalt - DSG LSA) Stellung.

Der Landesbeauftragte zeigt in seinem Tätigkeitsbericht in bewährter Form gangbare Wege auf, zu einem angemessenen Ausgleich zwischen der wirksamen Erfüllung staatlicher Aufgaben und der Wahrnehmung der Persönlichkeits- und Freiheitsrechte zu kommen. Die Landesregierung und die verantwortlichen Stellen in der Landesverwaltung sind sich angesichts der sich immer schneller fortentwickelnden Verarbeitungs- und Verknüpfungsmöglichkeiten von personenbezogenen und sonstigen Daten der Bedeutung des Datenschutzes bewusst.

Die Landesregierung dankt dem Landesbeauftragten für die geleistete Arbeit und die konstruktive Zusammenarbeit. Die Landesregierung wird im Rahmen der Fortentwicklung des Datenschutzrechts und der Klärung von Rechtsfragen auch künftig den besonderen Sachverstand des Landesbeauftragten nutzen.

Eine Befassung mit den Ausführungen des Landesbeauftragten erfolgt insbesondere zu denjenigen Themen, bei denen auf aktuelle Entwicklungen im Recht oder in der Praxis einzugehen ist, bei denen eine Positionsbestimmung der Landesregierung noch ausstand oder bei denen zwischen dem Landesbeauftragten und der Landesregierung Auffassungsunterschiede bestehen. Verzichtet wird generell auf Ausführungen zu Punkten, die der Landesbeauftragte abschließend dargestellt hat und bei denen erkennbar kein Anlass für ergänzende Äußerungen oder weitere Handlungen der Landesregierung oder der betroffenen öffentlichen Stellen besteht. Sofern nur zu einzelnen Punkten einer Gliederungsnummer eine Stellungnahme erfolgt ist, wurde dies durch eine unterstrichene Zwischenüberschrift hervorgehoben. Sofern zu einzelnen Punkten nichts ausgeführt wurde, sind die Anmerkungen des Landesbeauftragten zur Kenntnis genommen worden. Im Hinblick auf die Ausführungen zu Nr. 8 werden die Ausführungen des Landesbeauftragten für den Berichtszeitraum geteilt.

Soweit nachfolgend nicht ausdrücklich etwas anderes erwähnt ist (etwa bei den Ausführungen zu Nrn. 3.1.1, 3.1.5), bezieht sich die Stellungnahme auch im Hinblick auf laufende Vorhaben ausschließlich auf den Berichtszeitraum. Aus Achtung vor den

Parlamenten unterbleibt grundsätzlich eine Auseinandersetzung mit kritischen Aussagen des Landesbeauftragten zu bereits verabschiedeten Bundes- oder Landesgesetzen.

Hinsichtlich der zahlreichen Abkürzungen wird auf das Abkürzungsverzeichnis (S. 4, 5) verwiesen. Für das unmittelbare Textverständnis erforderliche Abkürzungen werden darüber hinaus im Kontext noch einmal erläutert.

Zu 1. Entwicklung und Situation des Datenschutzes

Im Berichtszeitraum gab es im Bereich der Informations- und Kommunikationstechnologie (IKT) der Landesverwaltung einige Veränderungen. Mit dem Beschluss der Landesregierung vom 3. Mai 2011 über den Aufbau der Landesregierung und die Abgrenzung der Geschäftsbereiche sind die Aufgaben der Informations- und Kommunikationstechnologie vollständig in die Zuständigkeit des Ministeriums der Finanzen übergegangen. Seitdem erfolgt die Vertretung des Landes Sachsen-Anhalt im IT-Planungsrat (IT-PLR) durch den dafür zuständigen Staatssekretär des Ministeriums der Finanzen.

Des Weiteren wurde im Ministerium der Finanzen die Funktion eines Beauftragten der Landesregierung für Informationstechnik (Chief Information Officer - CIO) eingerichtet. Diesem wurde ein neues Gremium, der IKT-Rat, zur Seite gestellt, dessen Aufgabe darin besteht, die strategischen Entscheidungen für die Landesverwaltung zu treffen. In ihm wirken die Staatssekretärinnen und Staatssekretäre mit.

Zur weiteren Unterstützung des IKT-Rates, insbesondere zur fachlichen Vorbereitung der Sitzungen des IT-Planungsrates wurde als zusätzliches Gremium der IKT-Kreis gebildet. In beiden Gremien wirkt der Landesbeauftragte neben Vertretern der kommunalen Spitzenverbände als beratendes Mitglied mit.

Mit der Bündelung der Aufgaben der Informations- und Kommunikationstechnik im Finanzministerium (Zusammenführung der IT-Strategie mit der E-Government-Strategie), einhergehend mit der Neustrukturierung der Gremien, zeigt das Land, dass es dem Thema Informations- und Kommunikationstechnik insbesondere unter Berücksichtigung des immer stärker zu berücksichtigenden demographischen Wandels, des Datenschutzes und der Datensicherheit eine besondere Gewichtung beimisst.

Da die Erfahrungen der letzten Jahre gezeigt haben, dass Belange des Datenschutzes und der Datensicherheit nicht erst bei der tatsächlichen Realisierung der einzelnen E-Government-Projekte berücksichtigt, sondern bereits bei den strategischen Überlegungen und Zielsetzungen für solche Projekte bedacht werden müssen, wird der Landesbeauftragte über diese Gremien frühzeitig mit einbezogen und die bisher gute Zusammenarbeit fortgeführt.

Zu 1.1 Sicherheit und Freiheit

Im Hinblick auf die vom Landesbeauftragten angesprochenen Ausführungen im VIII. Tätigkeitsbericht zum Primat der Freiheit (Nr. 1.1), im IX. Tätigkeitsbericht zum Abwehrcharakter der Grundrechte (Nr. 1.1) und im X. Tätigkeitsbericht zur Überwachungs-Gesamtrechnung (Nr. 1.1) verweist die Landesregierung auf ihre Stellungnahmen zu den jeweiligen Tätigkeitsberichten (X. TB: LT-Drs. 6/997, IX. TB: LT-Drs. 5/2385, VIII. TB: LT-Drs. 5/1097, jeweils zu Nr. 1.1). Diese gelten unverändert fort.

Zu 1.2 Nicht-öffentlicher Bereich

Verbraucherschutz

Die Landesregierung dankt dem Landesbeauftragten für die Teilnahme an der Beratung der interministeriellen Arbeitsgruppe zum Verbraucherschutz und den konstruktiven Austausch auf dieser Ebene. Sie ist der Auffassung, dass der begonnene Dialog im Interesse einer Weiterentwicklung des Verbraucherdatenschutzes fortgesetzt werden soll. Ein erstes gemeinsames Projekt ist derzeit bereits in Vorbereitung. Hinsichtlich der Abmahnfähigkeit von Datenschutzverstößen begrüßt die Landesregierung die im Koalitionsvertrag auf Bundesebene vorgesehene ausdrückliche gesetzliche Ermächtigung der Verbraucherverbände zur Abmahnung derartiger Rechtsverstöße.

Zu 1.3 Informations- und Kommunikationstechnologie – Big Data

Big Data steht als Synonym für riesige Datensammlungen, die aus frei zugänglichen Quellen wie dem Internet und Archiven, Unternehmens- und Behördendaten sowie Personendaten gespeist werden. Die gesammelten Daten werden sodann mit speziellen Methoden und Technologien ausgewertet und bewertet. Größere Datensammlungen befinden sich im

Zuständigkeitsbereich der Landesregierung nur in den Rechenzentren. Alle Daten wurden auf gesetzlicher Grundlage erhoben und auch Verknüpfungen finden nur auf Grund einer gesetzlichen Grundlage statt. Daran wird auch der Beitritt des Landes zu Dataport (vgl. Nr. 4.4) nichts ändern.

Zu 2. Der Landesbeauftragte

Zu 2.2 Schwerpunkte – Empfehlungen

Die Landesregierung dankt dem Landesbeauftragten für seine Empfehlungen und nimmt sie zur Kenntnis. Soweit sich aus den Empfehlungen die Notwendigkeit ergänzender Äußerungen oder weitere Handlungen der Landesregierung oder der betroffenen öffentlichen Stellen ergeben sollten, nimmt die Landesregierung dazu – wie bereits in der Vorbemerkung angemerkt - zur Vermeidung von Wiederholungen jeweils zu den vom Landesbeauftragten aufgeführten Gliederungspunkten Stellung.

Zu 3. Nationales und internationales Datenschutzrecht

Zu 3.1.1 Europäisches Recht

<u>Datenschutz-Grundverordnung</u>

Der am 25. Januar 2012 von der Europäischen Kommission vorgestellte Entwurf einer Datenschutz-Grundverordnung (BR-Drs. 52/12) und ein Vorschlag für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (BR-Drs. 51/12) sind im Juni 2013 im Rat der Europäischen Union zunächst gescheitert. Hintergrund waren zahlreiche, sehr unterschiedlich motivierte Bedenken unter anderem der Vertreter Deutschlands, Großbritanniens und Frankreichs. Die vor der Sommerpause 2013 avisierte Positionierung konnten damit sowohl Rat als auch Parlament nicht leisten. Am 21. Oktober 2013 hat sich das Europäische Parlament auf einen Entwurf für eine Änderung der von der Europäischen Kommission am 25. Januar 2012 vorgelegten Entwürfe geeinigt. Hierzu hat der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres am 21. November 2013 berichtet. Überdies wurde das Einigungsergebnis mehrfach im Rat der Europäischen Union erörtert. Zuletzt hat das Europäische Parlament auf Grundlage des Berichtes des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres am 12. März 2014 eine legislative

Entschließung gefasst. Die Verhandlungen zwischen Rat und Parlament dauern an. Der Bundesrat hat sich zuletzt am 23. Mai 2014 anlässlich der Mitteilung der Europäischen Kommission mit dem Titel „Ein offenes und sicheres Europa – Praktische Umsetzung“ (KOM(2014) 154) zur Reform des Europäischen Datenschutzrechts positioniert. In dem zu zu dieser Mitteilung verabschiedeten Beschluss (BR-Drs. 123/14) bedauert der Bundesrat unter Hinweis auf seine bisherigen Stellungnahmen im Verfahren, dass die Kommission in der Mitteilung die weitere Entwicklung des europäischen Datenschutzrechts nicht in den Blick genommen habe.

Zu 3.1.2 Beschäftigtendatenschutz

Im Rahmen der Novellierung des DSG LSA (vgl. 3.1.5) wurde davon abgesehen, den Beschäftigtendatenschutz für Angehörige des öffentlichen Dienstes im Lande grundlegend neu zu regeln. Der allgemeine Beschäftigtendatenschutz ist für nicht beamtete Beschäftigte der unmittelbaren und mittelbaren Landesverwaltung in § 28 DSG LSA und den in Bezug genommenen §§ 84 bis 91 des Landesbeamtengesetzes gegenwärtig umfassender geregelt als für entsprechende Bundesbedienstete in § 32 Bundesdatenschutzgesetz (BDSG). Zwar hat die Bundesregierung bereits im Jahre 2010 den Entwurf eines Gesetzes zur Neuregelung des Beschäftigtendatenschutzes (BT-Drs. 17/4230) vorgelegt, zu dem auch der Bundesrat eingehend Stellung genommen hatte. Da vor allem die Regelungen zur Videoüberwachung strittig geblieben sind, wurde im Februar 2013 entschieden, dieses Gesetzesvorhaben in der 17. Legislaturperiode des Deutschen Bundestages nicht zum Abschluss zu bringen. Es bleibt abzuwarten, ob die Pläne zur Neuregelung des Arbeitnehmerdatenschutzes in der 18. Legislaturperiode des Bundestages wieder aufgegriffen werden.

Zu 3.1.5 Novellierung DSG LSA 2013

Mit der letzten Änderung des Datenschutzgesetzes Sachsen-Anhalt im Jahr 2011 wurde dem Landesbeauftragten ab dem 1. Oktober 2011 auch die Aufgabe der Datenschutzkontrolle im nicht-öffentlichen Bereich übertragen. Mit einer zu diesem Gesetz angenommenen Entschließung vom 8. September 2011 (LT-Drs. 6/388) hat der Landtag die Landesregierung aufgefordert, einen Gesetzentwurf zur Änderung des Landesdatenschutzgesetzes vorzulegen. Damit sollte die nötige Anpassung der landesgesetzlichen Regelungen im Datenschutz an den Stand von Wissenschaft und

Technik gewährleistet und dem Bedürfnis der Bürgerinnen und Bürger nach mehr Transparenz und einer Stärkung des Rechts auf informationelle Selbstbestimmung Rechnung getragen werden.

Der von der Landesregierung in ihrer Sitzung am 10. Juni 2014 beschlossene und am 11. Juni 2014 in den Landtag eingebrachte Gesetzentwurf (LT-Drs. 6/3186) sieht im Hinblick auf die Vorgaben des Landtags zum Schutz sogenannter „Whistleblower“ ein Jedermann-Anrufungsrecht, also ein Recht auf Anrufung des Landesbeauftragten auch in fremden Angelegenheiten, vor. Ergänzt wird dieses Recht durch eine Pflicht zur Information des Landesbeauftragten und der Betroffenen bei Datenpannen. Darüber hinaus werden bei der Auftragsdatenverarbeitung erhöhte Anforderungen an die dafür zu treffende Festlegungen und deren Kontrolle eingeführt. Damit entspricht die Rechtslage in Sachsen-Anhalt zukünftig wieder derjenigen nach dem Bundesdatenschutzgesetz. Im Übrigen wird die Rechtsstellung von Beauftragten für den Datenschutz im Sinne des Gesetzes verbessert, indem deren Einsetzung nur aus „wichtigem Grund“ nach § 626 des Bürgerlichen Gesetzbuchs (BGB) widerrufen werden kann.

Ergänzend bestimmt der Entwurf die Anwendbarkeit der Regelungen des Gendiagnostikgesetzes des Bundes für Beschäftigte des Landes Sachsen-Anhalt, die in einem öffentlich-rechtlichen Dienst- oder Ausbildungsverhältnissen stehen, und trifft eine Regelung zur Wildbeobachtung in optisch-elektronischen Verfahren (vgl. auch Nr. 4.17.6).

Der Gesetzentwurf wurde gemeinsam mit dem Landesbeauftragen erarbeitet und von der Landesregierung am 15. April 2014 zur Anhörung freigegeben. Die Anhörungsfrist endete am 15. Mai 2014.

Gelegenheit zur Stellungnahme hatten der Landesbeauftragte für den Datenschutz, der Städte- und Gemeindebund Sachsen-Anhalt, der Landkreistag Sachsen-Anhalt, der Deutsche Gewerkschaftsbund Sachsen-Anhalt, der Deutsche Beamtenbund und Tarifunion Sachsen-Anhalt, der Präsident des Oberlandesgerichts, der Präsident des Oberverwaltungsgerichts, der Generalstaatsanwalt, die Rechtsanwaltskammer Sachsen-Anhalt, die Notarkammer Sachsen-Anhalt und der Bund der öffentlich bestellten Vermessungsingenieure. Inhaltlich nicht geäußert haben sich der Deutsche Gewerkschaftsbund Sachsen-Anhalt, der Präsident des Oberlandesgerichts, der Präsident des Oberverwaltungsgerichts, der Generalstaatsanwalt und die Rechtsanwaltskammer Sachsen-Anhalt.

Die Landesregierung hat im Vorblatt des Gesetzentwurfs zu den Positionen der Verbände Stellung genommen. Vor dem Hintergrund der Hinweise des Landesbeauftragten wurde auch die Regelung zur Wildbeobachtung noch einmal überarbeitet.

Ansonsten hat die Landesregierung den im Rahmen der Anhörung vorgetragenen Bedenken widersprochen. So hatten etwa die kommunalen Spitzenverbände alle vom Landtag unmittelbar geforderten Veränderungen abgelehnt.

zu 3.2.3 Flugpassagierdaten und Körperscanner

Zur Rechtsauffassung der Länder zum Vorschlag für eine Richtlinie des Europäischen Parlamentes und des Rates der Europäischen Union über die Verwendung von Fluggastdaten zu Zwecken der Verhütung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität wird auf die BR-Drs. 73/11 (Beschluss) verwiesen.

Zu 4. Technik, Organisation, Telekommunikation und Medien

Zu 4.1 IT-Planungsrat

Der aktuelle Aktionsplan des IT-Planungsrates umfasst eine Vielzahl von Projekten und Anwendungen, die laufend fortgeschrieben werden. Ein besonderes Augenmerk ist dabei auf das Steuerungsprojekt des IT-Planungsrates FIM (Aufbau eines föderalen Informationsmanagements) als auch auf die Anwendungen des IT-Planungsrates Leika (Leistungskatalog der öffentlichen Verwaltung) und den Behördenfinder zu richten, deren Weiterentwicklung insbesondere vom Land Sachsen-Anhalt vorangetrieben werden.

Über das Steuerungsprojekt des IT-Planungsrates FIM wurde der Landesbeauftragte frühzeitig in Vorbereitung der IT-Planungsratssitzungen über die Gremien des IKT-Kreises und des IKT-Rates informiert. Die Federführung für dieses Projekt tragen der Bund und das Land Sachsen-Anhalt.

Wesentlicher Ausgangspunkt für das Projekt sind die positiven Erfahrungen aus der Zusammenarbeit von Bund und Ländern bei der Erarbeitung des Leika. Sachsen-Anhalt war

federführend für die Analysen zur Vereinheitlichung von Informationen und deren Auswertung verantwortlich. Die Geschäfts- und Koordinierungsstelle Leika ist im Ministerium der Finanzen des Landes Sachsen-Anhalt angesiedelt.

Der Leika ist nunmehr eine Anwendung des IT-Planungsrates und bildet die Grundlage für ein föderales Stammtextmanagement. Zusätzlich wurden Qualitätsmerkmale für eine leicht lesbare Leistungsbeschreibung definiert. Damit sind die Stammtexte im besonderen Maße für die telefonische Auskunft (115-Service) und den Behördenfinder Deutschland nutzbar, dessen Betrieb von der im Finanzministerium des Landes Sachsen-Anhalt angesiedelten Geschäfts- und Koordinierungsstelle gewährleistet wird.

In der Folge entstand für die öffentliche Verwaltung ein Standardisierungsrahmen, der nahezu analog auf Formulare und Prozesse angewandt werden kann. Der Wert der Informationen ist heute unumstritten. Die Verwaltung wandelt sich immer mehr zum Dienstleister. Der Bedarf an standardisierten Informationen wächst zunehmend. Genau hier setzt das Projekt FIM an.

Mit fachlichen und technischen Standards soll ein Informationsmanagement aufgebaut werden, das alle föderalen Ebenen beim Informationsaustausch untereinander und mit den Bürgern im Verwaltungsverfahren unterstützt.

Wesentlich für ein Verwaltungsverfahren sind die Leistungsbeschreibung (Informationen über die Leistungen der öffentlichen Verwaltung), das Formular sowie der Prozess (innerhalb der Verwaltung wird durch den Antrag über ein Formular eine Leistung initiiert, an deren Ende in der Regel ein Bescheid zugestellt wird).

Ziel von FIM ist es, diese drei Bausteine in enger Kooperation mit den Vorhaben Leika und Nationale Prozessbibliothek (ein Koordinierungsprojekt des IT-Planungsrates) zu harmonisieren und zu verzahnen.

Gerade wegen der Komplexität dieses Steuerungsprojektes erfolgt die frühzeitige Einbeziehung des Landesbeauftragten über die Gremien.

Mit der Geschäfts- und Koordinierungsstelle Leika, der Geschäfts- und Koordinierungsstelle für den Behördenfinder und der Federführung für das Projekt FIM im Ministerium der

Finanzen des Landes Sachsen-Anhalt, besitzt das Land die Chance, das E-Government-Thema „Standardisierung“ entscheidend voranzubringen.

Zu 4.2 E-Government und IKT-Strategie in Sachsen-Anhalt

Auch in Zukunft werden Fragen des E-Government einen Schwerpunkt in der Zusammenarbeit der Kommunen und des Landes bilden. Ob es erforderlich ist, für Sachsen-Anhalt mit einem E-Government-Gesetz eine besondere gesetzliche Grundlage zu schaffen, ist noch nicht abschließend entschieden. Die Umsetzung des am 1. August 2013 in Kraft getretenen E-Government-Gesetzes des Bundes wird unter anderem Gegenstand eines Workshops im Ministerium für Inneres und Sport im September 2014 sein.

Zu 4.3 Leitlinie für Informationssicherheit und eID-Strategie

Im Zusammenhang mit der eID-Strategie hat der IT-Planungsrat in seiner Sitzung am 2. Oktober 2013 beschlossen, bei der Umsetzung der Maßnahmen die Erfordernisse des Datenschutzes besonders zu berücksichtigen. Hierzu sollen u.a. Handreichungen zum vereinfachten Einsatz von Vertrauensdiensten für Verwaltung, Bürgerinnen und Bürger, Unternehmen sowie für den datenschutzgerechten Einsatz von Bürgerkonten erarbeitet werden.

Zur Umsetzung der Maßnahmen der IT-Strategie und unter Berücksichtigung der Ausrichtung auf eine umfassende Informationssicherheit wurde in einer Arbeitsgruppe unter Beteiligung des Landesbeauftragten der Entwurf einer Landesleitlinie Informationssicherheit (LL IS) erarbeitet. Aufgrund der aktuellen Gefährdungslage hat der IT-Planungsrat am 8. März 2013 überdies eine verbindliche Leitlinie für Informationssicherheit für Bund und Länder beschlossen. Vor diesem Hintergrund wird die LL IS an den Vorgaben ausgerichtet werden, die Integration von Datenschutz und Datensicherheit soll dabei erhalten bleiben.

Die Umsetzungsplanung zur Leitlinie für Informationssicherheit für Bund und Länder (IT-PLR) sieht für die Verabschiedung der jeweiligen verbindlichen Leitlinie für Informationssicherheit in den Ländern einen Zeitraum von fünf Jahren vor und damit bis 2018 vor. Eine Beschlussfassung der Landesregierung wird aber für 2014 angestrebt. Bis 2018 sollen alle wesentlichen Vorbereitungen abgeschlossen sein und die Einführung eines Informationssicherheitsmanagements begonnen werden.

Zu 4.4 Zentraler IT-Dienstleister für Sachsen-Anhalt – Dataport

§ 15 Absatz 2d des Staatsvertrags zwischen dem Land Schleswig-Holstein, der Freien und Hansestadt Hamburg, dem Land Mecklenburg-Vorpommern, der Freien Hansestadt Bremen, dem Land Niedersachsen und dem Land Sachsen-Anhalt über den Beitritt des Landes Sachsen-Anhalt zur rechtsfähigen Anstalt des öffentlichen Rechts „Dataport“ bestimmt, dass der Landesbeauftragte Dataport in Fragen des Datenschutzes berät, soweit Dataport bzw. eine der Niederlassungen personenbezogene Daten für öffentliche Stellen des Landes Sachsen-Anhalt verarbeitet. Im Übrigen verweist die Vorschrift auf das DSG LSA sowie alle weiteren für öffentliche Stellen in Sachsen-Anhalt geltenden datenschutzrechtlichen Bestimmungen.

Zu 4.9 Mobile Computing – Datenschutz bei „Bring Your Own Device“

Zum Einsatz mobiler Endgeräte in der Landesverwaltung wurden und werden Sicherheit und Datenschutz betrachtet. Die Einbindung über Secure Access - Land Sachsen-Anhalt (SALSA) in das ITN-LSA kann in Verbindung mit administrativen Vorgaben eine Nutzungsmöglichkeit darstellen. Auch in den Gremien des IT-PLR werden Maßnahmen für den Umgang mit mobilen Endgeräten diskutiert.

Aufgrund der Problematiken des sogenannten „bring your own device“ (BYOD) werden in Sachsen-Anhalt derzeit grundsätzlich keine private Endgeräte eingebunden Die Konzepte für mobile Endgeräte werden in den IKT-Gremien des Landes beraten und dort auch mit dem Landesbeauftragten abgestimmt.

Zu 4.10 IPv6

Der Landesbeauftragte geht zutreffend davon aus, dass sich die Landesverwaltung mit der Thematik befasst hat. Das IPv6-Rahmenadresskonzept für Sachsen-Anhalt wurde erstellt und nach Abstimmung mit den Ressorts und den Kommunen dem Bundesverwaltungsamt (BVA) vorgelegt. Parallel wurde ein Rechte- und Rollenkonzept erstellt, welches noch mit Dataport als neuem IT-Dienstleister abzustimmen ist. Im Zusammenhang mit dem Aufbau des ITN-XT wird ein Migrationskonzept unter Beachtung des „IPv6 Migrationsleitfadens“ des BVA zu erstellen sein. Eine Einbeziehung des umfangreichen Expertenwissens des Landesbeauftragten wird angestrebt.

Zu 4.11 Kontaktformular im Landesportal – Teil II

Der im Tätigkeitsbericht dargestellte Sachverhalt entspricht nur teilweise den tatsächlichen Gegebenheiten. Richtig ist, dass es im Hinblick auf die Gestaltung und die Handhabung des Kontaktformulars Modifizierungsbedarf gab.

Diese Notwendigkeit der Modifizierung griff die Staatskanzlei im Februar 2013 auf und beauftragte einen externen Dienstleister mit der Erarbeitung einer Alternativlösung. Am 30. April 2013 wurde ein entsprechendes Konzept zur Umstellung des Kontaktformulars dem Landesbeauftragten sowie der Portalleitung zur Prüfung übermittelt. Die Freigabe des Konzepts durch den Landesbeauftragten und die Aktivierung im Livesystem des Landesportals Sachsen-Anhalt (LPSA) erfolgte mit Wirkung vom 15. Juli 2013.

Am 19. Juli 2013, also keineswegs wenige Stunden nach der Inbetriebnahme, musste das neu eingestellte Kontaktformular wieder deaktiviert werden, da bedingt durch ein fehlendes Pflichtfeld zur Absendereingabe, bei einem Teil der eingegangenen Anfragen die Möglichkeit der Beantwortung nicht mehr gegeben war.

Dieser Sachverhalt wurde auch dem Landesbeauftragten mitgeteilt und gleichzeitig verabredet, in einer gemeinsamen Besprechung das Kontaktformular ergänzend zu optimieren.

Aufgrund der Urlaubszeit fand der Termin erst am 5. September 2013 statt. In Übereinstimmung mit dem Landesbeauftragten wurde das Kontaktformular entsprechend ergänzt und eine Einbindung in den Rubrikenpfad vorbereitet.

Die Aktivierung dieser überarbeiteten Fassung musste allerdings wegen des zwischenzeitlich aufgetretenen Sicherheitsvorfalls vom 28. August 2013 zurückgestellt werden. Das gesamte LPSA wurde aus Sicherheitsgründen auf einen statischen Betrieb umgestellt, der eine Nutzung derartiger Formulare ausschloss. Auch das war dem Landesbeauftragten bekannt.

Nutzeranfragen konnten in der Phase des statischen Betriebs nur über die Mailadresse der Online-Redaktion entgegengenommen werden.

Teile des LPSA und auch das Kontaktformular in der Fassung vom 15. Juli 2013 waren ab Anfang Oktober im Livesystem wieder verfügbar.

In einem sehr zeitaufwändigen Migrationsprozess wurde das gesamte LPSA in eine neue sichere Hard- und Softwareumgebung übertragen und mit Wirkung vom 5. März 2014 vom statischen Betrieb auf das Livesystem umgestellt. Damit waren auch die Voraussetzungen für die Nutzung des am 5. September 2013 überarbeiteten Kontaktformulars gegeben und eine Aktivierung erfolgte unmittelbar nach der Umschaltung des gesamten LPSA. Seit diesem Zeitpunkt ist das Kontaktformular uneingeschränkt nutzbar.

Zu 4.12 Rundfunkfinanzierung – Sachstand und Umsetzung

Der Landesbeauftragte kritisiert im Hinblick auf die Mustersatzung nach § 9 Abs. 2 Rundfunkbeitragsstaatsvertrag, dass sie wichtige datenschutzrechtliche Regelungen "anstelle eindeutiger und normenklarer Formulierungen im Staatsvertrag" enthalte. Diese Auffassung ist nicht nachzuvollziehen, da nach eigenen Angaben des Landesbeauftragten die Rundfunkdatenschutzbeauftragten und mehrere Landesdatenschutzbeauftragte an der Ausarbeitung der Mustersatzung beteiligt waren und schon deswegen davon auszugehen ist, dass ausreichend Möglichkeiten bestanden, "eindeutige und normenklare Formulierungen" zu entwickeln. Ferner gilt auch für Satzungen das verfassungsrechtliche Bestimmtheitsgebot, so dass nicht von einer materiell minderen Normenqualität ausgegangen werden kann. Schließlich ist zu berücksichtigen, dass eine Normierung in Form einer Satzung im Unterschied zu einem Staatsvertrag aller Länder erheblich mehr Flexibilität für eventuelle Anpassungen zulässt, was besonders angesichts der differenzierten Anforderungen des Datenschutzes von Bedeutung ist. Auch deswegen hatte der Gesetzgeber in diesem Fall die Satzungsermächtigung geschaffen.

Zu 4.17 Videoüberwachungen

Zu 4.17.6 Wildkameras

<u>Einsatz von Wildkameras durch nicht-öffentliche Stellen</u>

Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) und die Verarbeitung und Nutzung der durch eine solche Videoüberwachung erhobenen Daten ist nur unter den Voraussetzungen des § 6b BDSG zulässig. Bei Feld- und Waldgebieten handelt es sich um einen öffentlich zugänglichen Raum im Sinne dieser Vorschrift, da gem. § 3 Abs. 1 Feld- und Forstordnungsgesetz

(FFOG) jedem das Betreten von Feld und Wald zum Zwecke der Erholung gestattet ist. Wildkameras sind daher als Videoüberwachungsanlagen zu qualifizieren.

Eine Videoüberwachung kann nach § 6b Abs. 1 BDSG beispielsweise zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke zulässig sein. Voraussetzung ist allerdings, dass sie erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Dem Persönlichkeitsrecht des Betroffenen, z. B. eines Spaziergängers oder Wanderers, der von der Kamera aufgezeichnet wird, ist in diesem Zusammenhang ein hoher Stellenwert einzuräumen.

Nicht eindeutig geklärt ist in diesem Zusammenhang die Frage, ob der Einsatz hoch auflösender Kameras, die es auch erlauben, u. U. Personen zu identifizieren, für rein private jagdliche Beobachtungszwecke (z. B. an Kirrungen) erforderlich ist. Feld und Wald sind ein Bereich, welcher der Erholung der Menschen dient und in dem man sich unbeobachtet bewegen können sollte. Wildkameras sind daher in der Regel unzulässig, weil die berechtigten Interessen der Erholungssuchenden überwiegen.

Datenschutzrechtlich nicht relevant ist hingegen der Einsatz von Wildkameras, wenn ein Bereich erfasst wird, der von Personen nicht betreten werden darf. Dies ist zum Beispiel auf Truppenübungsplätzen und in Naturschutzgebiete außerhalb von Wegen der Fall.

Einsatz von Wildkameras durch öffentliche Stellen des Landes

Das durch optisch-elektronische Einrichtungen unterstützte Erfassen von Tierarten zu Zwecken der Bestandsüberwachung und Bestandsbewertung gehört mittlerweile zu einer gängigen und unverzichtbaren Methode der Wildforschung. In vielen Fällen ist sie zudem die einzige Methode, die kontinuierliche und verifizierbare Ergebnisse erbringt. Insbesondere im Hinblick auf die sich in Deutschland wieder ausbreitenden Großraubtiere, wie Luchs und Wolf, und das sich daraus ergebende Konfliktpotential ist die Anwendung einer kosten- und personal reduzierenden Methode unerlässlich. Aus Gründen der Rechtssicherheit ist daher die Einführung einer Rechtsgrundlage für die Verwendung solcher Geräte geboten. Eine nur im Einvernehmen mit dem Revierinhaber zulässige und auf Zwecke der Hege beschränkte Befugnis soll allen in § 38 Abs. 1 des Landesjagdgesetzes für Sachsen-Anhalt (LJagdG) aufgeführten Jagdbehörden erteilt werden. Die entsprechende Änderung des LJagdG ist in Artikel 2 des Entwurfs eines Dritten Gesetzes zur Änderung datenschutzrechtlicher Vorschriften (LT-Drs. 6/3186) vorgesehen (vgl. auch Nr. 3.1.5).

Zu 4.19 Soziale Netzwerke

Zu 4.19.1 Nutzung sozialer Netzwerke durch öffentliche Stellen

Wie vom Landesbeauftragten angemerkt, hat die Ständige Konferenz der Innenminister und -senatoren der Länder einen Bericht ihres Arbeitskreises I „Staatsrecht und Verwaltung“ vom 4. April 2012 zum Datenschutz in Sozialen Netzwerken zur Kenntnis genommen, der von der Konferenz der Chefs der Staats- und Senatskanzleien der Länder in Auftrag gegeben wurde. Vor dem Hintergrund der auch vom Landesbeauftragten im Tätigkeitsbericht dargestellten Problemfelder wurde zur Förderung der Belange des Datenschutzes darum gebeten

- über die aktuellen Entwicklungen zu berichten und
- unter Einbeziehung von Initiativen der Bundesregierung sowie der Ergebnisse der Konferenz der Datenschutzbeauftragten erste gemeinsame Vorschläge zu machen.

Der Bericht wurde von der Ständigen Konferenz der Innenminister und -senatoren der Länder ich ihrer Sitzung am 6. und 7. Dezember 2012 freigegeben. Es wurde beschlossen, den Bericht den Fachministerkonferenzen sowie den Datenschutzbeauftragten zur Verfügung zu stellen. Das Ministerium für Inneres und Sport hat den Bericht darüber hinaus innerhalb der Landesregierung umfassend gestreut. Alle Organisationsbereiche des Hauses sowie alle obersten Landesbehörden wurden in Kenntnis gesetzt. Der Bericht ist auch dieser Stellungnahme als Anlage beigefügt.

Zu 5. Öffentliche Sicherheit, Einwohner- und Ausländerwesen

Zu 5.3 Anti-Terror-Maßnahmen

<u>Antiterrordatei</u>

Das Landeskriminalamt (als speichernde Stelle) wurde anlässlich des Verlaufs der mündlichen Verhandlung zur Verfassungsbeschwerde zum Antiterrordateigesetz durch Erlass vom 20. November 2012 angewiesen sicherzustellen, dass alle personenbezogenen Daten, die ausschließlich aufgrund heimlicher Eingriffe in die nach Art. 10 oder 13 GG geschützten Grundrechte erhoben wurden, in der Antiterrordatei verdeckt gespeichert werden.

Des Weiteren wurde das Landeskriminalamt mit Erlass vom 2. Mai 2013 angewiesen, auch die sich aus dem Urteil des Bundesverfassungsgericht ergebenden übrigen Beschränkungen beim Umgang mit der Antiterrordatei zu beachten.

Gemeinsames Informations- und Auswertungszentrum islamistischer Terrorismus (GIAZ)
Im Hinblick auf die Bedenken des Landesbeauftragten verweist die Landesregierung zum einen auf Ihre bisherigen Äußerungen (vgl. LT-Drs 6/997, S. 38) und zum anderen auf die intensiven und konstruktiven Erörterungen zur Novellierung des GIAZ-Erlasses sowie der Neufassung der Verwaltungsvorschriften zur Datenübermittlung zwischen der Polizei und der Verfassungsschutzbehörde im Jahr 2014.

Zu 5.4 Risikomanagement für besonders rückfallgefährdete Sexualstraftäter

Der Landesbeauftragte wurde vor dem Erlass der in Rede stehenden Verwaltungsvorschrift (Gem. RdErl. des Ministeriums für Inneres und Sport, des Ministeriums für Justiz und Gleichstellung und des Ministeriums für Arbeit und Soziales vom 20. März 2013, MBl. LSA S. 207), die den Umgang mit personenbezogenen Daten betrifft, gemäß dem DSG LSA gehört. Die von ihm vorgetragenen Bedenken wurden umfassend geprüft und in dem aus Sicht der Landesregierung erforderlichen Umfang bei den verwaltungsinternen Regelungen berücksichtigt.

Hinsichtlich der Auffassung des Landesbeauftragten, dass der Umfang der Speicherung personenbezogener Daten der (automatisierten) Datei „Risikomanagement für besonders rückfallgefährdete Sexualstraftäter im Land Sachsen-Anhalt“ für die Aufgabenerledigung der Polizei nicht erforderlich ist, ist folgendes anzumerken: Der Landesbeauftragte ist vor Einrichtung des in Rede stehenden Abrufverfahrens unterrichtet worden. Seine Anregungen hierzu wurden umfassend - auch durch den behördlichen Datenschutzbeauftragten des Landeskriminalamts – geprüft. Der sich aus der Überprüfung ergebende Änderungsbedarf wurde berücksichtigt und im entsprechend Verfahrensverzeichnis dokumentiert. Es werden bei der Polizei nur die personenbezogenen Daten der Betroffenen gespeichert, die nach den §§ 22, 23 Abs. 1 des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt (SOG LSA)

- zur Erfüllung der Aufgaben der Polizei,
- zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage,

- zur Vorgangsverwaltung oder befristeten Dokumentation behördlichen Handelns oder
- zur Abwehr einer Gefahr oder zur vorbeugenden Bekämpfung oder Vorsorge für die Verfolgung von Straftaten

erforderlich sind.

Zu 5.6 Öffentlichkeitsfahndung in sozialen Netzwerken

Wie der Landesbeauftragte selbst ausführt, wurden soziale Netzwerke in Sachsen-Anhalt im Berichtszeitraum nicht für die Öffentlichkeitsfahndung genutzt.

Zu 5.8 Nationales Waffenregister

Mit der Einführung des Nationalen Waffenregisters (NWR) wurde u. a. den Waffenbehörden im Hinblick auf die besondere Schutzbedürftigkeit der für das NWR relevanten personenbezogenen Daten aufgegeben, ein geeignetes IT-Sicherheitskonzept zu erstellen, das den jeweils aktuellen Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bzw. den Standards nach § 7 Abs. 3 der Verordnung zur Durchführung des Nationalen-Waffenregister-Gesetzes (NWRG-DV) entsprechen muss. Die Verantwortung für die Gewährleistung der IT-Sicherheit beim Betrieb des NWR liegt bei den beteiligten Behörden selbst. Die Gewährleistung der IT-Sicherheit ist ein dauerhafter Prozess, der kontinuierlicher Verbesserungen bedarf. Im Rahmen der Umsetzung der von den Waffenbehörden Sachsen-Anhalts erstellten IT-Sicherheitskonzepte wurde eine Priorisierung der einzelnen IT-Sicherheitsmaßnahmen vorgenommen. Zum 31. Dezember 2013 haben die Waffenbehörden dem Ministerium für Inneres und Sport zum Stand der Umsetzung der IT-Sicherheitskonzepte berichtet. Danach sind die Maßnahmen mit der höchsten Priorität in allen Behörden umgesetzt. Weitere Maßnahmen folgen im Laufe des Jahres 2014.

Zu 5.9.1 Bundesmeldegesetz

Der Landesbeauftragte geht auf die aus datenschutzrechtlicher Sicht maßgebenden Punkte beim Zustandekommen des Gesetzes zur Fortentwicklung des Meldewesens (MeldFortG) vom 3. Mai 2013 (BGBI. I S. 1084) ein. Das MeldFortG, mit dem der Bund die Regelungen

des bisherigen Rahmenrechts und der Landesmeldegesetze in einem neuen Bundesmeldegesetz (BMG) zusammenführt, tritt am 1. Mai 2015 in Kraft.

Das BMG sieht erstmalig verbindlich vor, dass bundesweit alle Polizei-, Sicherheits- und Justizbehörden sowie weitere durch Bundes- oder Landesrecht bestimmte öffentliche Stellen jederzeit Meldedaten mittels Online-Zugriff automatisiert abrufen können. Um die bundesrechtlichen Anforderungen an die jederzeitige Verfügbarkeit von Meldedaten und den datenschutzgerechten automatisierten Abruf sicher, effizient und kostengünstig erfüllen zu können, sollen die in den 122 kommunalen Melderegistern gespeicherten (Grund-)Meldedaten in einem vom Land betriebenen Spiegelregister zusammengeführt werden. Aufbau und Betrieb dieses Zentralen Meldedatenbestands auf Landesebene (ZMDB) sollen dabei durch den IT-Dienstleister des Landes (Dataport) realisiert werden.

Nach § 14 Abs. 1 Satz 2 DSG LSA ist der Landesbeauftragte rechtzeitig über grundlegende Planungen des Landes zum Aufbau oder zur Änderung von automatisierten Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zu unterrichten.

Dem wurde Rechnung getragen. Der Landesbeauftragte hat bereits an der Auftaktveranstaltung mit Dataport (Projekt-Kick-Off) am 19. März 2014 teilgenommen und somit die Möglichkeit erhalten, schon in der Planungs- und Projektierungsphase aus datenschutzrechtlicher Sicht an der technischen und organisatorischer Ausgestaltung des ZMDB mitzuwirken.

Darüber hinaus wird der Landesbeauftragte auch weiterhin beteiligt und in die in Aussicht genommene Projektarbeit eingebunden.

Zu 5.9.4 Gruppenauskunft über Jubiläumsdaten an Kommunalparlamente

Der Landesbeauftragte hat dem Ministerium für Inneres und Sport ein Schreiben der Stadt Sangerhausen vom 3. September 2012 mit der Bitte um Bewertung aus melderechtlicher Sicht zugeleitet. Gegenstand des Schreibens war a) die Frage der Erteilung von Gruppenauskünften gemäß § 34 Abs. 2 des Meldegesetzes des Landes Sachsen-Anhalt (MG LSA) über Alters- und Ehejubiläen an den Bürgermeister und den Landrat als Mitglied der jeweiligen kommunalen Vertretungskörperschaft und b) die Veröffentlichung von Altersjubiläen in den Amtsblättern der Kommunen.

Zu a) Nach § 34 Abs. 2 MG LSA ist die Erteilung einer Gruppenauskunft über Alters- und Ehejubiläen an Presse und Rundfunk sowie Mitglieder parlamentarischer und kommunaler Vertretungskörperschaften möglich, soweit die Betroffenen der Auskunftserteilung nicht nach § 34 Abs. 4 MG LSA widersprochen haben. Innerhalb der Verwaltung ist eine Datenweitergabe an den Bürgermeister bzw. die zuständigen Stellen der Gemeinden nach § 29 Abs. 5 MG LSA möglich.

Für die Gemeinde als Gebietskörperschaft handeln die nach den Vorschriften der Gemeindeordnung für das Land Sachsen-Anhalt (GO LSA) bestimmten Organe, nämlich der Gemeinderat und der Bürgermeister (vgl. § 35 GO LSA) bzw. dessen Stellvertreter. Verwaltungsorgane des Landkreises sind gemäß § 24 der Landkreisordnung für das Land Sachsen-Anhalt (LKO LSA) der Kreistag und der Landrat. Der Gemeinderat besteht nach § 36 Abs. 1 Satz 1 GO LSA aus den ehrenamtlichen Mitgliedern (Gemeinderäte) und dem Bürgermeister. Nach § 25 Abs. 1 LKO LSA besteht der Kreistag aus den ehrenamtlichen Mitgliedern und dem Landrat. Auch nach dem In-Kraft-Treten des Gesetzes zur Reform des Kommunalverfassungsrechts des Landes Sachsen-Anhalt und zur Fortentwicklung sonstiger kommunalrechtlicher Vorschriften (Kommunalrechtsreformgesetz) vom 17. Juni 2014 (GVBl. LSA S. 288) hat sich die dargestellte Rechtslage nicht verändert.

Es bleibt festzustellen, dass der Bürgermeister und der Landrat sowohl in der Eigenschaft als Mitglied einer kommunalen Vertretungskörperschaft als auch über eine Datenweitergabe innerhalb der Verwaltung Auskünfte über Alters- und Ehejubiläen erhalten können.

Zu b) Als Amtsblatt bezeichnet man ein behördliches Mitteilungsblatt für amtliche Bekanntmachungen, welche die Allgemeinheit betreffen und dazu dienen, einen Sachverhalt öffentlich bekannt zu geben. Teilweise beziehen sich die Bekanntmachungen auch auf den internen Dienstbetrieb. Neben den öffentlichen Bekanntmachungen der Gemeinde können im Amtsblatt auch weitere, nichtamtliche Informationen für die Bürger aufgenommen werden. Als Beiträge im nichtamtlichen Teil des Amtsblattes können Berichte, Meinungsäußerungen, Nachrichten oder Hinweise sowohl der Gemeinde als auch Dritter zu örtlichen Ereignissen wie kommunalpolitischen Fragen und Themen in Betracht kommen. Dem Amtsblatt kommt insoweit in seinem nichtamtlichen Teil die Funktion eines Informationsinstrumentes der Gemeinde zu. Hat sich die Gemeinde entschieden, das Amtsblatt auch zur

Veröffentlichung nichtamtlicher Informationen zugänglich zu machen, steht es im Ermessen der Gemeinde, welche Beiträge sie unter Berücksichtigung melderechtlicher Vorschriften im nichtamtlichen Teil abdrucken lässt. Die presserechtliche Verantwortung für das Amtsblatt liegt bei der Gemeinde bzw. der herausgebenden Körperschaft (vgl. Klang/Gundlach/Kirchmer, Rn. 5c zu § 6).

Eine Übermittlung zur Veröffentlichung im Amtsblatt hängt damit letztlich vom Sinn und Zeck der Regelung in § 34 MG LSA ab. Aus Sicht der Landesregierung ist keine kommunalrechtliche Norm erkennbar, die einer örtlichen und überörtlichen Bekanntmachung von Jubiläen in Amtsblättern entgegenstehen könnte.

Zu 7. Rechtspflege und Strafvollzug

Zu 7.2 Vorratsdatenspeicherung

Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 8. April 2014 - C-293/12 und C-594/12 - die Vorratsdatenspeicherungs-Richtlinie (2006/24/EG) wegen Verstoßes gegen das in Artikel 7 der Europäischen Grundrechtecharta normierte Grundrecht auf Achtung des Privat- und Familienlebens, wegen Verstoßes gegen das in Artikel 8 normierte Grundrechts auf Schutz der personenbezogenen Daten und wegen Verstoßes gegen das in Artikel 52 normierte Prinzip der Verhältnismäßigkeit als ungültig aufgehoben. Zur Begründung führte der EuGH unter anderem an, dass aus den Daten, die mit der Vorratsdatenspeicherung gesammelt werden, sehr genaue Schlüsse auf das Privatleben der Personen gezogen werden könnten, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen und das soziale Umfeld.

Allerdings hat der EuGH eine Vorratsdatenspeicherung nicht generell ausgeschlossen. Mithin wäre eine Neuregelung unter Beachtung der Prinzipien der Verhältnismäßigkeit denkbar. Die EU-Kommission hat allerdings angekündigt, keinen neuen Entwurf vorzulegen. Auch die Bundesregierung hat einen nationalen Alleingang zur Vorratsdatenspeicherung ausgeschlossen.

Die vom Landesbeauftragten angesprochene Klage der EU-Kommission gegen die Bundesrepublik Deutschland, die auf Grund der nicht erfolgten Umsetzung der Richtlinie erhoben wurden, wurde nach der Aufhebung der Richtlinie zurückgezogen.

Zu 7.3 PPP-Projekt Justizvollzugsanstalt Burg – Entwicklung/Sachstand
Zu 7.4 Sicherungsverwahrung

Die Hinweise des Landesbeauftragten konnten ganz überwiegend aufgegriffen werden. Ein Datenschutzkonzept für die Justizvollzugsanstalt Burg in Gestalt einer Datenschutzdienstanweisung ist bereits zum 1. Januar 2013 in Kraft getreten.

Zur Wahrung des Datenschutzes in der Justizvollzugsanstalt (JVA) Burg – sowohl im Bereich der Straf- und Untersuchungshaft als auch im Bereich der Sicherungsverwahrung – wird dabei weiterhin eine enge Abstimmung mit dem Landesbeauftragten gesucht.

Zuletzt fand am 18. Juni 2013 beim Landesbeauftragten ein Arbeitstreffen zum Zwecke der datenschutzrechtlichen Fortentwicklung des PPP-Modells „Justizvollzugsanstalt Burg“ statt. Im Ergebnis dieses Arbeitstreffens sind die Datenschutzdienstanweisungen für den Vollzug der Strafhaft, der Sicherungsverwahrung und der Untersuchungshaft in der Justizvollzugsanstalt Burg nochmals überarbeitet worden.

Die von Seiten des Landesbeauftragten darüber hinaus für erforderlich erachteten vertraglichen Regelungen zur Auftragsdatenverarbeitung befinden sich derzeit in einem engen Abstimmungsprozess mit dem privaten Partner, der Projektgesellschaft Justizvollzug Burg GmbH & Co. KG.

Am 25. Januar 2013 ist zwischen den Vertragsparteien bereits eine erste vertragliche Regelung zur Auftragsdatenverarbeitung in Gestalt eines Vertrages über die Übernahme und Vernichtung von Datenträgern der Justizvollzugsanstalt Burg geschlossen worden. Der für diesen Aufgabenbereich von der Projektgesellschaft Justizvollzug Burg GmbH & Co. KG eingesetzte Nachunternehmer ist der Vereinbarung am 18. Februar 2013 beigetreten.

Im Übrigen werden die im Rahmen des PPP-Projekts zur Justizvollzugsanstalt Burg an verschiedenen Stellen bereits bestehenden vertraglichen Regelungen zum Datenschutz derzeit geprüft, um einen konkreten Regelungsbedarf für den avisierten Vertrag zur Auftragsdatenverarbeitung zu ermitteln. Zusätzliche vertragliche Regelungen zum Datenschutz sind nicht zuletzt auch mit dem privaten Partner im Einzelnen eng abzustimmen, da jede Vertragsänderung grundsätzlich eine Zustimmung beider Vertragsparteien voraussetzt.

Unterschiedliche Auffassungen zwischen dem Landesbeauftragten und dem Ministerium für Justiz und Gleichstellung bestehen demgegenüber weiterhin zur Zulässigkeit einer Mitwirkung von Bediensteten des privaten Partners im Rahmen des Besuchshilfsdienstes in der Justizvollzugsanstalt Burg. Eine diesbezügliche Wahrnehmung von nur untergeordneten Hilfstätigkeiten bei der Besucherkontrolle durch private Bedienstete im Sinne einer sog. unselbstständigen Verwaltungshilfe ist jedoch rechtlich nicht zu beanstanden.

Um den vom Landesbeauftragten geäußerten Bedenken gleichwohl entgegenzukommen, ist die betreffende vertragliche Regelung zum Besuchshilfsdienst zwischenzeitlich überarbeitet worden. Die dem privaten Partner im Rahmen der Besucherkontrolle übertragenen Aufgaben sind nun noch enger gefasst worden, um deutlich zu machen, dass der private Partner in diesem Bereich – wie es schon bisher geübte Praxis ist – ausschließlich weisungsgebundene Hilfstätigkeiten unter ständiger Aufsicht staatlicher Bediensteter wahrnimmt. Damit dürften auch die zuletzt noch bestehenden rechtlichen Bedenken des Landesbeauftragten ausgeräumt worden sein.

Zu 7.5 Elektronische Fußfessel

Die Auffassung des Landesbeauftragten, dass dessen Beteiligung von vornherein nicht vorgesehen war, ist nicht zutreffend. Das Ministerium für Justiz und Gleichstellung hatte vielmehr von einer sehr frühzeitigen Beteiligung des Landesbeauftragten Abstand genommen, weil es davon ausging, wie es von Hessen avisiert wurde, dass der Hessische Landesbeauftragte für den Datenschutz, seine Kollegen der anderen Länder über die beabsichtigte bundesweite Ausgestaltung der Elektronischen Aufenthaltsüberwachung laufend informiert.

Der vom Landesbeauftragten angesprochene Runderlass zur elektronischen Aufenthaltsüberwachung liegt dem Landesbeauftragten seit geraumer Zeit zur Prüfung vor und wird nach dessen Stellungnahme in Kraft gesetzt werden.

Zu 8. Verfassungsschutz

Zu 8.2 Moratorium bei Aktenvernichtung und Löschung von Daten

Nach dem Wegfall der Zweckbestimmung wurden die personenbezogenen Daten gelöscht, die von Arbeitsgruppen im Verfassungsschutz und im Polizeibereich für konkrete Anfragen

auf Landesebene zur Terrorgruppe „Nationalsozialistischer Untergrund“ gespeichert wurden. Archivrechtliche Belange wurden bei der Löschung berücksichtigt.

Zu 8.3 Anbietungspflicht an das Landeshauptarchiv

Der Landesbeauftragte nimmt hier auf eine Diskussion Bezug, die Anfang 2013 im Landtag geführt wurde. Seinerzeit wurden dort unterschiedliche Positionen zu der Frage geäußert, ob der Verfassungsschutz des Landes auf der Grundlage des aktuell geltenden Rechts gehalten ist, die bei ihm entstehenden Akten dem Landeshauptarchiv anzubieten oder nicht. Es bestand jedoch Einigkeit darin, das Ministerium für Inneres und Sport zu beauftragen, in einer Gesetzesnovelle diese Fragen eindeutig und abschließend in Richtung Anbietungspflicht des Verfassungsschutzes zu klären.

Das Ministerium für Inneres und Sport erarbeitet gegenwärtig einen Gesetzentwurf, der diesen Auftrag umsetzen soll. Dabei wird nicht nur das Archivgesetz des Landes novelliert; auch verschiedene weitere Gesetze werden angepasst.

Im Gesetzgebungsverfahren wird der Landesbeauftragte erneut angehört werden, nachdem er in einer frühen Phase der Erarbeitung des Gesetzentwurfs schon einmal beteiligt worden war.

Zu 9. Forschung, Hochschulen und Schulen

Zu 9.3.1 Behördliche Datenschutzbeauftragte in Schulen

Das Kultusministerium hat den Landesbeauftragten bereits darüber unterrichtet, dass eine Regelung zu schulischen Datenschutzbeauftragten in der geplanten Datenschutzverordnung in Ausfüllung der neuen Schulgesetznormen vorgesehen ist. Bei der Erstellung der Verordnung ist auch zu berücksichtigen, dass die geplante Änderung des DSG LSA eine gesonderte Vorschrift zu behördlichen Datenschutzbeauftragten in Schulen enthält. Nach § 14a Satz 4 des Gesetzentwurfs (LT-Drs. 6/3186) kann für bis zu fünf Schulen ein gemeinsamer Beauftragter für den Datenschutz eingesetzt werden, sofern an dieser Schule nicht mehr als zehn Personen mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt sind. Die Möglichkeit der Bestellung eines gemeinsamen Beauftragten wird die Bestellung erleichtern. Die Änderung des DSG LSA wurde im Vorfeld mit dem Landesbeauftragten abgestimmt (vgl. auch Nr. 3.1.5).

Das Kultusministerium wird dafür Sorge tragen, dass im Rahmen eines Erlasses im Vorgriff auf die zurzeit in Bearbeitung befindliche Verordnung zum Umgang mit Personendaten in Schule und Schulbehörden die Regelung des Datenschutzgesetzes zur Bestellung von schulischen Datenschutzbeauftragten im kommenden Schuljahr umgesetzt werden wird. Die Beteiligung des Landesbeauftragten ist dabei selbstverständlich. Eine erste Beratung hat unter Mitwirkung des Landesbeauftragten bereits stattgefunden.

Gleichzeitig wird das Kultusministerium dem Landesbeauftragten Ansprechpartner aus dem Kreis der medienpädagogischen Beraterinnen und Berater benennen, die das Thema schulischer Datenschutz im Rahmen ihrer Arbeit verstärkt vermitteln werden.

Zu 9.3.2 Meldung besonderer Vorkommnisse im Landesschulamt

Seit September 2012 hält das Landesschulamt die Schulen mit Belehrung und Formularvorgabe nachdrücklich dazu an, auf Namensnennungen zu verzichten. Die neuen Formulare enthalten den Hinweis, die Schülerin oder den Schüler namentlich nicht zu erwähnen. Jeder gemeldete Fall wird schulfachlich ausgewertet und begleitet. In den gebotenen Fällen ist im Ergebnis dieser Auswertung schulfachliche und schulpsychologische Hilfe und Unterstützung vor Ort gewährt worden. Die Meldungen selbst sind sinnvoll und geboten. Weiterhin hat das Landesschulamt die Aufbewahrungsfristen festgelegt und sich dabei für eine kurze Frist von sechs Monaten entschieden.

Soweit der Landesbeauftragte eine fehlende Stellungnahme des Landesschulamts kritisiert, merkt die Landesregierung an, dass im Landesschulamt weder beim Direktor noch bei dessen Stellvertreter oder dem Datenschutzbeauftragten des Amtes eine Aufforderung zur Rückäußerung eingegangen ist. Es handelt sich mithin nicht um einen bewussten Verstoß gegen das Unterstützungsgebot nach § 23 DSG LSA. Das Kultusministerium hat in Auswertung der Kritik des Landesbeauftragten das Landesschulamt darauf hingewiesen, dass die Klärungen direkt zwischen dem Landesschulamt und dem Landesbeauftragten erfolgen müsse.

Zu 9.4 Änderung des Schulgesetzes – gläserner Schüler

Mit dem Gesetz zur Änderung schul-, besoldungs- und personalvertretungsrechtlicher Vorschriften vom 5. Dezember 2012 (GVBl. LSA S. 560) wurden die erforderlichen rechtlichen Grundlagen für eine zeitgemäße Datenverarbeitung geschaffen, deren Ergebnisse eine Evaluierung des Bildungswesens ermöglichen. Mit der Überarbeitung wird die schulübergreifende Verwaltungsarbeit verbessert, die z. B. bei der Einschulung oder dem Schulwechsel anfällt.

Neu hinzugekommen ist eine spezielle Ermächtigung des Landesschulamts zur Einrichtung einer automatisierten zentralen Schülerdatei. Aufgrund der neuen Rechtslage können Bildungsverläufe und -biographien erstellt werden, die eine Evaluierung des Bildungswesens erst ermöglichen. Das mittlerweile abgeschlossene Gesetzgebungsverfahren wurde von dem Landesbeauftragten kritisch begleitet. Aufgrund von Hinweisen des Landesbeauftragten wurden Vorschläge aus dem Regierungsentwurf noch geändert.

Die nunmehr geltenden Paragraphen des Schulgesetzes enthalten mehrere Verordnungsermächtigungen. Der Prozess zur Erstellung einer Verordnung über den Umgang mit personenbezogenen Daten im Schulwesen des Landes Sachsen-Anhalt hat begonnen. Das Kultusministerium wird den Landesbeauftragten frühzeitig mit einbeziehen.

Zu 9.5 Medienkompetenz

Für die Sekundarschulen stellt der neue Lehrplan durch Benennung der Medienkompetenz als eine der Schwerpunktkompetenzen sicher, dass der Medienbildung der Schülerinnen und Schüler ausreichend Rechnung getragen wird. Gleiches ist für den in Erstellung befindlichen Lehrplan für die Gymnasien beabsichtigt.

Bereits im Oktober 2008 hat das Landesinstitut für Schulqualität und Lehrerbildung (LISA) allen Grundschulen des Landes Sachsen-Anhalt eine Broschüre mit dem Titel "Medienbildung - Ein kompetenzorientiertes Konzept für die Grundschule mit Beispielaufgaben und einem Medienpass“. (Hrsg: LISA, 2008) und im ersten Quartal 2011 allen Schulen mit Sekundarschulbildungsgang eine Broschüre „Medienbildung. Ein kompetenzorientiertes Konzept für die Sekundarschule mit Beispielaufgaben“ (Hrsg. LISA, 2010) zur Verfügung gestellt.

Weiterhin hat die Martin-Luther-Universität Halle-Wittenberg in die erziehungswissenschaftliche Grundlagenausbildung medienpädagogischer Pflichtmodule eingebunden. Die Fortbildungsangebote für die Lehrkräfte sind entsprechend des neuen Fortbildungsanlasses als Abrufangebote durch die Lehrkräfte formuliert worden. Diese können in ihrer fachlichen Zuständigkeit und unter Berücksichtigung des jeweiligen Fortbildungskonzeptes der Schule den für sie notwendigen Fortbildungsbedarf somit decken. Eine verbindliche Vorgabe existiert für die Teilnahme an Fortbildungen in thematischer Hinsicht allerdings nicht. Sie würde dem Gedanken der Eigenverantwortlichkeit der Lehrkräfte für ihre Fortbildung widersprechen.

Angesichts dieser Umstände ist die Kritik des Landesbeauftragten an der Umsetzung des Konzepts der Landesregierung nicht nachvollziehbar.

Zu 10. Gesundheits- und Sozialwesen

Zu 10.1.4 Landeskrebsregister

Wie vom Landesbeauftragten bereits angemerkt, konnte in den Beratungen ein Konzept erarbeitet werden, das unter anderem infolge des Einsatzes verschiedener Verschlüsselungsverfahren eine pseudonyme Datenhaltung im Landeskrebsregister gewährleistet, und dennoch alle von den Forschern gewünschten Informationen zur Verfügung stellt. Hinsichtlich der Schwierigkeiten mit einer kurzen und verständlichen Gestaltung der Einwilligungserklärung werden die Anmerkungen des Landesbeauftragte im Hinblick auf die bundesgesetzlichen Vorgaben zur Schaffung von Krebsregister im Krebsfrüherkennungs-und Registergesetz geteilt.

Zu 10.1.9 Langfristige Aufbewahrung von Patientenakten

Die Ausführungen des Landesbeauftragten zu Aufbewahrungsfristen für Patientenakten werden von der Landesregierung nicht geteilt. Richtig ist, dass es hier keine einheitlichen einschlägigen rechtlichen Vorschriften gibt. Maßgeblich sind deswegen die Regelungen zur Verjährung von Schadensersatzansprüchen (§ 199 BGB). Danach können Ansprüche noch 30 Jahre nach dem Eintritt des Schadensfalls geltend gemacht werden. Bei ärztlichen Kunstfehlern oder Fehlverhalten des Krankenhauses können dabei durchaus Ansprüche entstehen, die für einzelne Ärzte oder auch ein ganzes Krankenhaus existenzbedrohend

sind. Insofern empfehlen die Landeskrankenhausgesellschaften ebenso wie die Deutsche Krankenhausgesellschaft, Patientenakten grundsätzlich 30 Jahre aufzubewahren. Eine Differenzierung nach Gefährdungspotenzial kann aus hiesiger Sicht nicht vorgenommen werden, da sich praktisch aus jeder Art der Erkrankung Langzeitwirkungen entwickeln können, die in Schadensersatzklagen münden.

Hinsichtlich des Wunsches der Hochschulkliniken nach längeren Aufbewahrungsfristen aufgrund von Forschungsvorhaben weist die Landesregierung darauf hin, dass Forschung eine genuine Aufgabe der Universitätsklinika ist. Die - auch längerfristige - Verfügbarkeit von bestimmten Patientenakten dient mithin der Dienstaufgabe und ist bereits deswegen gesetzlich legitimiert.

Zu 11. Personalwesen

Zu 11.1 Personalvermittlungsstelle

Das Ministerium der Finanzen teilt die Einschätzung des Landesbeauftragten bezüglich der ressortübergreifenden Übermittlung von Personalaktendaten, der Auslegungen des § 88 des Beamtengesetzes des Landes Sachsen-Anhalt (Landesbeamtengesetz - LBG LSA), der Aufgaben der Personalvermittlungsstelle (PVS) und der Notwendigkeit, eine neue erweiterte gesetzliche Grundlage zu schaffen.

Nachdem die Landesregierung in der Haushaltsklausur am 30. Mai 2013 das Ministerium der Finanzen beauftragt hatte, einen klarstellenden Änderungsvorschlag für § 88 Abs. 1 Satz 1 LBG LSA zu erarbeiten, wurde der Entwurf des Haushaltsbegleitgesetzes 2014 (LT-Drs. 6/2362) dem Landtag zeitnah am 21. August 2013 vorgelegt und am 18. Dezember 2013 beschlossen.

Zu 12. Finanzen, Kataster, Kommunales und Statistik

Zu 12.2 Evaluierung des „anderen sicheren Verfahrens“ bei ElsterOnline

Der Landesbeauftragte thematisiert unter Fortführung seiner Betrachtung unter Nr. 8.3 seines X. Tätigkeitsberichtes die Nutzungsmöglichkeit des neuen Personalausweises (nPA) zur Registrierung und damit zur erstmaligen Identifizierung am ElsterOnlinePortal. Die Landesregierung teilt grundsätzlich die positive Einschätzung zur Nutzungsmöglichkeit.

Der Schlussfolgerung, dass der nPA das qualifizierte elektronische Zertifikat für Authentifizierungszwecke zurückdrängen wird, tritt die Landesregierung entgegen. Die eID-Funktion (elektronische Identifizierung) bietet eine komfortable Möglichkeit sich gegenüber einer Zertifizierungsstelle zum Erwerb eines qualifizierten elektronischen Zertifikats zu identifizieren. Der nPA wirkt daher bezüglich Erwerb und Nutzung eines solchen Zertifikats konzeptionell förderlich.

Wie bereits vom Landesbeauftragten selbst ausgeführt, unterscheidet sich der nPA mit der eID-Funktion funktional grundlegend von einem qualifizierten elektronischen Zertifikat. Hinsichtlich der Nutzungsmöglichkeit gibt es allerdings eine Schnittmenge für die aus datenschutzrechtlicher Sicht beide Varianten die gleiche Qualität bieten. Im Moment der Nutzung kann die Identität des Nutzers nachgewiesen werden. Eine solche Funktion ist für die Nutzung des ElsterOnlinePortals als sogenanntes anderes sicheres Verfahren gemäß § 87a Abs. 6 Abgabenordnung (AO) notwendig. Der Einsatz des nPA hierfür wurde vom Gesetzgeber folgerichtig und ausdrücklich zugelassen. Eine entsprechende Funktion ist im ElsterOnlinePortal allerdings derzeit nicht implementiert.

Die Landesregierung teilt nicht die Kritik des Landesbeauftragten an dem Verfahren für die Übermittlung von Steuererklärungen, soweit keine elektronische Authentisierung vorgesehen ist. Diese Verfahren sind an die (zusätzliche) papiergebundene Übermittlung einer unterschriebenen Steuererklärung gekoppelt. Gerade papiergebundene Verfahren bieten ein Höchstmaß an Authentizität.

Zu 12.6 Statistik – Auswertung Zensus 2011

Der Landesbeauftragte beschäftigt sich mit der Auswertung des Zensus 2011. Dieser war EU-weit vorgeschrieben und wurde in der Bundesrepublik Deutschland nach einheitlichen Maßgaben durchgeführt. Zur Umsetzung dieses EU-weiten Zensus hat sich die Bundesrepublik Deutschland – statt wie in der Vergangenheit für eine Vollerhebung – für eine registergestützte Methode entschieden. Registergestützte Methoden nutzen bereits vorhandene Verwaltungsregister (u.a. Melderegister) als Datenquellen, die in bestimmten Bereichen durch eine Verknüpfung von Vollerhebungen und Stichprobenerhebungen ergänzt werden. Da diese Verwaltungsdaten u.a. keine verlässlichen Informationen etwa zur Bildung, zum konkreten Beruf eines Menschen, zur Wohnsituation, zur Erwerbstätigkeit für bestimmte Gruppen (zum Beispiel für Selbstständige) enthalten und für Gebäude und Wohnungen

flächendeckend überhaupt keine Registerdaten zur Verfügung stehen, mussten beim Zensus 2011 ergänzende Befragungen durchgeführt werden: Beispielsweise die Gebäude- und Wohnungszählung, die Haushaltebefragung und die Befragung in Wohnheimen und Gemeinschaftsunterkünften.

Zur Durchführung des Zensus wurden gem. § 2 des Ausführungsgesetzes des Landes Sachsen-Anhalt zum Zensusgesetz 2011 (Zensusausführungsgesetz Sachsen-Anhalt - ZensAG LSA) in festgelegten Gemeinden örtliche Erhebungsstellen eingerichtet. Von deren Kontrolle war der aktuelle Berichtszeitraum vom 1. April 2011 bis 31. März 2013 geprägt. Das Statistische Landesamt hat die örtlichen Erhebungsstellen über die datenschutzrechtlichen Aspekte im Zusammenhang mit der Aufgabenerledigung im Rahmen des Zensus 2011 unterrichtet. Umfangreiche Schulungsmaßnahmen dienten der Sicherstellung, dass die gesetzlichen und methodischen Vorgaben und insbesondere die Vorschriften zur statistischen Geheimhaltung eingehalten wurden. Dazu wurde u.a. Informationsmaterial insbesondere zu den gesetzlichen Grundlagen des Zensus 2011 und zur Einrichtung der Erhebungsstellen übergeben. Dieses beinhaltete auch Hinweise und Muster zur Erstellung einer Dienstanweisung, Muster für die Niederschrift über die Verpflichtung auf das Statistikgeheimnis sowie die Regelungen zur Abschottung. Auch über einzuhaltende Kriterien bei der Auswahl geeigneter Erhebungsbeauftragter wurden die Erhebungsstellen seitens des Statistischen Landesamtes geschult. Darüber hinaus wurden im Hinblick auf die IT-seitigen Aspekte entsprechende Vorkehrungen getroffen.

Da die Europäische Union ab dem Jahr 2011 für alle Mitgliedstaaten die Durchführung von Volks-, Gebäude- und Wohnungszählungen im Abstand von zehn Jahren vorschreibt, ist die Durchführung des Zensus 2011 stetig auf dem Prüfstand und wird evaluiert. Insofern bestehen Bestrebungen auf Bund-Länder-Ebene, welche mit Anregungen zur Verbesserung etwaiger Regelungen und Verfahren verbunden sind. Diese wurden zum Teil auch im Tätigkeitsbericht aufgenommen, wobei in der weiteren Prüfung der Umsetzbarkeit dieser Vorschläge zum Einen landesspezifische Gegebenheiten zu berücksichtigen bleiben und zum Anderen zu überprüfen bleibt, inwieweit das technische Verfahren und die praktische Umsetzung der Erhebung Änderungen zulässt. Jedenfalls konnte auch bisherigen Bund-Länder-Austausch noch kein abschließender Katalog von möglichen oder notwendigen Änderungen abschließend erarbeitet werden.

Zu 13. Wirtschaft und Verkehr

Zu 13.6.2 Schwarzfahrerdatei beim ÖPNV

Mit Schreiben vom 3. Juli 2012 hat sich der Landesbeauftragte mit der Bitte um Prüfung der Regelung zur Speicherung personenbezogener Daten von Schwarzfahrern an das Ministerium für Landesentwicklung und Verkehr gewandt. Das Thema wurde in länderübergreifenden Fachgremien diskutiert. So haben sich der AK Öffentlicher Personenverkehr am 28. Februar 2013, die Gemeinsame Konferenz der Verkehrs- und Straßenbauabteilungsleiter der Länder am 13. und 14. März 2013 sowie die Verkehrsministerkonferenz am 10. und 11. April 2013 mit dem Thema befasst. Dem Landesbeauftragten wurde im Ergebnis dieser Befassungen mit Schreiben vom 21. Juni 2013 mitgeteilt, dass die bereits existierende Regelung aus Sicht der Fachgremien als ausreichend angesehen werde.

Hinsichtlich der Speichermöglichkeit wird nochmals darauf hingewiesen, dass privatrechtlich organisierte Verkehrsunternehmen personenbezogene Daten von Schwarzfahrern nach § 28 Abs. 1 S. 1 Nr. 2 BDSG speichern können. Im Hinblick auf die öffentlich-rechtlich organisierten Verkehrsunternehmen ist die Speicherung personenbezogener Daten nach § 10 Abs. 1 DSG LSA zulässig. Die Speicherfrist orientiert sich jeweils an der Verjährungsfrist der zugrunde liegenden Straftat von drei Jahren (§ 78 Abs. 3 Nr. 5, § 265a des Strafgesetzbuchs (StGB)). Das Erschleichen geringwertiger Leistungen ist gem. § 265a Abs. 3 i.V.m. § 248a StGB ein Antragsdelikt. Gem. § 77b StGB muss der Antrag auf Strafverfolgung zwar binnen drei Monaten gestellt werden. Nach Ablauf dieser Antragsfrist ist der Blick allerdings auf den Wiederholungstäter zu richten. Verkehrsunternehmen haben häufig nur ein Interesse an der strafrechtlichen Verfolgung des Wiederholungstäters. Das setzt voraus, dass die Daten über einen längeren Zeitraum gespeichert werden. Erst dann ist für Antragsdelikte die Verjährungsfrist von drei Jahren entscheidend. Könnten die Daten nicht mehr bis zum Ablauf der Verjährungsfrist gespeichert werden, so wäre die Folge, dass die Verkehrsunternehmen einen Strafantrag nicht nur im Fall des Wiederholungstäters, sondern bereits bei einem Ersttäter stellen würden. Die Datenspeicherung liegt daher im Interesse des Betroffenen.

Ferner liegt es selbst in der Verantwortung der angesprochenen Verkehrsunternehmen, insbesondere der Straßenbahnunternehmen (MVB, HVAG bzw. Naumburger Straßenbahn), die aufgrund ihrer besonderen Beförderungsverhältnisse (mehrere unbeaufsichtigte Einstiegsmöglichkeiten) in erster Linie zum Adressatenkreis gehören, für die Einhaltung der

Vorschriften zu sorgen. Das Ministerium für Landesentwicklung und Verkehr hat diesbezüglich keine Aufsichtsbefugnisse. Daher bleibt es dem Landesbeauftragten vorbehalten, auf diese Unternehmen in Form von Hinweismaterialien bzw. durch konkretes Aufgreifen der Problematik einzuwirken.

Zu 13.6.3 Fahrgastzählung im ÖPNV

Die Landesregierung teilt die Auffassung des Landesbeauftragten, dass die Datenerhebung auf freiwilliger Basis erfolgen muss und im Vorfeld der Abfrage darauf hinzuweisen ist, dass der Befragte diese auch ablehnen kann bzw. dass der Befragende seine diesbezügliche Handlungsberechtigung ohne Aufforderung auch darzulegen hat. Für Zählungen im Auftrag des Landes hat das Ministerium für Landesentwicklung und Verkehr die Angelegenheit mit der NASA GmbH erörtert und auf Beachtung der Rechtslage hingewirkt.

Zu 13.6.4 Verwarnungen auf Vorrat im ruhenden Verkehr

Das Landesverwaltungsamt berichtete dem Ministerium für Inneres und Sport mit Schreiben vom 7. Oktober 2013, dass die Stadt Naumburg die erhobenen personenbezogenen Daten löschen und in Zukunft bei der Verteilung von „Gelben Karten“ keine personenbezogenen Daten mehr speichern wird. Dieses Ergebnis teilte das Ministerium für Inneres und Sport dem Landesbeauftragten mit Schreiben vom 29. Oktober 2013 mit. Somit sind die Forderungen sowohl des Landesbeauftragten als auch des Ministeriums für Inneres und Sport erfüllt.

Das Ministerium für Inneres und Sport prüft gegenwärtig einen Erlass, der auf die geltende Rechtslage und die Unzulässigkeit dieser Vorratsdatenspeicherung hinweist. Insoweit wird der Empfehlung des Landesbeauftragten nachgekommen.

Anlage

Ergebnisbericht der Arbeitsgruppe des AK I „Staatsrecht und Verwaltung“ zum Datenschutz in Sozialen Netzwerken vom 4. April 2012

Inhaltsverzeichnis

Der Ergebnisbericht beruht auf den Arbeiten einer vom AK I anlässlich der Berichtsbitte der CdS-Jahreskonferenz vom 22./23. September 2011 eingerichteten länderoffenen Arbeitsgruppe. Eine Sitzung der Arbeitsgruppe unter Federführung des Landes Berlin und des Freistaats Bayern fand am 17. Februar 2012 statt.

I. Einleitung

Ein Grund für die Popularität von Sozialen Netzwerken liegt darin, dass deren Betreiber durch neue Funktionen die Kommunikationsmöglichkeiten für die Nutzer ausbauen und dadurch die „soziale Vernetzung" weiter steigern. Den Nutzern wird ermöglicht, ihr Leben immer schneller und einfacher mit ihren „Freunden" in Sozialen Netzwerken zu teilen.

In letzter Zeit geschieht dies auch dadurch, dass Soziale Netzwerke ihren Wirkungskreis über die eigene Internetpräsenz hinaus mittels „Social Plugins" ausdehnen. Insbesondere der Like-Button von Facebook hat sich rasant über das gesamte Internet verbreitet. Durch dessen Einbettung können Betreiber von Webseiten Facebook-Nutzern individualisierte Nutzungsmöglichkeiten für ihre Webseite anbieten. Ein Facebook-Nutzer kann durch einen Klick auf den Like-Button seine Facebook-Freunde auf seiner Profilseite auf die Webseite aufmerksam machen. Zudem wird einem eingeloggten Facebook-Nutzer, der eine Webseite mit Like-Button besucht, personalisierter Inhalt angeboten: er erfährt, welche seiner Facebook-Freunde die Webseite ebenfalls empfohlen haben und ggf. welche Kommentare sie über die Webseite gepostet haben.

Die Funktionsweise des Like-Buttons verdeutlicht, dass damit nicht nur die Kommunikationsmöglichkeiten der Facebook-Nutzer erweitert werden, sondern für einen Webseitenbetreiber durch die Empfehlung im Facebook-Profil des klickenden Mitglieds ein neuer Marketingweg für seine Seite (und damit für die angebotenen Produkte und Dienstleistungen) eröffnet wird. Soziale Netzwerke werden daher für öffentliche und private Institutionen im Hinblick auf Öffentlichkeitsarbeit und Marketing immer bedeutender.

Neben Social Plugins bieten die Betreiber von sozialen Netzwerken in zunehmendem Maß auch innerhalb der eigenen Internetpräsenz privaten und öffentlichen Institutionen Möglichkeiten für Öffentlichkeitsarbeit. Prominentestes Beispiel sind die Fanpages von Facebook. Dies sind Seiten auf der Plattform Facebook, welche von Unternehmen und Institutionen zur Eigendarstellung betrieben werden können und Facebook-Nutzern die unmittelbare Kommunikation mit dem Unternehmen unter Einbindung ihrer Facebook-Freunde ermöglichen.

Eine anlässlich der Erstellung dieses Berichts initiierte Umfrage im Länderkreis hat ergeben, dass öffentliche Stellen insbesondere Fanpages, aber auch in geringerem Maße Social Plugins für ihre Öffentlichkeitsarbeit vielfältig nutzen. Aus dem Polizeibereich wurde neben klassischer Öffentlichkeitsarbeit auch die Nutzung von Fanpages als Veröffentlichungsplatt-

form für Fahndungsaufrufe und Vermisstensuche genannt. Die sich hieraus ergebenden besonderen Fragestellungen bedürfen einer gesonderten polizeifachlichen Prüfung und sind nicht Gegenstand dieses Berichts.

II. Öffentlichkeitsarbeit in sozialen Netzwerken als Gegenstand datenschutzaufsichtlicher Diskussion

Im August 2011 hat das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) alle Webseitenbetreiber in Schleswig-Holstein aufgefordert, ihre Fanpages bei Facebook und Social Plugins auf ihren Webseiten zu entfernen. Diese verstießen in ihrer gegenwärtigen Ausgestaltung gegen Bestimmungen des Telemediengesetzes (TMG).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung vom 28./29. September 2011 hervorgehoben, dass die direkte Einbindung des Like-Buttons und anderer Social Plugins in die Webseiten deutscher Anbieter momentan ohne hinreichende Information der Nutzer über die ausgelösten Datenverarbeitungsvorgänge und ohne Einräumung eines Wahlrechtes nicht mit deutschen und europäischen Datenschutzstandards in Einklang stehe. Öffentliche Stellen sollten daher von der Nutzung absehen; gleiches gelte für Fanpages.

Der Düsseldorfer Kreis hat am 8. Dezember 2011 beschlossen, dass die Betreiber von Fanpages und von Webseiten mit Like-Button eine Mitverantwortung für die Einhaltung der Datenschutzvorschriften treffe. Hierzu gehöre die umfassende Aufklärung der Nutzer über die erhobenen Daten. Insbesondere beim Like-Button seien den Webseitenbetreibern die Datenflüsse an Facebook nicht in vollem Umfang bekannt, sodass sie diesen nicht ohne weiteres in das eigene Angebot einbinden dürften.

III. Berichtsbitte der CdS-Jahreskonferenz vom 22./23. September 2011

Die Chefinnen und Chefs der Staats- und Senatskanzleien der Länder haben auf ihrer Jahreskonferenz vom 22./23. September 2011 die Diskussion über die Verbesserung des Datenschutzes in sozialen Netzwerken begrüßt, insbesondere wenn Webseitenbetreiber Fanpages z.B. bei Facebook oder Social Plugins auf ihren Webseiten eingerichtet haben (Ziffer 1 des CdS-Beschlusses). Sie stellen fest, dass die Sozialen Netzwerke von öffentlichen Stellen auf allen Ebenen, von privaten Institutionen und von Unternehmen als neue Form der Kommunikation genutzt würden. Zur Förderung der Belange des Datenschutzes sei ein zwischen Bund und Ländern abgestimmtes gemeinsames Handeln erforderlich, das europäi-

sche und internationale Bezüge berücksichtige und hierbei auch die Notwendigkeit der Änderung gesetzlicher Regelungen einbeziehe (Ziffer 2 des CdS-Beschlusses). Sie haben die Konferenz der Innenminister und -senatoren der Länder gebeten

- über die aktuellen Entwicklungen zu berichten und
- unter Einbeziehung von Initiativen der Bundesregierung sowie der Ergebnisse der Konferenz der Datenschutzbeauftragten erste gemeinsame Vorschläge zu machen (Ziffer 3 des CdS-Beschlusses).

Zur Erstellung des Berichts hat der Arbeitskreis I „Staatsrecht und Verwaltung" der Innenministerkonferenz eine Arbeitsgruppe einberufen.

IV. Aktuelle Entwicklungen

1. Sachstand Schleswig-Holstein

Nach einer Pressemitteilung des ULD hat es hinsichtlich des Betreibens von Fanpages gegenüber sechs öffentlichen Stellen Beanstandungen ausgesprochen sowie gegenüber drei nicht-öffentlichen Stellen eine Anordnung nach § 38 Abs. 5 des Bundesdatenschutzgesetzes (BDSG) erlassen. Gegen die Anordnungen nach § 38 Abs. 5 BDSG wurde jeweils Anfechtungsklage zum VG Schleswig erhoben.

2. Gutachten, Untersuchungen und Gremienbefassung

2.1. Nationale Ebene

Neben Veröffentlichungen in der datenschutzrechtlichen Literatur liegen mittlerweile eine Vielzahl von technischen und rechtlichen Analysen zur Nutzung von Fanpages sowie der Einbindung des Like-Buttons vor. Hervorzuheben sind:

- Arbeitspapier des ULD „*Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook*" vom 19. August 2011
- Ausarbeitung des Wissenschaftlichen Dienstes Dt. Bundestag „*Die Verletzung datenschutzrechtlicher Bestimmungen durch sogenannte Facebook Fanpages und Social-Plugins*" vom 7. Oktober 2011
- Ausarbeitung des Wissenschaftlichen Dienstes Landtag Schleswig-Holstein vom 24. Oktober 2011

Zu technischen Fragen ist zudem eine umfassende Korrespondenz zwischen dem ULD und dem Unternehmen Facebook öffentlich zugänglich.

2.2. Europäische Ebene

Die irische Datenschutzaufsichtsbehörde hat anlässlich einer Betriebsüberprüfung bei „*Facebook Ireland Ltd.*" neben der Konzernstruktur des Unternehmens Facebook eine Vielzahl von Funktionen von Facebook (darunter auch den Like-Button) untersucht und bewertet. Der Untersuchungsbericht vom 21. Dezember 2011 enthält als Anlage auch eine technische Analyse der Funktionen. Der Bericht soll voraussichtlich in der Art-29-Datenschutzgruppe beraten werden. Diese hat sich in der Vergangenheit zudem bereits mit dem Datenschutz in sozialen Netzwerken beschäftigt (Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke vom 12. Juni 2009, WP 163).

3. Würdigung der Sach- und Rechtsfragen

3.1. Allgemeines

Für die datenschutzrechtliche Beurteilung ist Kenntnis der technischen Abläufe erforderlich, d.h. Kenntnis davon, welche Arten von Daten bei Social Plugins und Fanpages unter welchen Bedingungen von wem verarbeitet werden. Die unter Ziffer 2.1. zitierten Ausarbeitungen, die Korrespondenz von Facebook mit dem ULD sowie der Untersuchungsbericht der irischen Datenschutzaufsichtsbehörde tragen hier zur Klärung bei. Die technischen Abläufe werden daher im Folgenden für den Like-Button und die Facebook-Fanpages beschrieben. Jedoch verbleiben Unsicherheiten, auf deren Auswirkung bei der Würdigung der Sach- und Rechtslage nachfolgend im Einzelnen einzugehen ist.

3.2. Technische Abläufe beim Like-Button und bei Fanpages

(1) Grundlagen

Die Einbindung des Like-Buttons in Webseiten erfolgt mittels eines sog. Inline-Frames, der auch bei vielen anderen Internetseiten zur Zusammenführung von Text- und Bildinhalten verschiedener Anbieter genutzt wird. Dies bedeutet, dass beim Aufruf einer Webseite mit Like-Button auch der Webserver von Facebook aufgerufen wird, ohne dass dies im Browser des Nutzers erkennbar ist. Es werden die gleichen Informationen an den Facebook-Server übertragen, die auch bei einem ausdrücklichen Aufruf der Seite durch Eingabe in den Browser übertragen werden. Dies ermöglicht es zum Beispiel, dass Cookies, welche Facebook zu einem früheren Zeitpunkt

im Browser des Nutzers gesetzt hat, beim Besuch einer Webseite mit Like-Button an Facebook übertragen werden.

Fanpages sind Webseiten von Facebook und enthalten daher auch die URL der Facebook-Seite (Beispiel: Fanpage des FC Bayern München, abrufbar unter http://de-de.facebook.com/FCBayern). Das Aufrufen einer Fanpage ist somit ein Aufrufen der Facebook-Seite.

(2) Datenflüsse

Sowohl beim Like-Button als auch bei Fanpages ist nach Fallgruppen zu unterscheiden. Differenziert werden muss zwischen:

- Facebook-Mitgliedern und Nicht-Facebook-Mitgliedern
- Eingeloggten und nicht eingeloggten Facebook-Mitgliedern
- Klicken des Like-Buttons und bloßem Besuch einer Webseite mit Like-Button

Betreffend die Art von Daten sind die IP-Adressen der Nutzer und die von Facebook gesetzten und an Facebook übertragenen Cookies für die datenschutzrechtliche Beurteilung von Bedeutung.

IP-Adressen

Sowohl beim Like-Button als auch bei Fanpages findet eine Übertragung der IP-Adresse des Nutzers an Facebook statt. Ohne Übertragung der IP-Adresse des Nutzers könnte diesem der Inhalt des Like-Buttons und der Fanpage nicht dargestellt werden. Nach Angaben von Facebook wird die IP-Adresse in den meisten Fallgruppen unmittelbar nach Übertragung in eine „*generische IP-Adresse*" umgewandelt. Dieser Begriff ist kein IT-Fachbegriff, sondern eine Bezeichnung von Facebook, die eine Anonymisierung meint. Details hierzu sind bislang nicht bekannt.

Cookies

Facebook setzt sowohl über den Like-Button als auch bei Fanpages Cookies im Webbrowser der Nutzer, wobei hier zwischen den Fallgruppen zu unterscheiden ist. Für die datenschutzrechtliche Würdigung bedeutsam sind der sog. datr-Cookie sowie der c_user-Cookie. Der datr-Cookie, der bei jedem Aufruf der Webseite www.facebook.com gesetzt wird (Anm.: durch den Klick auf den Like-Button öffnet sich diese in einem separaten Fenster; bei Fanpages findet ein Aufruf der Facebook-Webseite statt), hat eine Gültigkeit von zwei Jahren, kann aber durch entsprechende Browsereinstellung blockiert und gelöscht werden. Er dient Facebook nach eigenen

Angaben zur Identifizierung des Webbrowsers, der die Verbindung mit der Facebook-Seite aufbaut, und spielt eine Schlüsselrolle beim Schutz des Sozialen Netzwerks vor „böswilligen Aktivitäten". Der c_user-Cookie wird von Facebook gesetzt, wenn sich das Facebook-Mitglied einloggt, und enthält die Anmeldekennnummer (User-ID) des Facebook-Mitglieds. Facebook kann dadurch das Mitglied identifizieren, den Aufruf der Webseite mit Like-Button oder der Fanpage einer konkreten Person zuordnen und auf diese Weise den Inhalt des Like-Buttons bzw. der Fanpage personalisieren. Die Gültigkeit des c_user-Cookies hängt davon ab, ob das Facebook-Mitglied in seinen Kontoeinstellungen die Option „Angemeldet bleiben" gewählt hat oder nicht. Hat es diese gewählt, verliert der Cookie seine Gültigkeit erst, wenn das Facebook-Mitglied den Facebook-Webserver 30 Tage nicht mehr aufruft. Ansonsten wird der c_user-Cookie mit dem Schließen des Browsers gelöscht.

Die nachfolgenden Tabellen 1 und 2 stellen die Datenflüsse dar, die Facebook beim Besuch einer Webseite mit Like-Button bzw. einer Fanpage vom Nutzer erhält.

Tabelle 1: Like-Button

	Fallgruppe	Technische Abläufe
1	Nicht-Facebook-Mitglied besucht erstmalig eine Webseite mit Like-Button und klickt diesen nicht	Übertragung der IP-Adresse und Speicherung als generische IP-Adresse
2	Nicht-Facebook-Mitglied besucht erstmalig eine Webseite mit Like-Button und klickt auf diesen	Übertragung der IP-Adresse/Speicherung als generische IP-Adresse und Setzen des datr-Cookie
3	Nicht-Facebook-Mitglied besucht, nachdem es früher bereits auf derselben oder einer anderen Webseite auf den Like-Button geklickt hatte, erneut eine Webseite mit Like-Button und - klickt aber den Like-Button nicht erneut - klickt den Like-Button erneut	Übertragung der IP-Adresse/Speicherung als generische IP-Adresse und Übertragung des datr-Cookie (soweit noch gültig und noch nicht gelöscht)
4	Facebook-Mitglied, das gerade nicht eingeloggt ist, besucht eine Webseite mit Like-Button und klickt diesen nicht	Übertragung der IP-Adresse/Speicherung als generische IP-Adresse und Übertragung des datr-Cookie (soweit noch gültig und noch nicht gelöscht)
5	Facebook-Mitglied, das gerade nicht eingeloggt ist, besucht eine Webseite mit Like-Button und klickt auf diesen	Übertragung der IP-Adresse und Speicherung als spezifische IP-Adresse und Übertragung des datr-Cookie (soweit noch gültig und noch nicht gelöscht)
6	Eingeloggtes Facebook-Mitglied besucht eine Webseite mit Like-Button	Übertragung der IP-Adresse und Speicherung als spezifische IP-Adresse und Übertragung des datr-Cookie (soweit noch gültig und noch nicht gelöscht) und

		Übertragung des c_user-Cookie

Tabelle 2: Fanpage

	Fallgruppe	Technische Abläufe
1	Nicht-Facebook-Mitglied oder Facebook-Mitglied, das gerade nicht eingeloggt ist, besucht eine Fanpage	Übertragung der IP-Adresse (unklar, ob Speicherung als generische oder spezifische IP-Adresse) und Setzen/Übertragen des datr-Cookie
2	Eingeloggtes Facebook-Mitglied besucht eine Fanpage	Übertragung der IP-Adresse (unklar, ob Speicherung als generische oder spezifische IP-Adresse) und Setzen/Übertragung des datr-Cookie und Übertragung des c_user-Cookies

(3) Facebook Insights

Webseitenbetreiber, die den Like-Button einbinden, und Betreiber von Fanpages können mit Hilfe des von Facebook kostenfrei zur Verfügung gestellten Werkzeugs „Facebook Insights" Statistikinformationen über Nutzer abrufen. Die durch Facebook erstellten Statistiken enthalten Angaben über die Nutzung der Webseite/Fanpage. Dazu gehören Informationen über den Nutzerzuwachs, die Demographie der Nutzer und über die Nutzung der einzelnen Funktionalitäten von Like-Button/Fanpage.

3.3. Rechtsfragen – Würdigung

Die Darstellung der Rechtsfragen behandelt ausschließlich den Like-Button und Facebook-Fanpages, über deren Funktionsweise am meisten bekannt ist.

Like-Button und Fanpages ermöglichen dem Nutzer durch entsprechende Verwendung der Funktionen eine Kommunikation, d.h. das Teilen von Inhalten mit anderen. Aufgrund seiner Funktionsweise ist der Like-Button insbesondere nicht nur eine auf eine einfache Transportfunktion von Inhalten reduzierte Leistung. Auch Fanpages bieten einem Besucher Bedienmöglichkeiten zur Interaktion mit dem Fanpage-Betreiber und den anderen Nutzern des Sozialen Netzwerks, die über eine einfache Transportfunktion von Inhalten hinausgeht. Aus diesem Grund sind Like-Button und Fanpage als Telemedien nach § 1 Abs. 1 Satz 1 TMG zu qualifizieren, sodass der sachliche Anwendungsbereich des TMG eröffnet ist.

Im Überblick stellen sich dann bei der Nutzung von Like-Button und Fanpage auf der Grundlage des Telemediengesetzes folgende Rechtsfragen, die nachfolgend im Einzelnen zu würdigen sind.

Tabelle 3: Überblick zu den Rechtsfragen

Aufgeworfene Rechtsfrage	Würdigung unter
Internationales Datenschutzrecht: Anwendbarkeit deutschen Rechts?	(1)
Personenbezug der erhobenen Daten?	(2)
Verantwortlichkeit der Betreiber von Webseiten mit Like-Button und der Betreiber von Fanpages?	(3)
Verstoß gegen § 15 Abs. 3 TMG wegen Facebook Insights und/oder Setzen/Übertragen von Cookies?	(4)
Cookies nur noch mit Einwilligung des Nutzers?	(5)
Zulässigkeit der Übertragung und Speicherung der generischen IP-Adresse?	(6)
Zulässigkeit der Speicherung der spezifischen IP-Adresse?	(7)
Zulässigkeit des Setzens/der Übertragung des datr-Cookie?	(8)
Zulässigkeit der Übertragung des c_User-Cookie?	(9)

(1) Internationales Datenschutzrecht: Anwendbarkeit deutschen Rechts?

Dies wird kontrovers diskutiert. Facebook ist der Auffassung, dass seine irische Niederlassung *Facebook Ireland Ltd.* verantwortliche Stelle für die Datenverarbeitung seiner deutschen (und europäischen) Mitglieder sei und daher irisches Datenschutzrecht Anwendung finde. Das ULD sieht die Verantwortlichkeit bei *Facebook Inc.* in den USA, sodass deutsches Datenschutzrecht anwendbar sei. Die irische Niederlassung sei lediglich eine Anlauf- und Beschwerdestelle, trage jedoch für die Datenverarbeitung keine Verantwortlichkeit.

Würdigung

Die Anwendbarkeit deutschen Datenschutzrechts kann aufgrund des Untersuchungsberichts der irischen Datenschutzaufsicht kritisch hinterfragt werden. Die Befassung der Art-29-Datenschutzgruppe und v.a. die in Schleswig-Holstein anhängigen Gerichtsverfahren können diesbezüglich zur Klärung beitragen.

Im Einzelnen:

Die Datenschutzvorschriften des TMG (§§ 11ff.) finden gemäß § 3 Abs. 3 Nr. 4 TMG, § 1 Abs. 5 Satz 2 BDSG nur Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt.

Im Fall des Like-Buttons und der Fanpage wäre dies der Fall, wenn

- die Betreiber deutscher Webseiten mit Like-Button/Fanpages die Daten erheben und sie dann an Facebook übermitteln oder
- Facebook die Daten durch seine US-Niederlassung *Facebook Inc.* erhebt.

Übermitteln ist gemäß § 12 Abs. 3 TMG, § 3 Abs. 4 Satz 2 Nr. 3 BDSG das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass die Daten an den Dritten weitergegeben werden oder der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft. Erforderlich ist neben einem Bereithalten der Daten, dass Gegenstand der Übermittlung „gespeicherte" oder „durch Datenverarbeitung gewonnene" personenbezogene Daten sind.

Im Hinblick auf den Betreiber einer Webseite mit Like-Button oder einer Fanpage ist dies aber nicht der Fall, da diese den Datenbestand, der Facebook zur Kenntnis gelangt, nicht auf einem Datenträger festhalten, d.h. also nicht „speichern". Der Datenbestand, den Facebook in Bezug auf die IP-Adresse von Nutzern zur Kenntnis erhält, mag inhaltlich der gleiche sein wie ihn auch der Webseitenbetreiber erhält. Er ist jedoch nicht „durch die Hände" des Webseitenbetreibers gegangen und besteht unabhängig von dessen Datensatz. Besonders evident ist die fehlende Speicherung bei den von Facebook gesetzten Cookies. Auf diese hat nur Facebook Zugriff; der Webseitenbetreiber kann sie weder einsehen noch verändern. Die von Facebook empfangenen Daten stellen auch keine unmittelbar „durch Datenverarbeitung gewonnenen" Daten dar, da sie vom Webseiten-/Fanpagebetreiber in keiner Weise für Facebook aufbereitet werden. Ein Übermitteln durch den Webseitenbetreiber erfolgt somit nicht.

Für die Frage, ob Facebook die Daten durch seine US-Niederlassung *Facebook Inc.* erhebt, ist entscheidend, ob die irische Niederlassung *Facebook Ireland Ltd.* eine für die Datenerhebung verantwortliche Stelle ist. Wird dies bejaht, findet gemäß § 1 Abs. 5 Satz 1 BDSG irisches Datenschutzrecht Anwendung, welches die deutschen Datenschutzaufsichtsbehörden gemäß § 1 Abs. 5 Satz 5, § 38 Abs. 1 Satz 1 BDSG ihrer datenschutzrechtlichen Beurteilung zugrunde legen müssten. Gemäß § 12 Abs. 3 TMG, § 3 Abs. 7 BDSG ist verantwortliche Stelle jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt, wobei es darauf ankommt, wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (vgl. Art. 2 lit. d RL 95/46/EG). Die irische Datenschutzauf-

sichtsbehörde hat die Struktur und die Aufgaben von *Facebook Ireland Ltd.* – v.a. im Verhältnis zu *Facebook Inc. USA* – eingehend untersucht. Aus dem Untersuchungsbericht sind folgende Gesichtspunkte besonders hervorzuheben:

- Zwischen *Facebook Ireland Ltd.* und *Facebook Inc. USA* besteht ein „*Data Transfer and Processing Agreement*", in dem Facebook Ireland für Daten von Mitgliedern außerhalb der USA und Kanada als „data exporter" und Facebook Inc. als „data importer" bezeichnet wird.
- *Facebook Ireland Ltd.* hat *Facebook Inc.* durch ein „*Data hostings service agreement*" als Serviceprovider mit der Datenverarbeitung beauftragt.
- Sowohl das „*Data Transfer and Processing Agreement*" als auch das „*Data hostings service agreement*", die beide seit September 2010 gelten, werden als rechtsgültig und wirksam betrachtet.
- *Facebook Ireland Ltd.* (400 Mitarbeiter) führt für Mitglieder außerhalb der USA und Kanada u.a. die Bereiche „Developer Relations", „Site Reliability Operations", „User Operations", „Network Operations" und „Database Operations".

Gerade die (von der irischen Datenschutzaufsicht gewürdigten) vertraglichen Vereinbarungen zwischen *Facebook Ireland Ltd.* und *Facebook Inc.* könnten die Schlussfolgerung zulassen, dass die irische Niederlassung über Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der europäischen Nutzer entscheidet und daher auch für deutsche Nutzer eine datenschutzrechtliche Beurteilung nach irischem Recht erfolgen muss. Die Frage ist bislang noch nicht abschließend geklärt, das ULD ist anderer Auffassung.

Unabhängig von der endgültigen Beantwortung der Frage des anwendbaren Rechts werden nachfolgend die zu prüfenden Fragen auf der Grundlage des deutschen Rechts bewertet. Denn sowohl das ggf. auf Facebook anzuwendende irische als auch das deutsche Recht setzen EU-Recht um, so dass in jedem Fall die gleichen Schutzziele zugrunde liegen.

(2) Personenbezug der erhobenen Daten?

Das ULD ist der Auffassung, dass mit dem Like-Button und bei Fanpages folgende personenbezogenen Daten im Sinne des § 3 Abs. 1 BDSG erhoben und verarbeitet werden:

- die durch die Facebook-Mitglieder gespeicherten persönlichen Informationen,

- die IP-Adressen von Besuchern der Fanpages bzw. der Webseiten mit Like-Button (sowohl bei Facebook-Mitgliedern als auch bei Nicht-Facebook-Mitgliedern),
- die durch Facebook genutzten/gesetzten Cookies (sowohl bei Facebook-Mitgliedern als auch bei Nicht-Facebook-Mitgliedern)

Würdigung

Die durch die Facebook-Mitglieder gespeicherten persönlichen Informationen und der c-user-Cookie sind personenbezogene Daten.

Ob dynamische IP-Adressen generell personenbezogene Daten sind, ist gerichtlich nicht abschließend geklärt. Eine richtlinienkonforme Auslegung könnte für eine Bejahung des generellen Personenbezugs sprechen, sodass für deren Übertragung §§ 11ff. TMG gelten.

Ob der datr-Cookie als personenbezogenes Datum qualifiziert werden kann, für dessen Nutzung dann §§ 11ff. TMG gilt, ist aufgrund des Untersuchungsberichts der irischen Datenschutzaufsicht fraglich, kann aber aufgrund des gegenwärtigen Sachstands nicht mit Sicherheit ausgeschlossen werden. Eine Offenlegung des Inhalts des datr-Cookies durch Facebook gegenüber den deutschen Datenschutzaufsichtsbehörden wäre zu begrüßen.

Im Einzelnen:

Gespeicherte persönliche Informationen der Facebook-Mitglieder:

Die bei der Facebook-Registrierung durch die Nutzer gemachten Angaben wie Name, Alter, Geschlecht und Beruf sind personenbezogene Daten. Beim Besuch einer Webseite mit Like-Button bzw. beim Besuch einer Fanpage durch ein eingeloggtes Facebook-Mitglied kommt es zu einer Verknüpfung mit seinem Account, weswegen eine Identifizierung möglich ist (vgl. Tabelle 1 Fallgruppe 6 und Tabelle 2 Fallgruppe 2) Insoweit werden beim Like-Button und beim Besuch einer Fanpage personenbezogene Daten verarbeitet.

IP-Adressen:

Die Frage nach dem Personenbezug von dynamischen IP-Adressen ist weder auf nationaler noch europäischer Ebene höchstrichterlich entschieden. Die Rechtsprechung der Instanzgerichte ist nicht einheitlich.

Eine Auffassung prüft den Personenbezug relativ und bejaht ihn nur für diejenige datenverarbeitende Stelle, die über Kenntnisse, Mittel und Möglichkeiten (dementsprechend ein etwaiges Zusatzwissen) zur Zuordnung zu einer bestimmten Person verfügt. Dies trifft i.d.R. nur für den Access-Provider (Anbieter des Internetzugangs) zu, da dieser dem Nutzer mit jeder Einwahl die IP-Adresse zuweist und daher über die Mittel und Möglichkeiten der Zuordnung verfügt. Die Anbieter des Webseiteninhalts (wie Facebook und die Betreiber der Webseite mit Like-Button/Fanpagebetreiber) haben dieses Zusatzwissen hingegen nicht. Die andere Auffassung lässt bereits die theoretische Möglichkeit der Bestimmbarkeit einer Person genügen, um generell von einem personenbezogenen Datum auszugehen, auch wenn die Person nur durch einen Dritten bestimmt werden kann und dieser das notwendige Zusatzwissen nicht an die verarbeitende Stelle weitergibt.

Zumindest Erwägungsgrund 26 der EG-Datenschutzrichtlinie 95/46/EG könnte für letztgenannte Auffassung sprechen. Darin heißt es zum Begriff des personenbezogenen Datums in Art. 2 a) der Richtlinie, dass bei der Entscheidung, ob eine Person bestimmbar ist, alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden können, um die betreffende Person zu bestimmen. Daher könnte folglich die Identifizierbarkeit allein durch einen Dritten für eine Bestimmbarkeit ausreichen und ein genereller Personenbezug von dynamischen IP-Adressen zu bejahen sein, sodass die IP-Adresse auch für Facebook und die Webseitenbetreiber/Fanpagebetreiber ein personenbezogenes Datum wäre.

Auch der von der Europäischen Kommission vorgelegte Entwurf einer EU-Datenschutzgrundverordnung lässt insoweit bislang keine eindeutige Festlegung erkennen (Wortlaut des Art. 4 Abs. 1 und Abs. 2 sowie Erwägungsgrund 24).

Cookies:

Ob bei der Nutzung von Cookies von einer Erhebung/Verarbeitung personenbezogener Daten auszugehen ist, hängt davon ab, ob im Cookie als einem Datenpaket/Textdatei personenbezogene Informationen über den Nutzer gespeichert sind. Wenn Cookies personenbezogene Daten enthalten und dem Zweck dienen, personenbezogene Daten zu sammeln, gelten für die Nutzung die Datenschutzvorschriften des TMG.

Der c_user-Cookie enthält die Anmeldekennnummer des Facebook-Mitglieds, d.h. dessen personenbezogene Informationen. Damit kann Facebook eingeloggte Mitglieder identifizieren, was auch gewollt ist, um den Like-Button und die Fanpage mit personalisiertem Inhalt anbieten zu können. Für den c_user-Cookie gelten daher §§ 11ff. TMG.

Nach Angaben von Facebook ist alleiniger Zweck des datr-Cookie, „*böswillige Aktivitäten zu verhindern und unsere Nutzer zu schützen*". Er werde nicht dazu eingesetzt, personenbezogene Daten zu sammeln. Ob die Verwendung des datr-Cookies tatsächlich nur die Abwehr missbräuchlicher Nutzung des sozialen Netzwerks bezweckt, wird von den deutschen Aufsichtsbehörden kritisch hinterfragt. Es werden zum einen erhebliche Zweifel an der Effektivität zur „Missbrauchsabwehr" geäußert. Zum anderen könne bei entsprechender inhaltlicher Gestaltung insbesondere bei Nicht-Facebook-Mitgliedern, bei denen der datr-Cookie einmal gesetzt wurde und die später Mitglied werden, durchaus die Möglichkeit bestehen, personenbezogene Daten zu erheben und Nutzerprofile unter Einbeziehung und Zuordnung der besuchten Webseiten mit Like-Button und Fanpages (vor Mitgliedschaft) zu erstellen; v.a. die zweijährige Geltungsdauer könnte dies nahelegen. Allerdings ist die Einschätzung der irischen Datenschutzaufsicht zur alleinigen „Sicherheitsrelevanz" des datr-Cookie wohl eine andere: diese hat bei ihrer Prüfung keine Anhaltspunkte dafür feststellen können, dass der datr-Cookie der Sammlung personenbezogener Daten dient. Jedoch ist dabei nicht zu verkennen, dass Facebook den genauen Inhalt des datr-Cookie bislang zumindest gegenüber den deutschen Aufsichtsbehörden nicht offengelegt hat.

(3) Verantwortlichkeit der Betreiber von Webseiten mit Like-Button und der Betreiber von Fanpages?

Das ULD ist der Auffassung, dass diese neben Facebook die rechtliche Verantwortung für die Einhaltung der Datenschutzvorschriften des TMG tragen. Diese Verantwortung stellt auch der Beschluss des Düsseldorfer Kreises zu Sozialen Netzwerken vom 8. Dezember 2011 heraus.

Würdigung

Beim Like-Button ist für die Webseitenbetreiber zumindest eine datenschutzrechtliche Mitverantwortung gut begründbar. Bei Fanpages kann man diese in Frage stellen, allerdings lässt sich nicht ausschließen, dass deutsche Gerichte auf die Einflussnahmemöglichkeit hinsichtlich des Ob der Datenverarbeitung abstellen.

Im Einzelnen:
Eine Verantwortlichkeit, die sich für die Datenschutzvorschriften des TMG nach § 3 Abs. 7 BDSG richtet, kommt für Webseitenbetreiber/Fanpage-Betreiber in Betracht, wenn

- sie selbst personenbezogene Daten erheben, verarbeiten oder nutzen,
- Facebook durch den Like-Button bzw. mit der Fanpage im Auftrag der Webseitenbetreiber/Betreiber von Fanpages personenbezogene Daten erhebt oder
- Facebook und die Webseitenbetreiber/Betreiber von Fanpages eine gemeinsame Verantwortung tragen.

Erhebung/Verarbeitung durch Webseitenbetreiber/Fanpage-Betreiber:
Die Datenflüsse erfolgen unmittelbar an Facebook. Eine Verarbeitung in Form einer Datenübermittlung durch den Webseitenbetreiber/Fanpage-Betreiber findet wie oben dargelegt nicht statt.

Auftragsdatenverarbeitung durch Facebook:
Beim Like-Button könnte dies deshalb in Betracht kommen, weil Facebook den Webseitenbetreibern den Dienst „Facebook Insights" zur Verfügung stellt, mit dem diese Informationen zur Reichweite der Nutzung ihrer Webseite erlangen können. Allerdings ist die Bereitstellung von „Facebook Insights" im Hinblick auf die sonstigen Funktionen des Like-Buttons nicht Hauptzweck der Vertragsbeziehung. Insbesondere steht für Facebook beim Like-Button im Vordergrund, seinen Mitgliedern Zusatzfunktionen im Sinne einer erleichterten Kommunikation mit Facebook-Freunden und einer Personalisierung von Webseiteninhalten anzubieten, und durch die zunehmende Präsenz des Like-Buttons verstärkt neue Mitglieder zu werben. Die Tätigkeit von Facebook im Zusammenhang mit dem Like-Button wird damit nicht nur durch die für die Auftragsdatenverarbeitung kennzeichnenden Merkmale eines Über-/Unterordnungsverhältnisses oder bloßer Hilfsfunktionen für einen Webseitenbetreiber geprägt.

Bei den Fanpages spricht für eine Auftragsdatenverarbeitung, dass ein eigener Internetauftritt des Betreibers unter der Oberfläche von Facebook vorliegt und dass Facebook die technischen Möglichkeiten zur Verfügung stellt, damit z.B. Kommentare auf der Pinnwand gepostet werden können. Gegen eine Auftragsdatenverarbeitung spricht, dass der Betreiber nur sehr geringe Einflussmöglichkeiten auf die optische Gestaltung einer Fanpage und v.a. die ihm zur Verfügung stehenden Funktionen hat. Zudem ist die Fanpage eine Facebook-Domain, der Dienst „Facebook Insights" wird

kostenlos zur Verfügung gestellt. Allerdings wurde das rechtliche Verhältnis zwischen Fanpage-Betreiber und Facebook von den deutschen Aufsichtsbehörden – soweit ersichtlich – noch nicht näher untersucht. Deren Einschätzung, dass Facebook die Nutzungsbedingungen für Fanpages strikt vorgibt und keine Abweichungen verhandelbar sind, dürfte jedoch schwer widerlegbar sein. Hierfür sprechen die Marktmacht von Facebook sowie dessen bestehende Intention einer einheitlichen Optik und Funktionalität von Facebook-Seiten.

Gemeinsame datenschutzrechtliche Verantwortung:
In richtlinienkonformer Auslegung von § 3 Abs. 7 BDSG kann ein Selbsterheben, -verarbeiten und -nutzen auch vorliegen, wenn die Erhebung, Verarbeitung oder Nutzung zwar durch eine andere Stelle erfolgt, jedoch diese nicht allein über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, sondern eine gemeinsame Entscheidung vorliegt (vgl. Art. 2 lit. d RL 95/46/EG).

Die Art-29-Datenschutzgruppe hat sich zur gemeinsamen Verantwortlichkeit eines Webseitenbetreibers geäußert, der den Betreibern sog. Werbenetzwerken seine Webseite zur Verfügung stellt. Für die Datenerhebung durch die Betreiber der Werbenetzwerke wurde für die Webseitenbetreiber, die die Werbung technisch ermöglichen, eine datenschutzrechtliche Mitverantwortung hinsichtlich der Verpflichtungen zur Unterrichtung der Nutzer über die Zwecke und Mittel der Datenverarbeitung bejaht. Beim Like-Button ist die Konstellation vergleichbar. Die Dienstleistungen von Facebook sind zwar kostenlos, der Platz für das Social Plugin wird daher auch nicht „vermietet", allerdings trifft ein Webseitenbetreiber durch die Einbindung eines Like-Buttons die technischen Voraussetzungen für die Datenerhebung durch Facebook, welches zumindest bei eingeloggten Mitgliedern eine personalisierte Einblendung des Like-Buttons zur Steigerung der Attraktivität des Netzwerks bezweckt. Bei Fanpages ist die Konstellation hingegen nicht vergleichbar. Hier werden die technischen Voraussetzungen für die Datenerhebung durch Facebook selbst geschaffen; lediglich der Inhalt der Fanpage stammt von deren Betreiber. Jedoch lehnt die Art-29-Datenschutzgruppe in einer weiteren Stellungnahme eine (gemeinsame) Verantwortung nur ab, wenn eine Stelle weder rechtlichen noch tatsächlichen Einfluss auf die Entscheidung hat, wie personenbezogene Daten verarbeitet werden. Bei den Fanpages ist zumindest ein tatsächlicher Einfluss vorhanden, weil die Betreiber auf die Errichtung der Fanpage verzichten und dadurch das Ob der Datenerhebung maßgeblich steuern können. Ob dies die Art-29-Datenschutzgruppe in ihrer Einschätzung auch so sieht, ist aber eher fraglich. Sie setzt wohl die Entscheidung über das Ob der

Datenverarbeitung voraus und stellt auf den rechtlichen und tatsächlichen Einfluss auf das Wie der Datenverarbeitung ab. Ein solcher Einfluss des Fanpage-Betreibers ist aber wie oben dargelegt mehr als fraglich. Allerdings lässt sich nicht ausschließen, dass deutsche Gerichte in einem Erst-Recht-Schluss auf die Einflussnahmemöglichkeit hinsichtlich des Ob der Datenverarbeitung abstellen könnten.

(4) Verstoß gegen § 15 Abs. 3 TMG wegen „Facebook Insights" und/oder Setzen/Übertragen von Cookies?

Das ULD bejaht im Hinblick auf den beim Like-Button und bei Fanpages angebotenen Dienst „Facebook Insights" die Anwendbarkeit der Profilbildungsregelung in § 15 Abs. 3 TMG. Zum einen sieht es mangels unstreitig nicht angebotener Widerspruchsmöglichkeit einen Verstoß gegen § 15 Abs. 3 Satz 1 und 2 TMG. Zum anderen bejaht das ULD einen Verstoß gegen § 15 Abs. 3 Satz 3 TMG, d.h. eine unzulässige Zusammenführung der Nutzungsprofile mit den Daten über den Träger des Pseudonyms. Zudem äußert auch der Hamburgische Beauftragte für den Datenschutz aufgrund einer Prüfung den Verdacht, dass durch die Nutzung des datr-Cookies Trackingprofile der Nutzer erstellt würden, die ohne entsprechenden Hinweis auf das hiergegen bestehende Widerspruchsrecht nicht zulässig seien.

Würdigung

Die Anwendbarkeit von § 15 Abs. 3 TMG in Bezug auf „Facebook Insights" ist noch nicht abschließend geklärt.

Hinsichtlich des Setzens und Übertragens von Cookies stehen sich die Befunde der irischen Datenschutzaufsicht und des Hamburger Datenschutzbeauftragten gegenüber. Eine Offenlegung des Inhalts des datr-Cookies durch Facebook gegenüber den deutschen Aufsichtsbehörden wäre zu begrüßen.

Insgesamt darf nicht verkannt werden, dass seitens des ULD der Verstoß gegen § 15 Abs. 3 TMG den Hauptvorwurf bildet und insoweit eine erste gerichtliche Klärung in den bereits in Schleswig-Holstein anhängigen Verfahren noch aussteht.

Im Einzelnen:

Ob mit „Facebook Insights" ein pseudonymisiertes Nutzungsprofil im Sinne von § 15 Abs. 3 Satz 1 TMG verbunden ist, welches auch für die Anwendbarkeit des § 15 Abs. 3 Satz 3 TMG zwingende Voraussetzung ist, ist unklar. Ein Profil ist eine zielgerichtete Verknüpfung von personenbezogenen Daten durch ein logisches zueinander in Beziehung setzen, wodurch zumindest eine Wiedergabe des Teilabbilds der Persön-

lichkeit erfolgt. Die im ULD-Arbeitspapier vom 19. August 2011 enthaltenen Auszüge aus „Facebook Insights“ zeigen, dass Einzelstatistiken zu verschiedensten Punkten der Nutzung von Like-Button und Fanpage zur Verfügung gestellt werden und diese jeweils auf die Gesamtheit der Nutzer bezogen sind. Ein Profil als (pseudonymisierte) Wiedergabe des Teilabbilds der Persönlichkeit eines Nutzers ist hiermit wohl nicht verbunden. Dies wäre eher der Fall, wenn z.B. Informationen darüber bereitgestellt würden, wie viele männliche deutsche Nutzer der Altersgruppe XX aus X eine Seite mit Like-Button oder eine Fanpage auf welche Weise bedienen (Beitragsaufrufe, Beitrag „gefällt mir“, Kommentierte Beiträge, Pinnwandeinträge etc.). „Facebook Insights“ ist eher eine Nutzungsstatistik, aber kein Nutzungsprofil.
In Bezug auf beim Like-Button gesetzte und übertragene Cookies hat die irische Datenschutzaufsicht ausgeführt, dass es damit technisch sowohl bei Facebook-Mitgliedern (unabhängig, ob eingeloggt oder nicht) als auch bei Nicht-Facebook-Mitgliedern möglich sei, Profile der Nutzer zu erstellen. Man habe jedoch bei einer technischen Analyse keine Anhaltspunkte für eine solche Nutzung feststellen können. Sollte sich dieser Befund als zutreffend herausstellen, würde zumindest ein Verstoß gegen § 15 Abs. 3 Satz 3 TMG unabhängig von der Frage, ob „Facebook Insights“ überhaupt ein Nutzungsprofil darstellt, ausscheiden, da dann eine Zusammenführung im Sinne dieser Bestimmung ausgeschlossen werden könnte. Der Hamburgische Datenschutzbeauftragte kommt hier zu einem anderen Ergebnis (Pressemitteilung vom 2. November 2011). Die Erörterung des irischen Untersuchungsberichts in Rahmen der Art-29-Datenschutzgruppe wird hier möglicherweise Klarheit bringen. Es sollte jedoch nicht verkannt werden, dass Facebook insbesondere den genauen Inhalt des datr-Cookie bislang zumindest gegenüber den deutschen Aufsichtsbehörden nicht offengelegt hat.

(5) Cookies nur noch mit Einwilligung des Nutzers?
Hintergrund ist die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009, die u.a. die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (E-Privacy-Richtlinie) ändert und die von den Mitgliedstaaten bis zum 25. Mai 2011 umzusetzen war.

Art. 5 Abs. 3 RL 2002/58/EG i.d.F. der RL 2009/136/EG in Verbindung mit Erwägungsgrund 66 der RL 2009/136/EG sieht für die Verwendung von Cookies grundsätzlich das Erfordernis einer Einwilligung des Nutzers vor, es sei denn, dass diese unbedingt erforderlich sind, damit der Anbieter eines Dienstes der Informationsge-

sellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann. Wenn es technisch durchführbar und wirksam ist, kann die Einwilligung des Nutzers über die Handhabung der entsprechenden Einstellungen eines Browsers oder einer anderen Anwendung ausgedrückt werden.

Im August 2011 wurde vom Bundesrat der Entwurf eines Gesetzes zur Änderung des TMG eingebracht (BT-Drs. 17/6765). In der Stellungnahme der Bundesregierung äußerte diese, dass derzeit geprüft werde, wie durch eine Regelung im TMG Art. 5 Abs. 3 der (geänderten) E-Privacy-Richtlinie umgesetzt werden könne. Die Bundesregierung werde dem Bundestag hierzu im Zuge der bereits im parlamentarischen Verfahren befindlichen Novellierung des Telekommunikationsgesetzes (TKG) eigene Vorschläge unterbreiten. Die Novellierung des TKG wurde mittlerweile nach Anrufung des Vermittlungsausschusses Anfang Februar 2012 abgeschlossen (BT-Drs. 17/5707, BT-Drs. 17/7521, BT-Drs. 17/8569). Vorschläge der Bundesregierung zur TMG-Änderung wurden in diesem Verfahren nicht vorgelegt. Im ursprünglichen Gesetzentwurf der Bundesregierung zur TKG-Novellierung heißt es, dass Einzelfragen der Umsetzung der Änderung von Art. 5 Abs. 3 E-Privacy-Richtlinie derzeit Gegenstand umfangreicher Konsultationen auf europäischer Ebene seien, die auch Selbstregulierungsansätze umfassten. Das Ergebnis dieses Prozesses werde vor einer Entscheidung über weitergehenden gesetzgeberischen Handlungsbedarf abgewartet. Bei der Beratung des Gesetzentwurfs zur TKG-Änderung im federführenden Ausschuss für Wirtschaft und Technologie wurden seitens der Fraktionen SPD und Bündnis 90/DIE GRÜNEN ein Entschließungsantrag zur Umsetzung der Änderungen der E-Privacy-Richtlinie gestellt und festgestellt, dass die von der Bundesregierung angekündigten Vorschläge zur Umsetzung von Art. 5 Abs. 3 E-Privacy-Richtlinie nicht vorlägen (Ausschussdrucksache 17(9)684). Der Antrag fand im Ausschuss keine Mehrheit. Ein aktueller Gesetzentwurf der Fraktion der SPD vom Januar 2012 zur Änderung des TMG mit dem Ziel der Umsetzung des Art. 5 Abs. 3 der E-Privacy-Richtlinie (BT-Drs. 17/8454) wurde Ende Januar 2012 eingebracht. Nach Beschlussempfehlung des Wirtschaftsausschusses vom 1. März 2012 wird Ablehnung vorgeschlagen (BT-Drs. 17/8814).

Vor diesem Hintergrund ist zumindest für die nachfolgende Beurteilung der Rechtsfragen Folgendes festzuhalten:

1. Eine unmittelbare Wirkung der Richtlinie 2009/136/EG kann nach Ablauf der Umsetzungsfrist weder sicher angenommen noch ausgeschlossen werden. Nach der ständigen Rechtsprechung des EuGH kann sich zwar der Einzelne in Fällen, in de-

nen die Bestimmungen einer Richtlinie inhaltlich unbedingt und hinreichend genau sind, vor den nationalen Gerichten gegenüber dem Mitgliedstaat auf diese Bestimmungen berufen, wenn der Mitgliedstaat die Richtlinie nicht fristgemäß oder unzulänglich in nationales Recht umgesetzt hat. Eine unmittelbare Wirkung einer Richtlinie wurde bislang jedoch ausgeschlossen, wenn sie nicht nur eine Begünstigung des Bürgers bedeutet, sondern auch zu einer Verpflichtung oder Belastung einer nichtstaatlichen Stelle führen würde. Der Grundsatz der Rechtssicherheit, so bislang der EuGH, steht der Begründung von Verpflichtungen für den Einzelnen durch Richtlinien entgegen, sodass gegenüber dem Einzelnen die Bestimmungen einer Richtlinie nur Rechte begründen können. Die Rechtsprechung des EuGH geht bislang davon aus, dass der Einzelne sich nicht gegenüber einem Mitgliedstaat auf eine Richtlinie berufen kann, wenn mit der Erfüllung dieser Richtlinie eine unmittelbare Inpflichtnahme eines Dritten verbunden ist (EuGH, Urteil vom 07.01.2004, Rs. C-201/02 – Wells – Rn. 56 m.w.N.). Bei einer direkten Anwendung von Art. 5 Abs. 3 RL 2002/58/EG in der Fassung der RL 2009/136/EG käme es aber gerade zu einer solchen unmittelbaren Inpflichtnahme.

Die Richtlinien, deren unmittelbare Horizontalwirkung der EuGH bislang mit Verweis auf den Grundsatz der Rechtssicherheit abgelehnt hatte (s.o.), datieren jedoch – soweit ersichtlich – aus der Zeit vor Inkrafttreten des Vertrags von Maastricht, als eine Veröffentlichung von Richtlinien im Amtsblatt der EU nicht vorgesehen war. Es ist nicht auszuschließen, dass nunmehr, nachdem auch für Richtlinien die Veröffentlichung im Amtsblatt zwingend vorgeschrieben (Art. 297 Abs. 1 AEUV) und damit Publizität hergestellt ist, der EuGH eine unmittelbare Horizontalwirkung von Richtlinien bejaht, soweit auch die übrigen Voraussetzungen für eine unmittelbare Geltung erfüllt sind.

2. Die (geänderte) E-Privacy-Richtlinie ist wohl dahingehend auszulegen, dass eine Einwilligung zum Setzen von Cookies nicht erforderlich ist, wenn dies nicht die Erhebung personenbezogener Daten bezweckt, d.h. Cookies keine personenbezogenen Daten enthalten. Dies ergibt sich aus deren Anwendungsbereich, der die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation umfasst.

3. Eine Einwilligung ist zumindest dann nicht erforderlich, wenn ein Cookie unverzichtbar ist, um die Nutzung eines vom Nutzer ausdrücklich angeforderten Dienstes zu ermöglichen.

(6) Zulässigkeit der Übertragung und Speicherung der generischen IP-Adresse?

Die Übertragung und Speicherung der generischen IP-Adresse ist nach gegenwärtigem Sachstand nach § 15 Abs. 1 Satz 1 TMG zulässig. Sehr zweifelhaft ist jedoch, ob diesbezüglich auch die Unterrichtungspflicht nach § 13 Abs. 1 Satz 1 TMG insbesondere gegenüber Nicht-Facebook-Mitgliedern ausreichend erfüllt wird.

Im Einzelnen:

Rechtsgrundlage für die nicht-anonymisierte Übertragung der IP-Adresse des Nutzers an Facebook ist § 15 Abs. 1 TMG. Danach darf der Diensteanbieter personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten). Wie oben dargelegt kann – obwohl gerichtlich nicht abschließend geklärt – die Einordnung der IP-Adresse als generell personenbezogenes Datum nicht ausgeschlossen werden. Aus technischer Sicht ist die Übertragung der IP-Adresse erforderlich. Nur durch die Übertragung kann Facebook den Like-Button und die Fanpage mit Inhalt darstellen. Dass einem Nicht-Facebook-Mitglied die (Facebook-)Funktion durch den Besuch der Webseite mit Like-Button oder der Fanpage letztlich „aufgedrängt" wird, ändert an der Erforderlichkeit nichts. Ein Vertragsverhältnis zwischen Telemedienanbieter und Nutzer muss bei § 15 Abs. 1 Satz 1 TMG – im Gegensatz zu § 14 TMG – nicht vorliegen. Durch die über das Ende des Nutzungsvorgangs hinausgehende Speicherung als generische IP-Adresse liegt auch kein Verstoß gegen § 15 Abs. 4 Satz 1 TMG vor, weil durch die Anonymisierung keine Nutzungsdaten gemäß § 15 Abs. 1 Satz 1 TMG mehr vorliegen. Nur diese wären nach Ende des Nutzungsvorgangs zu löschen. Hier darf jedoch nicht verkannt werden, dass die Anonymisierung von Facebook vorgetragen wird und noch nicht abschließend verifiziert ist.

Auch bei einer Datenerhebung nach § 15 Abs. 1 Satz 1 TMG hat der Diensteanbieter die Unterrichtungspflicht nach § 13 Abs. 1 Satz 1 TMG zu erfüllen. Unabhängig von der Frage des anwendbaren Rechts auf Facebook trifft diese Pflicht mitverantwortlich auch den Webseitenbetreiber, der den Like-Button einbettet, und – auch wenn man dies eher in Frage stellen kann – den Betreiber der Fanpage. Gerade ein Nicht-Facebook-Mitglied wird jedoch beim Besuch einer Webseite mit Like-Button oder einer Fanpage mangels Kenntnis der Datenschutzerklärung und den Nutzungsbedingungen von Facebook jedenfalls keine Kenntnis über die Übertragung der IP-Adresse an Facebook erlangen.

(7) Zulässigkeit der Speicherung der spezifischen IP-Adresse?

Die Speicherung der spezifischen IP-Adresse bedarf wohl einer informierten Einwilligung und kann nicht auf § 14 oder § 15 TMG gestützt werden. Die Zustimmung zu den Datenverwendungsrichtlinien von Facebook kann als Einwilligung gelten, wobei allerdings die Wahrung der auch diesbezüglich geltenden Unterrichtungspflichten nach § 13 Abs. 1 Satz 1 TMG unterschiedlich beurteilt werden kann.

Im Einzelnen:

Für die Speicherung der spezifischen IP-Adresse bei zunächst nicht-eingeloggten Facebook-Mitgliedern, die einen Like-Button bestätigen (und sich dadurch i.d.R. einloggen werden), sowie bei eingeloggten Facebook-Mitgliedern, die eine Webseite mit Like-Button besuchen, ist wohl eine (informierte) Einwilligung des Facebook-Mitglieds erforderlich. § 14 Abs. 1 TMG, wonach der Diensteanbieter personenbezogene Daten eines Nutzers erheben und verwenden darf, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind (Bestandsdaten), scheidet als Rechtsgrundlage aus. Die Erforderlichkeit der Erhebung und Verwendung von Bestandsdaten wird von der herrschenden Auffassung eng ausgelegt und nur bejaht, wenn sie für die Gestaltung des Telemediendienstevertrags unerlässlich ist. Für die Inanspruchnahme der Funktionalität Like-Button ist die Speicherung der spezifischen IP-Adresse jedoch nicht unerlässlich, da diese auch ohne sie technisch umsetzbar ist. Auch § 15 Abs. 1 TMG kommt für die Speicherung nicht in Betracht, da die spezifische IP-Adresse als Nutzungsdatum nach Ende des Nutzungsvorgangs zu löschen ist (§ 15 Abs. 4 Satz 1 TMG); aufgrund der Unentgeltlichkeit von Facebook ist die Speicherung gerade nicht für Zwecke der Abrechnung mit dem Nutzer erforderlich.

Maßgeblich für die hiernach erforderliche Einwilligung sind die „Datenverwendungsrichtlinien" von Facebook, denen bei Registrierung zugestimmt werden muss. Diese enthalten verschiedene Themenrubriken mit anklickbaren und z.T. untereinander verlinkten Untermenüs. Unter den Rubriken „*Daten, die wir über dich erhalten*", „*Wie wir uns bereitgestellte Daten verwenden*" und „*Teilen von Inhalten mit anderen Webseiten und Anwendungen – Über soziale Plug-ins*" werden Informationen u.a. über die Speicherung der mit den sozialen Plug-ins gesammelten Daten (hierzu gehören auch die IP-Adressen) bereitgehalten. Über den Verwendungszweck werden pauschale Aussagen getroffen, die v.a. auf die Ermöglichung eines sozialeren und persönlichen Nutzungserlebnisses abstellen. Ob dies den auch für die Einwilligung geltenden An-

forderungen an die Transparenz einer Unterrichtung nach § 13 Abs. 1 Satz 1 TMG genügt, wird unterschiedlich beurteilt. Allerdings sollten an eine Unterrichtung in allgemein verständlicher Form auch keine zu hohen Anforderungen gestellt werden: gerade eine zu große Detailliertheit wäre für die allgemeine Verständlichkeit eher abträglich.

(8) Zulässigkeit des Setzens/der Übertragung des datr-Cookie?

Die Einordnung des datr-Cookie als personenbezogenes Datum kann nach gegenwärtigem Sachstand nicht ausgeschlossen werden. Bejaht man den Personenbezug, ist die Übertragung eines gesetzten datr-Cookies beim Like-Button ohne Einwilligung unzulässig, wenn Nutzer (Facebook-Mitglieder und Nicht-Mitglieder) in der Folge beim Besuch von Webseiten mit Like-Button diesen nicht klicken.

Ansonsten ist das Setzen und Übertragen des datr-Cookies nach § 15 Abs. 1 TMG zulässig, sofern sich die Befunde der irischen Datenschutzaufsicht zur ausschließlichen Sicherheitsrelevanz des datr-Cookies als zutreffend erweisen. Der Hamburger Datenschutzbeauftragte ist hier anderer Auffassung. Eine Offenlegung des Inhalts des datr-Cookies durch Facebook gegenüber den deutschen Datenschutzaufsichtsbehörden wäre zu begrüßen.

Im Einzelnen:
Wie oben darlegt kann die Einordnung des datr-Cookie als personenbezogenes Datum nach gegenwärtigem Sachstand nicht ausgeschlossen werden.

Für den Fall, dass weitere Untersuchungen einen Personenbezug des datr-Cookie bestätigen sollten, gilt neben den unter (4) dargelegten Fragen zur Nichtanwendbarkeit der Profilbildungsregelung in § 15 Abs. 3 TMG Folgendes:

- Bei Nicht-Facebook-Mitgliedern, die mehrmals Like-Buttons klicken oder Fanpages besuchen, sowie bei Facebook-Mitgliedern, die sich anlässlich der Bestätigung des Like-Buttons oder der Bedienung einer Fanpage einloggen, bzw. im eingeloggten Zustand Webseiten mit Like-Button oder Fanpages besuchen, mag das Setzen und die spätere Übertragung des datr-Cookies nach § 15 Abs. 1 Satz 1 TMG zulässig sein. Mit dem Klicken des Like-Buttons bzw. dem Besuch der Fanpage wird die Facebook-Plattform geöffnet mit der Möglichkeit, sich zu registrieren und einzuloggen, und damit auch mit der Möglichkeit, sich mit der Identität eines Facebook-Mitglieds missbräuchlich einzuloggen. Mit dem Übertragen des datr-Cookies will Facebook solche Versuche verhindern, um dadurch seine re-

gistrierten Nutzer zu schützen. Insoweit ließe sich von einer Erforderlichkeit zur Ermöglichung der Inanspruchnahme von Facebook sprechen, da hierzu auch die Nutzung unter Ausschluss von Missbrauch gehört.

- Vor diesem Hintergrund ist dann aber beim Like-Button nicht ersichtlich, dass eine Übertragung des beim ersten Klicken eines Like-Buttons sowohl bei Facebook-Mitgliedern als auch bei Nicht-Facebook-Mitgliedern gesetzten datr-Cookies auch erforderlich ist, wenn bei späteren Besuchen von Webseiten mit Like-Buttons diese nicht geklickt werden. Hier erfolgt nämlich jeweils kein Anmeldeversuch bei Facebook, der die Gefahr einer missbräuchlichen Nutzung herbeiführen würde. § 15 Abs. 1 Satz 1 TMG kann daher nicht als Rechtsgrundlage herangezogen werden. Vielmehr bedarf es – unabhängig von den Vorgaben der E-Privacy-Richtlinie – einer Einwilligung des Nutzers.

(9) Zulässigkeit der Übertragung des c_User-Cookie?

Die Übertragung des c_User-Cookie kann auf § 15 Abs. 1 Satz 1 TMG gestützt werden. Es gilt die spezielle Unterrichtungspflicht nach § 13 Abs. 1 Satz 2 TMG. Hier besteht unter dem Gesichtspunkt der Transparenz Verbesserungsbedarf.

Im Einzelnen:
Die Übertragung des c_user-Cookies bei eingeloggten Facebook-Mitgliedern (beim Like-Button als auch bei Fanpages) kann auf § 15 Abs. 1 Satz 1 TMG gestützt werden, da sie gerade erforderlich ist, um für Facebook-Mitglieder die personalisierte Nutzung des Like-Button/der Fanpage zu ermöglichen. Unabhängig von der – abzulehnenden – horizontalen Drittwirkung der E-Privacy-Richtlinie ist das Setzen/Übertragen des c-user-Cookie weiter auf der Grundlage von § 15 Abs. 1 Satz 1 TMG möglich und nicht erst aufgrund einer Einwilligung zulässig. Damit Facebook die von seinen Nutzern ausdrücklich gewünschte personalisierte Darstellung einer Fanpage zur Verfügung stellen kann, ist der c_user-Cookie unverzichtbar, sodass auch nach der Richtlinie eine Ausnahme vom Einwilligungserfordernis greift.

Für den c_user-Cookie ist die spezielle Unterrichtungspflicht nach § 13 Abs. 1 Satz 2 TMG einschlägig. Der c_user-Cookie ermöglicht nämlich eine spätere Identifizierung des Facebook-Mitglieds und dient daher auch der Vorbereitung der Erhebung/Verwendung personenbezogener Daten. Insoweit kommt es darauf an, ob Facebook seine Mitglieder zu Beginn des Verfahrens über solche personalisierten Inhalte mit Hilfe der Nutzung von Cookies unterrichtet oder dies bei der Registrierung bereits in allgemeiner Form getan hat. Solche Hinweise gibt Facebook tatsächlich; diese

sind aber unter dem Gesichtspunkt der Transparenz verbesserungswürdig. In den „Datenverwendungsrichtlinien" erhält der Nutzer diese Hinweise nur versteckt unter der Rubrik „*Was du sonst noch wissen solltest*", Unterrubrik „*Cookies*" mit einem Link auf „*Hilfebereich*" unter der Rubrik „*Etwas funktioniert nicht - Cookies*" (dort allerdings in gut verständlicher Form).

V. Ausblick – weitere Entwicklung

Neben Social Plugins und Fanpages sind weitere technische Entwicklungen und Änderungen der Geschäftspraktiken der Sozialen Netzwerke Gegenstand intensiver datenschutzrechtlicher Diskussionen. So untersucht die Art-29-Datenschutzgruppe mit dem Ziel eines abgestimmten Vorgehens der europäischen Datenschutzaufsichtsbehörden die Änderungen der Nutzungsbedingungen bei Google, die für die Nutzer eine Zusammenführung der über sie bei den einzelnen Google-Diensten – darunter auch das Soziale Netzwerk Google+ – gespeicherten Daten ohne Widerspruchsmöglichkeit vorsehen. Bei Facebook ist zu erwarten, dass die jetzt eingefügte Funktion einer umfassenden digitalen Nutzerbiographie („Timeline") noch eingehender datenschutzrechtlicher Untersuchung unterzogen wird. Das gleiche gilt für die von Facebook beabsichtigte, von vielen Nutzern abgelehnte und von Datenschützern kritisierte Änderung der Nutzungsbedingungen („Datenverwendungsrichtlinien").

Die Ergebnisse dieser laufenden Untersuchungen der zuständigen unabhängigen Datenschutzaufsichtsbehörden sind derzeit weder auf nationaler noch auf europäischer Ebene absehbar. So steht die endgültige Entscheidung der irischen Datenschutzaufsicht über die konkret zu einzelnen Funktionen von Facebook erhobenen Beschwerden noch aus. Der Untersuchungsbericht zeigt aber bereits auf, dass in vielen Bereichen Verbesserungen bei der Transparenz der Datenerhebung angemahnt werden, hinsichtlich derer Facebook erste Zusagen gemacht hat. Ebenfalls noch nicht abgeschlossen sind die vom Bundesminister des Innern im November 2011 initiierten, unter Federführung der Freiwilligen Selbstkontrolle Multimedia-Diensteanbieter (FSM) geführten Verhandlungen über eine Selbstverpflichtung der Betreiber Sozialer Netzwerke.

Vor diesem Hintergrund beschränken sich die nachfolgenden gemeinsamen Vorschläge des AK I auf die in der Berichtsbitte der CdS-Jahreskonferenz in den Mittelpunkt gestellte Nutzung von Social Plugins und Fanpages.

VI. Gemeinsame Vorschläge des AK I

Die unter Ziffer IV.3. dargestellte Würdigung der einzelnen Sach- und Rechtsfragen zeigt, dass die datenschutzkonforme Ausgestaltung der Nutzung von Social Plugins wie dem Like-Button sowie von Fanpages sowohl in tatsächlicher Hinsicht –weitere Auskünfte von Facebook insbesondere zu Nutzung und Verwendungszweck von Cookies – als auch in rechtlicher Hinsicht – insbesondere bezüglich der Unterrichtungspflichten nach dem TMG und Erfordernis von Einwilligungen in bestimmten Fallkonstellationen – noch nicht abschließend geklärt ist. Die Würdigung bestimmter Rechtsfragen hängt dabei von der Klärung tatsächlicher Fragen ab. Der Untersuchungsbericht der irischen Datenschutzaufsichtsbehörde gibt für diese Klärung Anhaltspunkte, kann aber nicht als abschließende Klärung auch im Verhältnis zu den deutschen Aufsichtsbehörden und in den bereits anhängigen gerichtlichen Verfahren gelten.

Aufgrund dieses Sach- und Rechtsstands ergeben sich gegenwärtig folgende Vorschläge und Empfehlungen betreffend die Nutzung von Social Plugins und Fanpages durch öffentliche Stellen:

1. Öffentliche Stellen trifft bei der Öffentlichkeitsarbeit mittels Sozialer Netzwerke die Pflicht, hierbei sorgfältig auf ein hohes Datenschutzniveau zu achten. Bei Social Plugins wie dem Like-Button kann diese datenschutzrechtliche Mitverantwortung neben den Betreibern der Sozialen Netzwerke bereits aus den einfachgesetzlichen Bestimmungen des Telemediengesetzes und des Bundesdatenschutzgesetzes abgeleitet werden. Bei Fanpages sollte eine solche Mitverantwortung zumindest aufgrund einer „Vorbildfunktion“ des Staates bejaht werden, der das Recht auf informationelle Selbstbestimmung seiner Bürgerinnen und Bürger schützen sollte.
2. Diese datenschutzrechtliche Mitverantwortung legt nahe, Gefährdungen der informationellen Selbstbestimmung durch neue Technologien und Vorteile bei der sachgerechten Erfüllung öffentlicher Aufgaben wie der Wahrnehmung des Informationsauftrags öffentlicher Stellen sorgsam gegeneinander abzuwägen. Es sollte dabei nicht verkannt werden, dass für den Betreiber des Sozialen Netzwerks, der notwendigerweise in die Öffentlichkeitsarbeit der öffentlichen Stelle eingebunden ist, personenbezogene Daten und deren Nutzung für Werbezwecke die Währung sind, mit der Bürgerinnen und Bürger für die „unentgeltliche“ Bereitstellung von Sozialen Netzwerken tatsächlich bezahlen. Dies gilt umso mehr, als bei Social Plugins und Fanpages auch

Bürgerinnen und Bürger betroffen sind, die die Nutzung Sozialer Netzwerke für sich bislang nicht in Betracht ziehen.

3. Zur Minimierung der Gefährdungen für die informationelle Selbstbestimmung bei der Nutzung von Social Plugins und Fanpages trifft die Betreiber der Sozialen Netzwerke die Hauptverantwortung. Zur Wahrung dieser Verantwortung wäre ein mit den Datenschutzaufsichtsbehörden abzustimmendes Maßnahmenkonzept begrüßenswert. Für die Erarbeitung und Vorlage eines solchen Maßnahmenkonzepts bieten die gegenwärtig laufenden, vom Bundesminister des Innern im November 2011 initiierten Beratungen zu einem allgemeinen Datenschutzkodex für Soziale Netzwerke Gelegenheit. Diese Beratungen unter Federführung der Freiwilligen Selbstkontrolle Multimedia-Diensteanbieter (FSM) sollten ausdrücklich um die Gesichtspunkte Social Plugins und Fanpages erweitert werden. Die Einbeziehung der Datenschutzaufsichtsbehörden in diesen Beratungsprozess ist hierbei von großer Wichtigkeit.

   Ein Maßnahmenkonzept sollte insbesondere folgende Defizite aufgreifen und Lösungsmöglichkeiten aufzeigen:

   - Technische Abläufe bei Social Plugins und Fanpages sind gegenüber den deutschen Aufsichtsbehörden umfassend offenzulegen (insbesondere Nutzungszweck von Cookies).
   - Die Erstellung von Nutzerprofilen durch den Besuch von Webseiten mit Like-Button und von Fanpages ist insbesondere im Hinblick auf Nichtnutzer von Sozialen Netzwerken auszuschließen. Die Nachprüfbarkeit durch die Datenschutzaufsicht sollte hierbei sichergestellt sein.
   - Im Interesse einer umfassenden Gewährleistung der informationellen Selbstbestimmung sollte bei jeder Art von Statistikverfahren betreffend die Reichweite der Nutzung einer Webseite ein Widerspruchsrecht nach § 15 Abs. 3 TMG bestehen, unabhängig davon, ob das Verfahren im Einzelnen als pseudonymisiertes Nutzungsprofil im Sinne dieser Vorschrift zu qualifizieren ist.
   - Bei der Entscheidung über Art und Weise der Verwendung von Cookies sollten die Anforderungen der überarbeiteten E-Privacy-Richtlinie nicht unbeachtet bleiben.
   - Die Verwendung personenbezogener Daten im Rahmen von Mechanismen zum Ausschluss missbräuchlicher Nutzung Sozialer Netzwerke sollte sich strikt an dem Grundsatz der Erforderlichkeit orientieren. Dies gilt insbesondere für die Bemessung von Speicherfristen.
   - Die Unterrichtungspflichten nach dem Telemediengesetz (§ 13 Abs. 1 TMG) sind umfassend zur Geltung zu bringen. Social Plugins und Fanpages sind so auszu-

gestalten, dass insbesondere Nichtnutzer Sozialer Netzwerke idealerweise vor dem Datenfluss über die Erhebung und Verwendung personenbezogener Daten informiert werden.

- Im Interesse der umfassenden Gewährleistung der informationellen Selbstbestimmung sollten die Betreiber Sozialer Netzwerke bei Social Plugins aktiv oder zumindest wohlwollend unterstützend an technischen Lösungen mitwirken, bei denen personenbezogene Daten der Nutzer erst an den Betreiber übertragen werden, wenn die entsprechende Schaltfläche durch den Nutzer nach einer Information über die dann fließenden Daten und deren Verwendung freigegeben wird. Mit einer solchen Funktion werden Einwilligungslösungen ermöglicht, die neben der praktischen Handhabbarkeit der Unterrichtungspflichten auch Anforderungen aus der E-Privacy-Richtlinie und an Statistikverfahren berücksichtigen können. Bei Fanpages sollten die Betreiber Sozialer Netzwerke adäquate Lösungen entwickeln.

4. Betreiber von Webseiten mit Social Plugins können durch die (durch ein IT-Informationsportal entwickelte) Zwei-Klick-Lösung das soeben dargelegte Maßnahmenkonzept auch ohne den Betreiber des Sozialen Netzwerks in gewissem Maße bereits jetzt grundsätzlich erfüllen und dadurch Gefährdungen für die informationelle Selbstbestimmung der Nutzer minimieren. Aufgrund des bestehenden Aufklärungsbedarfs tatsächlicher Art hinsichtlich der technischen Abläufe ist insbesondere die umfassende Information der Nutzer jedoch mit Unwägbarkeiten behaftet. Bei Fanpages könnten ergänzende Nutzerinformationen über die Datenverarbeitungsprozesse, die zunächst bei Aufruf der Fanpage eingeblendet werden, einen ersten Ansatz für eine Risikominimierung darstellen. Der sofortige Datenfluss beim bloßen Besuch der Fanpage kann hier jedoch ohne Mitwirkung von Facebook nicht unterbunden werden.
5. Die Debatte über den Einsatz von Social Plugins und Fanpages zeigt wiederum, dass insbesondere die Umsetzung folgender rechtspolitischer Forderungen dringend geboten ist:
   - völkerrechtliche Vereinbarungen zur datenschutzrechtlichen Verantwortlichkeit, die auch für nichtöffentliche Stellen, die ihren Sitz außerhalb der EU haben, verbindlich sind und deren Einhaltung von den deutschen Datenschutzaufsichtsbehörden wirksam überprüft werden können
   - Regelungen zur Verbesserung der Transparenz bei der Datenverarbeitung durch erweiterte Informations- und Auskunftspflichten der verantwortlichen Stellen

- Regelungen, die der Bildung von Persönlichkeitsprofilen (z. B. Konsumentenprofile, Bewegungsprofile, Nutzerprofile im Internet) möglichst enge Grenzen setzen
- Regelungen für soziale Netzwerke zum Schutz des Persönlichkeitsrechts der Nutzer (z. B. Verpflichtung der verantwortlichen Stelle zu datenschutzfreundlichen Voreinstellungen, zu besonderem Schutz für minderjährige Nutzer, Löschungsanspruch bei Ausscheiden aus dem Netzwerk)

Die Reform des Europäischen Datenschutzrechts und die parallel dazu auch in den Vereinigten Staaten von Amerika angelaufene Debatte über einen neuen Rechtsrahmen für den Datenschutz in der Informationsgesellschaft eröffnen die Chance, diese Forderungen in umfassend verbindlicher und zeitgemäßer Gewährleistung der informationellen Selbstbestimmung umzusetzen.