Tätigkeitsbericht 2017
des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

BERICHTSZEITRAUM: 2015/2016

REDAKTIONSSCHLUSS: 01.06.2017

LANDTAGSDRUCKSACHE 19/10

(36. TÄTIGKEITSBERICHT DER LANDESBEAUFTRAGTEN FÜR DATENSCHUTZ)

Marit Hansen

Landesbeauftragte für Datenschutz Schleswig-Holstein

Leiterin des Unabhängigen Landeszentrums
für Datenschutz Schleswig-Holstein, Kiel

Impressum

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Holstenstraße 98

24103 Kiel

Mail: mail@datenschutzzentrum.de

Web: https://www.datenschutzzentrum.de/

Satz und Lektorat: Gunna Westphal, Kiel

Umschlaggestaltung: Martin Papp, Eyekey Design, Kiel

Titelfoto: ULD unter Verwendung des Fotos "europafahne" von Lupo / pixelio.de

Druck: hansadruck, Kiel

Inhaltsverzeichnis

1	**Datenschutz und Informationsfreiheit**	**9**
1.1	Die Landesbeauftragte für Datenschutz – Wechsel in der Leitung des ULD	9
1.2	Gestaltung ist der Schlüssel!	10
1.3	Digitalisierung in Schleswig-Holstein	11
1.4	Wachsende Herausforderungen im Blick – die Dienststelle	13
2	**DATENSCHUTZ – GLOBAL UND NATIONAL**	**17**
2.1	Europäische Datenschutz-Grundverordnung – von Europa über Deutschland nach Schleswig-Holstein	17
2.2	EU-Richtlinie für den Datenschutz bei der Verfolgung und Verhütung von Straftaten	18
2.3	Informationssicherheit – von „I love you“ bis „WannaCry“	20
2.4	Datenschutz neu denken!	21
3	**LANDTAG**	**25**
3.1	Datenschutzgremium	25
3.2	Auditierung Zutrittsberechtigungssystem und Videoüberwachung des Landeshauses	25
4	**DATENSCHUTZ IN DER VERWALTUNG**	**27**
4.1	Allgemeine Verwaltung	27
4.1.1	Digitalisierung von Personalakten in der Landesverwaltung	27
4.1.2	Neufassung des Landesmeldegesetzes	28
4.1.3	Regeln für E-Government im Landesverwaltungsgesetz – mit Datenschutz	28
4.2	Polizei und Verfassungsschutz	30
4.2.1	Gefahrengebiete auch in Schleswig-Holstein	30
4.2.2	Prüfung der Falldatei Rauschgift	31
4.2.3	Prüfung der Datei „Fußball SH“	32
4.2.4	Polizeilicher Informations- und Analyseverbund im Betrieb	33
4.2.5	Rechen- und Dienstleistungszentrum zur Telekommunikationsüberwachung	34
4.2.6	Reichsbürger – Meldung von Behörden an die Polizei	35
4.3	Justiz	37
4.3.1	IT-Gesetz für die Landesjustiz – Regeln für ein Outsourcing	37
4.3.2	Verantwortung für die Datenverarbeitung klarstellen – zentrale Stelle in der Justiz	37
4.3.3	Kontrollmitteilungen an Finanzämter zu Geldauflagen bei Einstellung von Strafverfahren	38
4.3.4	Weitergabe von Familienfotos aus einer Durchsuchung an den Urheberrechtsverband GVU	39
4.3.5	Akteneinsichtsrecht für Europaratsausschuss zur Verhütung von Folter	40
4.3.6	Fehladressierung von E-Mails bei Polizei und Justiz	41
4.3.7	Mehr Transparenz bei Funkzellenabfragen	41
4.4	Ausländerverwaltung	43
4.4.1	Quartiersmanagement für Geflüchtete	43
4.4.2	Hinweise für ehrenamtliche Helferinnen und Helfer für Geflüchtete	44
4.5	Soziales	45
4.5.1	Die Dauerbrenner im Sozialleistungsbereich	45
4.5.2	Personaldaten der Jugendhilfe – das Online-Meldeportal des Landesjugendamts	46

4.6 Schutz des Patientengeheimnisses 47
4.6.1 Der neue Selbst-Check für Arztpraxen 47
4.6.2 Outsourcing in Kliniken und Arztpraxen – künftig auch ohne Einwilligung möglich 48
4.6.3 Speicherung von Patientendaten – bitte verschlüsseln! 49

4.7 Wissenschaft und Bildung 49
4.7.1 Planungen für eine einheitliche Schulverwaltungssoftware nehmen Fahrt auf 49
4.7.2 Die digitale Schule – aber bitte mit eingebautem Datenschutz 50
4.7.3 Aktuelle Messenger-Dienste – für die schulische Kommunikation tabu 51
4.7.4 Die digitale Fotowelt in der Schule wirft Fragen auf 52
4.7.5 Digitales Klassenbuch im Pilotversuch getestet 52
4.7.6 Risiken: Lehrer-Apps ersetzen den klassischen Lehrerkalender 53

4.8 Steuerverwaltung 53
4.8.1 Zusammenarbeit der Steuerverwaltungen der norddeutschen Länder 53
4.8.2 Immer Ärger mit der Zweitwohnungssteuer 54

5 DATENSCHUTZ IN DER WIRTSCHAFT 57
5.1 ULD prüft Datentransfer nach Safe-Harbor-Urteil 57
5.2 Mindestlohngesetz und Datenschutz 58
5.3 Keine juristischen Personen als betriebliche Datenschutzbeauftragte nach dem BDSG 58
5.4 Einwilligung per Unterschriften-Pad nicht wirksam 59

5.5 Einzelfälle aus der Praxis 60
5.5.1 Kundenkarten und Werbeeinwilligungen 60
5.5.2 Datenlecks in Online-Zugangssystemen 60
5.5.3 Personalausweiskopien – Identifizierungspflichten im Bankenbereich 61
5.5.4 Weitergabe der vollständigen IBAN an Zahlungsempfänger 62
5.5.5 Begehung von Mietwohnungen und Veröffentlichung von Fotos ohne Einwilligung 63
5.5.6 Briefkastenaufbrüche bei Sparkassen 63
5.5.7 Weitergabe von Beschäftigtendaten im Rahmen eines Personalabbaukonzepts 64
5.5.8 Umgang mit privaten Daten beim Ausscheiden aus dem Unternehmen 65

5.6 Videoüberwachung 65
5.6.1 Urlaubsland Schleswig-Holstein – Einsatz von Webcams 65
5.6.2 Wolfsmonitoring mit Wildkameras 66
5.6.3 Videoüberwachung im Fitnessstudio 67
5.6.4 Videoüberwachung in Schwimmbädern 67
5.6.5 Videoüberwachung auf Toiletten 68

6 SYSTEMDATENSCHUTZ 71
6.1 Zusammenarbeit für IT-Sicherheit und technischen Datenschutz 71

6.2 Länderübergreifende Zusammenarbeit der Datenschutzbeauftragten 72
6.2.1 Arbeitskreis Technik 72
6.2.2 Arbeitsgruppe der Datenschutzbeauftragten der Dataport-Trägerländer 72
6.2.3 Standardisierung von Datentransporten im E-Government (XTA) 73

6.3 Das Standard-Datenschutzmodell (SDM) 74
6.4 Datenschutz-Folgenabschätzung – ein neues Instrument aus der Grundverordnung 75

6.5 Ausgewählte Ergebnisse aus Vorabkontrollen und Prüfungen 76
6.5.1 Verfahrensdokumentation bei zentralen Verfahren am Beispiel von „KoPers kommunal“ 76
6.5.2 Vorabkontrolle beim BAföG-Verfahren 77
6.5.3 eBeihilfe – automatisierte Bearbeitung von Beihilfeanträgen 78
6.5.4 Personalbefragungen zum betrieblichen Gesundheitsmanagement 79

7 NEUE MEDIEN 83
7.1 EuGH-Verfahren zu Facebook-Seiten 83
7.2 Rundfunkbeitragsstaatsvertrag – Meldedatenabgleich und (zunächst) keine Adresskäufe 84
7.3 WhatsApp im Einsatz bei datenverarbeitenden Stellen 85
7.4 „Pokémon Go“ und was Ortsinformationen verraten 86
7.5 Länderübergreifende Untersuchung von Wearables 87
7.6 Medienkompetenz für Schülerinnen und Schüler 87

8 MODELLPROJEKTE UND STUDIEN 91
8.1 Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt 91
8.2 Identitätenmanagement und Selbstdatenschutz 92
8.2.1 Projekt FutureID – europaweite Nutzung von Identitätsnachweisen 93
8.2.2 Projekt AN.ON-Next – praktikable und rechtssichere Anonymität im Internet 94
8.2.3 Projekt AppPETs – Datenschutz eingebaut in Smartphone-Anwendungen 94
8.2.4 Projekt VVV – Verschlüsselung einfacher machen 95
8.2.5 Projekt PARADISE – Selbstdatenschutz für die Dopingkontrolle im Sport 96
8.3 Projekt SPLITCloud – mehr Kontrolle beim Cloud Computing 97
8.4 Cybersicherheit und Datenschutz 97
8.4.1 Projekt ITS.APT – Stärken des Bewusstseins für IT-Sicherheit 98
8.4.2 Projekt EIDI – korrekte und hilfreiche Benachrichtigung von Betroffenen nach einem Cybervorfall 99
8.4.3 Projekt CANVAS – Cybersicherheit zwischen Technik, Ethik und Recht 100
8.5 Big Data, soziale Netzwerke und Datenschutz 100
8.5.1 Projekt iTESA – Reisewarnungen auf Grundlage von sozialen Netzwerken 101
8.5.2 Projekt SPECIAL – Transparenz- und Einwilligungsmanagement für das semantische Netz 102
8.5.3 Projekt VALCRI – Big Data für die Polizei 103
8.6 Internet der Dinge 104
8.6.1 Projekte iKoPA und SeDaFa – Datenschutz für den vernetzten Verkehr 104
8.6.2 Projekt Privacy&Us – Usability für das Internet of Things 105

9 AUDIT UND GÜTESIEGEL 109
9.1 Zertifizierung wird europäisch 109
9.1.1 Auswirkungen der Datenschutz-Grundverordnung 109
9.1.2 AG Zertifizierung 110
9.2 Datenschutz-Gütesiegel 110
9.2.1 Abgeschlossene Gütesiegelverfahren 110
9.2.2 Sachverständige 112

9.3	Datenschutzaudits	113
9.3.1	Wie ein typisches Datenschutzaudit in der Verwaltung abläuft	113
9.3.2	Audit für den SafeMail-Dienst der Kassenärztlichen Vereinigung Schleswig-Holstein (KVSH)	114
9.4	Auditberatungen – IT-Grundschutz wird zunehmend nachgefragt	115
9.4.1	Grundschutz für die IT der Kernkraftfernüberwachung	115
9.4.2	Grundschutz in einem Forschungsinstitut	116
10	**AUS DEM IT-LABOR**	**119**
10.1	Webbrowser und Erweiterungen – Spionage durch die Hintertür	119
10.2	Webseitenverschlüsselung – HTTPS wird immer moderner	120
10.3	Windows 10 – Datenabfluss by Design	122
10.4	Metadaten und Schwärzungen in PDF-Dateien	123
10.5.	Home Smart Home	124
10.6	Absicherung von Online-Diensten mit Zwei-Faktor-Authentifizierung	125
10.7	Datenschutz unter dem Weihnachtsbaum – Tipps gegen Risiken bei Geschenken	126
11	**EUROPA UND INTERNATIONALES**	**129**
11.1	Safe-Harbor-Entscheidung des Gerichtshofs der Europäischen Union	129
11.2	Safe-Harbor-Nachfolger – Privacy Shield	130
11.3	Grenzüberschreitende Übung – Umgang mit Datenpannen	132
11.4	Kooperation im „Internet Privacy Engineering Network“	133
11.5	Privacy Engineering und Reifegrad datenschutzfördernder Technik	133
12	**INFORMATIONSFREIHEIT**	**137**
12.1	Ein Transparenzgesetz für Schleswig-Holstein	137
12.2	Informationsfreiheit im NDR-Staatsvertrag verankern	138
12.3	Zugang zu Unterlagen des Wissenschaftlichen Dienstes	138
12.4	Einsicht in Prüfberichte der Heimaufsichten	139
12.5	Anhörungsverfahren bei Informationen zu Emissionen	140
12.6	Kammersatzungen versus Informationsfreiheit?	140
12.7	Keine Pflicht zur Informationsbeschaffung und zur Beantwortung von Rechtsfragen	141
12.8	Ausschluss des Informationszugangs durch Spezialgesetze	142
12.9	Privates Handeln einer informationspflichtigen Stelle	142
12.10	Beanstandung wegen Nichtbeantwortung von Fragen	143
12.11	Leitfaden zur Anwendung des IZG in Bauordnungsbehörden	144
12.12	Anonyme Anfragen über das Internetportal „FragDenStaat“	144
13	**DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN**	**147**
13.1	Kurse im Programm der DATENSCHUTZAKADEMIE	147
13.2	Datenschutz-Sommerakademien	149
	Index	**150**

01

KERNPUNKTE

Gestaltung für Datenschutz und Informationsfreiheit
Digitalisierung in Schleswig-Holstein
Wachsende Herausforderungen

1 Datenschutz und Informationsfreiheit

1.1 Die Landesbeauftragte für Datenschutz – Wechsel in der Leitung des ULD

Mitte Juli 2015 wählte der Landtag die neue Landesbeauftragte für Datenschutz Schleswig-Holstein: Marit Hansen. Sie folgt Dr. Thilo Weichert nach, der seit 2004 das Amt innehatte.

„Die Neue“ ist gar nicht so neu: Marit Hansen arbeitet seit 1995 in der Dienststelle, die damals noch keine 15 Personen zählte und sehr viel weniger Aufgaben hatte. Der damalige Landesbeauftragte für den Datenschutz Schleswig-Holstein, Dr. Helmut Bäumler, stellte die Informatikerin für den Bereich Neue Medien ein – mit diesem Sammelbegriff bezeichnete man damals die Entwicklungen zu mehr Digitalisierung und Vernetzung. Viele Dienststellen hatten in dem Jahr noch keine E-Mail-Adressen oder gar einen Webauftritt – zugegeben ein Kulturschock für die Informatikerin Hansen, als sie damals ihren Dienst antrat. Aber es gab nichts, was sie nicht ändern konnte: Schon kurze Zeit später war die Dienststelle des Landesbeauftragten für den Datenschutz per E-Mail erreichbar – und zwar auch per verschlüsselter Kommunikation mit einem eigenen PGP-Schlüssel.

Während Bäumler – in Vorwegnahme dessen, was nun mit der europäischen Datenschutz-Grundverordnung (DSGVO) als Zertifizierung auf alle Datenschutzbehörden zukommt – dafür sorgte, dass neue Instrumente des Datenschutzes wie Gütesiegel und Audit in das im Jahr 2000 reformierte Landesdatenschutzgesetz aufgenommen wurden, war Hansen mit dem ULD-Team daran beteiligt, dies in die Praxis umzusetzen. Auch das Virtuelle Datenschutzbüro (https://www.datenschutz.de/) als gemeinsame Informationsplattform aller deutschen Datenschutzbehörden entstand unter ihrer Leitung.

Hansen betonte von Anfang an, dass Technik im Datenschutz mehr bedeutet, als „nur“ für eine verbesserte Informationssicherheit zu sorgen. Sie prägte seit Mitte der 90er-Jahre die Debatte um datenschutzfreundliche Technologien, Datenschutz durch Technik, Systemdatenschutz und Selbstdatenschutz mit. Weil eine kleine Datenschutz-Dienststelle allein in diesem komplexen und so wichtigen Thema nicht genug bewegen kann, baute Hansen Kooperationen mit in diesem Bereich aktiven Forscherinnen und Forschern auf. Dabei können alle Beteiligten voneinander lernen, wie sich unsere Grundrechte und Menschenrechte in der Welt der Informationstechnik umsetzen lassen.

Diese Kooperationen sind teilweise informell und anlassbezogen, teilweise wirkt das ULD auch mit dem von Hansen über viele Jahre geleiteten Projektbereich in Konsortien solcher Vorhaben mit, die sich Datenschutz besonders auf die Fahnen geschrieben haben. Im ULD wird dies unter der Bezeichnung „ULD-i – Innovationszentrum Datenschutz und Datensicherheit“ (Tz. 8) gebündelt. Dieses Engagement ist nur möglich mithilfe von Drittmitteln, die Fördergeber wie deutsche Bundesministerien oder die Europäische Kommission in den jeweiligen Forschungsprogrammen für diese Zwecke zur Verfügung stellen. Das ULD wird vielfach nachfragt, um sich an neuen Ideen der Datenschutzforschung zu beteiligen.

Die europäische Datenschutz-Grundverordnung (Tz. 2.1) verlangt von den Datenschutzaufsichtsbehörden u. a., dass sie „maßgebliche Entwicklungen verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken“. Auch in der Beratung, welche Maßnahmen im Bereich der datenschutzfördernden Technikgestaltung und zur Eindämmung von Risiken für Rechte und Freiheiten natürlicher Personen getroffen werden müssen oder sollten, ist dieses Wissen wesentlich. Für die Erfüllung dieser Aufgaben leisten die Beteiligung an Forschungsprojekten und die Kooperation mit zahlreichen Expertinnen und Experten einen wichtigen Beitrag.

Nach der Wahl zur Landesbeauftragten für Datenschutz gab Hansen diesen Bereich in andere Hände im ULD. Als Dienststellenleiterin mit zahlreichen weiteren Aufgaben kann sie sich nur noch manchmal persönlich bei den Forschungsprojekten beteiligen. Die ULD-Aktivität läuft selbstverständlich weiter. Die Erkenntnisse aus der Forschung sind bedeutsam, um Gesetzgeber, Entwickler und Anwender auch über neue Lösungsmöglichkeiten kompetent beraten zu können.

Insgesamt steht Hansen aus Überzeugung für Kontinuität der Arbeit, die ihre Vorgänger Bäumler und Weichert geleistet haben und für die sie den beiden dankbar ist. Natürlich unterscheidet sich ihr Blickwinkel als Informatikerin von dem ihrer Vorgänger, aber damals wie heute kommt es auf das gesamte Team an, das im ULD interdisziplinär – Jura, Informatik, Verwaltungs-, Wirtschafts- und Geisteswissenschaften – aufgestellt ist und bei dem die verschiedenen Mitarbeiterinnen und Mitarbeiter mit ihrem jeweiligen fachlichen Hintergrund eng zusammenwirken.

Zu den wichtigsten Pflichtaufgaben einer Datenschutzaufsichtsbehörde gehören die Prüfung und die Beratung von öffentlichen und nichtöffentlichen Stellen: Wo es falsch läuft, drohen Sanktionen; wer es richtig machen möchte, kann Hilfe bekommen und sich beraten lassen. Jeder Beschwerde wird nachgegangen. Bürgerinnen und Bürger, Verbraucherinnen und Verbraucher erhalten Unterstützung – hier ist die Datenschutzbehörde Service-Stelle. Dasselbe gilt für Abgeordnete und für die Gesetzgeber, die das ULD in ihre Arbeit einbeziehen und dadurch die Perspektive zu Datenschutz und Informationsfreiheit von Anfang an berücksichtigen können.

Jede Beauftragte und jeder Beauftragter für Datenschutz und für Informationsfreiheit legt darüber hinaus eigene Schwerpunkte – so kann man sich im Föderalismus erfolgreich ergänzen. Bei Hansen ist es daher auch nicht nur ein „Weiter so“, sondern sie setzt ihre Impulse im Land Schleswig-Holstein und – wo es sinnvoll ist – über das Land hinaus: zum einen im Bereich der Systemgestaltung (Tz. 1.2), zum anderen im Bereich der Praxis, um Datenschutz und Informationsfreiheit, die manchen Personen und den kleinen Verwaltungen und Unternehmen als überkomplex erscheinen, handhabbar zu machen.

In Hansens erster Amtszeit wird das ULD ebenso wie alle anderen Datenschutzbeauftragten des Bundes und der Länder vieles neu gestalten – schon aufgrund der Datenschutzreform auf EU-Ebene. Dazu gehören organisatorische Prozeduren, juristische Festlegungen und technische Unterstützungen, die im Orchester aller Datenschutzbeauftragten in Europa optimal aufeinander abgestimmt werden sollen. Der europäische Rechtsrahmen verspricht ein einheitliches Datenschutzniveau. Damit dies Realität wird, müssen zahlreiche Punkte ins Bewusstsein gerückt und unter den Mitgliedstaaten mit ihren Unterschieden in Kultur und nationalem Rechtsgefüge verhandelt werden. Hier gilt es, in allen wichtigen Bereichen mit guten Argumenten zu überzeugen. Das ULD mischt sich ein und trägt auch auf europäischer Ebene zum konstruktiven Diskurs bei.

Für Sie wichtig

Marit Hansen steht als Landesbeauftragte für Datenschutz Schleswig-Holstein mit ihrem Team für Ihre Fragen in Sachen Datenschutz und Informationsfreiheit zur Verfügung.

1.2 Gestaltung ist der Schlüssel!

Jede und jeder von uns ist Teil unserer Gesellschaft. Dabei haben wir nicht nur den Beobachterstatus, der uns dazu verdammen würde, die Entwicklungen, die andere voranbringen, hinzunehmen. Sondern wir können unsere Gesellschaft aktiv gestalten.

Dies betrifft bei der Informationsgesellschaft nicht nur die Technik: Geräte, die wir haben, Anwendungen, die wir nutzen, Infrastrukturen, auf die wir uns verlassen. Nicht nur Organisatorisches: die Abläufe und Prozesse, die bei staatlichen oder wirtschaftlichen Akteuren defi-

nieren, in welchen Schritten vorgegangen wird – mit mehr oder weniger Bürokratie. Sondern die Gestaltungsmöglichkeiten umfassen auch das Recht: Was soll rechtlich festgelegt sein? Und vor allem: Wie soll es geregelt werden? Wie werden Verstöße sanktioniert? Eine wesentliche Rolle spielt zudem die Kultur im Umgang miteinander, z. B. die zwischenmenschlichen Spielregeln. Und wichtig sind auch die Anreizsysteme: die Förderungen, die Belohnungen, die Motivation aller zur Gestaltung einer lebenswerten Gegenwart und Zukunft.

All diese Facetten mitzudenken bedeutet umfassende Systemgestaltung. Das Fundament dafür sind unsere Werte, die sich in den Menschenrechten manifestieren, um die über Jahrhunderte gerungen wurde. Diese Menschenrechte müssen auch in der Informationsgesellschaft die Basis für das Handeln und für die Weiterentwicklung bleiben. Digitalisierung kann jedoch Machtasymmetrien begünstigen und eröffnet damit Möglichkeiten für unfaires Verhalten und Willkür. Die Konzentration von personenbezogenen Informationen in der Hand der Staaten – dazu gehören auch die geheimdienstlichen Datensammlungen – und einer kleinen Zahl von den Markt dominierenden Unternehmen im Internet stellt ein massives Risikopotenzial dar. Die Abhängigkeit der Informationsgesellschaft von einer komplexen Technik, die heute wahrscheinlich keiner in all ihren Auswirkungen vollständig versteht oder auch nur nachvollziehen könnte, bedeutet einen Kontrollverlust für die Gesellschaft. Es ist ein ungeheuerliches Wagnis, auf einem solchen Fundament von verletzlicher Informationstechnik und faktischer Informationskonzentration die Zukunft aufzubauen.

Datenschutz im Sinne der Persönlichkeitsrechte der Betroffenen und Informationsfreiheit für mehr Transparenz des Verwaltungshandelns sind wichtige Elemente, um die Entwicklung so umzulenken, dass die Menschenrechte wieder in den Fokus kommen und effektiv verwirklicht werden. Die Beauftragten für Datenschutz und für Informationsfreiheit wollen Garanten für diese Schutzgüter sein und gehen den Beschwerden nach. Oft ist diese Arbeit allerdings vergleichbar mit dem Herumdoktern an Symptomen, während die Ursachen ungelöst bleiben und in der weiteren Entwicklung sich die Probleme für die Menschenrechte sogar verschärfen können.

Dies ist aber nicht alternativlos. Der Lösungsraum lässt sich erweitern, insbesondere durch die Arbeit an der Schnittstelle zwischen Wissenschaft und Praxis, durch das Erforschen der juristischen, technischen und organisatorischen Möglichkeiten für die Implementierung der Menschenrechte, durch das Verstehen von gesellschaftlichen und wirtschaftlichen Implikationen vor Ort und im globalen Kontext. Ohne diese Perspektive würden der Politik, den Entscheidungsträgern und uns allen relevante Optionen fehlen, die wir als Gesellschaft für eine Systemgestaltung entlang der Leitlinien unserer Werte benötigen.

Der Brückenschlag zwischen Wissenschaft und Praxis ist dringend nötig, da die verschiedenen Communities zu wenige Berührungspunkte aufweisen und verschiedene Sprachen sprechen. Bei Datenschutz und Informationsfreiheit ist die Lücke zwischen Forschungsergebnissen und der Realität besonders groß. Viele innovative Konzepte warten darauf, mit Leben gefüllt zu werden – und zumindest für den Bereich Datenschutz bietet die Grundverordnung mit dem Artikel 25 nun endlich eine rechtliche Grundlage für eine verbesserte Systemgestaltung und eingebauten Datenschutz.

Was ist zu tun?

Die Aufgabe für alle Disziplinen lautet: Gesucht sind clevere Lösungen, um die Menschenrechte in der Informationsgesellschaft zu bewahren und auch künftig zu gewährleisten.

1.3 Digitalisierung in Schleswig-Holstein

Die Digitalisierung schreitet voran: In jedem Bereich unseres Lebens spielen Computer eine Rolle. Informationstechnik erhält Einzug in Alltagsgeräte, die vorher ohne Chip und Datenverarbeitung ausgekommen sind. Unsere Autos, Häuser und Städte werden „smart“. Das Arbeitsleben wandelt sich durch Plattform-Ökonomie oder Industrie 4.0. Datenmassen können

auf versteckte Zusammenhänge hin durchforstet werden. Algorithmen nehmen uns Entscheidungen ab.

Digitalisierung hat mehrere Bedeutungen:

Zum einen bezeichnet Digitalisierung das Überführen von Informationen, die nicht digital zur Verfügung stehen, in ein digitales Format, das sich direkt mithilfe von Informationstechnik verarbeiten lässt. Dies geschieht beispielsweise bei der Umwandlung von papierenen Akten zur e-Akte.

Zum anderen geht es bei der Debatte um Digitalisierung um die Folgen durch die Verwendung von Informationstechnik in immer mehr Lebensbereichen und um geeignete Rahmenbedingungen, die negative Auswirkungen und Risiken minimieren sollen.

Dies alles betrifft auch Schleswig-Holstein. Wir sehen die Chancen für unsere Gesellschaft, die Digitalisierung mit sich bringt. Jedoch sind Risiken mit der Digitalisierung verbunden: Immer mehr Daten geben detaillierte Auskunft über die Menschen. Technik wird eingesetzt, um das Verhalten von Menschen vorherzusagen oder zu steuern. Wie passt dies noch zusammen mit der informationellen Selbstbestimmung – der Basis für den Datenschutz in Deutschland –, dass jeder wissen können muss, wer was über ihn weiß? Hier gilt es, die digitalisierte Welt und die Rahmenbedingungen der Digitalisierung mitzugestalten und auf solche Lösungen hinzuwirken, bei denen die Risiken eingedämmt und insbesondere die Grundrechte und Menschenrechte gestärkt werden.

Das ULD bringt sich daher in regionalen, nationalen und europäischen Diskussionen zur Digitalisierung ein, an denen Verwaltung, Wirtschaft, Zivilgesellschaft, Gesetzgeber und Aufsichtsbehörden beteiligt sind. Das ULD ist nicht nur als Aufsichtsbehörde mit den Themen befasst, sondern wird auch für Beratungen, Schulungen, Vorträge und Forschungsprojekte im Bereich der Digitalisierung und des digitalen Grundrechtsschutzes angefragt. Seit vielen Jahren wirkt das ULD an Vorhaben zur Einführung neuer IT-Verfahren im Land und bei Kommunen intensiv mit. Dies ermöglicht eine Gestaltung, in der die Anforderungen von Datenschutz und Informationsfreiheit frühzeitig durch rechtliche, technische und organisatorische Maßnahmen umgesetzt werden. Im Berichtszeitraum hat das ULD den Entstehungsprozess der Digitalen Agenda begleitet und in der Zuständigkeit für Datenschutz und Informationsfreiheit Stellung genommen.

Aus unserer Sicht müssen Datenschutz und Informationsfreiheit in einer Digitalen Agenda eine übergeordnete Rolle spielen. Würde man diese Kernthemen vergessen, liefe man Gefahr, Verfahren, Anwendungen und Infrastrukturen zu entwickeln, die die rechtlichen Anforderungen nicht ausreichend berücksichtigen. Grundlegende Weichenstellungen in einem frühen Stadium können darüber entscheiden, ob empfehlenswerte und solide Lösungen mit eingebautem Grundrechtsschutz entstehen.

Was kann das Land Schleswig-Holstein dazu beitragen? Natürlich sollte das Land Vorbild sein bei der Gestaltung und Beschaffung der eigenen Informationstechnik. Auch sollte der Landesgesetzgeber im Rahmen der jeweiligen Gesetzgebung Anforderungen des Datenschutzes „by Design“ und „by Default“ (wie in Artikel 25 der Datenschutz-Grundverordnung formuliert) ebenso wie der Informationsfreiheit und der Transparenz umsetzen, wo dies möglich ist. Weiterhin gehören diese Themen in die Förder- und Beratungspolitik des Landes, damit Implementierungen und die Entwicklung neuer Geschäftsmodelle nicht nur rechtlich abgesichert werden, sondern Forscher, Start-Ups und etablierte Unternehmen dabei auch neue Impulse für ein zukunftsfähiges Design setzen können. Das ULD will im Rahmen seiner Möglichkeiten daran unterstützend mitwirken.

Wichtig ist, dass keiner den leider oft wiederholten, aber damit nicht richtigen generalisierenden Aussagen glaubt, es sei für das Angebot integrierter und interaktiver Dienstleistungen für Bürgerinnen und Bürger notwendig, „mehr aus den bereits verfügbaren Daten zu schöpfen“. Verwaltungsdaten sind mit gutem Grund zweckgebunden – Bürgerinnen und Bürger dürfen nicht gläsern werden, was leicht passieren kann, wenn die Daten, die bei verschiedenen Behörden für ihre jeweiligen Aufgaben vorhanden sind, zusammengeführt werden. Eine zweckübergreifende Nutzung à la naivem Big Data steht im Widerspruch zu Datenschutzgrundsätzen der Erforderlichkeit, der Zweckbindung und der Transparenz und ist in der Regel unzulässig.

Es gibt aber sehr wohl rechtskonforme Ausprägungen des mittlerweile in der Landesregierung diskutierten „Data Driven Government“, damit Entscheidungen auf Basis von Daten und Analysen getroffen werden. Für diesen Zweck sei ein Blick in Konzepte des technischen Daten-

schutzes angeraten: Es ist nämlich möglich, die notwendigen Informationen zu erhalten, ohne dass sich Daten über individuelle Bürgerinnen und Bürger verknüpfen lassen. Bei vorhandenen Datenbeständen können hier Techniken zur Anonymisierung und Aggregation zum Einsatz kommen. Noch besser wäre es, bereits bei der Erhebung der personenbezogenen Daten dafür zu sorgen, dass bestimmte Verknüpfungen und damit zusammenhängende Datenschutzrisiken technisch unterbunden werden, aber gleichzeitig die gewünschte Datenverarbeitung im Fachbereich erfolgen kann (beispielsweise durch Konzepte wie „attributbasierte Berechtigungszertifikate“ (35. TB, Tz. 8.2.1). Weiterhin könnten technisch durchsetzbare Regeln zur erlaubten Verarbeitung der Daten an die Datensätze selbst gebunden werden. So kann grundrechtskonforme Systemgestaltung funktionieren.

Digitalisierung im Land bedeutet auch mehr Transparenz des Verwaltungshandelns durch eine Open-Data-Strategie, bei der die Rechte und schutzwürdige Interessen der betroffenen Personen und Parteien gewahrt bleiben. Dies bedeutet, dass bei Anlage und Bearbeitung der elektronischen Akten die notwendigen Schritte zur proaktiven Veröffentlichung aller veröffentlichungsfähigen (Teil-)Akten vorgenommen werden und gleichzeitig möglicherweise enthaltene sensible Teile geschützt bleiben. Dies lässt sich beispielsweise durch Trennung von Aktenteilen verschiedenen Schutzbedarfs oder durch Anonymisierungs- oder Schwärzungsfunktionalität erreichen.

Sowohl für die Open-Data-Strategie als auch für „Data Driven Government“ ist der gesamte Lebenszyklus der Daten zu berücksichtigen, um zu guten und grundrechtskonformen Lösungen zu gelangen. Wichtige Impulse für eine faire Digitalisierung setzen dabei die Instrumente Audit und Gütesiegel, Datenschutz-Folgenabschätzung sowie das Standard-Datenschutzmodell (Tz. 6.3), das die Umsetzung der rechtlichen Anforderungen aus Land, Bund und Europa in die Praxis erleichtert. Das ULD steht gerne beratend zur Verfügung.

Was ist zu tun?

Das Land Schleswig-Holstein sollte in seiner eigenen gesetzgeberischen Kompetenz die Anforderungen an eine grundrechtskonforme Gestaltung der digitalisierten Welt umsetzen. Weiterhin sollte das Land seinen Einfluss im Bundesrat auf die Bundesgesetzgebung in diesem Sinne nutzen. Gute Ideen, Konzepte und Lösungen aus dem Land sollten gefördert werden, damit sie über die Grenzen hinweg ausstrahlen können.

1.4 Wachsende Herausforderungen im Blick – die Dienststelle

Die Dienststelle vergrößert sich: Der Schleswig-Holsteinische Landtag hat dem ULD ermöglicht, fünf zusätzliche Personen einzustellen. Damit stehen dem ULD insgesamt 32 Stellen zur Verfügung. Zwei der neuen Stellen sind befristet bis Ende 2019. Grund für den dringend notwendigen Zuwachs ist einerseits das gestiegene Bewusstsein für Datenschutz und Informationsfreiheit, andererseits die Erweiterung des Aufgabenspektrums, das von der Dienststelle zu erfüllen ist.

In den letzten Jahren haben immer mehr öffentliche und nichtöffentliche Stellen verstanden, dass das ULD ihnen dabei behilflich sein kann, die rechtlichen Anforderungen von Datenschutz und Informationsfreiheit zu erfüllen. Die Beratungsanfragen aus Verwaltung, Wirtschaft und Politik haben daher zugenommen. Gleichzeitig merken wir, dass immer mehr Personen das ULD kennen und ihre Beschwerden vorbringen, denen wir dann nachgehen, oder Tipps wünschen, wie sie selbst ihre Rechte besser wahrnehmen können. Dies liegt auch daran, dass die Verarbeitung von Daten immer mehr Bestandteil des Alltagslebens wird. Viele Beschwerden beziehen sich auf Datenverarbeitungen durch Privatpersonen, z. B. auf Videoüberwachungen von Privatgrundstücken aus oder auf Veröffentlichungen im Internet. Wegen dieses hohen Zeitanteils für Beratung und Beschwerden konnten in der Vergangenheit kaum noch anlasslose Prüfungen durchgeführt werden. Proaktives Handeln war mit der

zur Verfügung stehenden Personalausstattung stark eingeschränkt.

Prüfungen sind aber dringend notwendig – auch dann, wenn es (noch) keine Beschwerde über die Datenverarbeitung gibt. Für den Bereich der Polizei und des Verfassungsschutzes wurde den Datenschutzbehörden angesichts der Intransparenz von Datensammlungen vom Bundesverfassungsgericht aufgegeben, Prüfungen durchzuführen. So schreiben das Antiterrordatei- und das Rechtsextremismusdateigesetz Prüfungen durch die Datenschutzbeauftragten im Abstand von höchstens zwei Jahren vor. Nun können wir diesen sehr kleinen Bereich – unser Referat für Polizei und Justiz – mit einer Sachbearbeiterin verstärken.

Die große Unbekannte für das Mehr an Arbeitslast ist aber die europäische Datenschutzreform, die über verschiedene Gesetzeswerke neue Aufgaben definiert: Die Datenschutz-Grundverordnung (Tz. 2.1), die ab dem 25. Mai 2018 gilt, enthält für das ULD als Datenschutzaufsichtsbehörde gleich 22 Aufgaben (Artikel 57 Abs. 1 Buchst. a bis v DSGVO), wobei der letzte Eintrag mit der Formulierung „jede sonstige Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten“ sicherstellt, dass keine Aufgabe vergessen wurde. Für den Telekommunikations- und Telemedienbereich ist auf EU-Ebene zurzeit die E-Privacy-Verordnung in Arbeit, die ebenfalls ab Mai 2018 gelten soll. Die Datenschutz-Richtlinie für Justiz und Inneres (Tz. 2.2) gilt zwar im Gegensatz zu den EU-Verordnungen nicht unmittelbar, aber umfasst ebenfalls neue Instrumente, zu denen das ULD beraten wird.

Neue Herausforderungen ergeben sich daraus, dass durch die EU-Verordnungen ein stärkerer europaweiter Gleichklang gefordert ist: Die Datenschutzbeauftragten auf nationaler und europäischer Ebene werden zu einer Koordinierung ihres Vorgehens verpflichtet. Bei grenzüberschreitenden Fällen geschieht diese Koordinierung über das Kohärenzverfahren und den für diese Zwecke eingerichteten Ausschuss. Es zeigt sich, dass bei allen Abstimmungen, die die EU-Ebene betreffen, die mündliche und schriftliche Kommunikation häufig zweisprachig, d. h. sowohl in der Amtssprache als auch auf Englisch, erfolgen muss.

Was bedeutet dies für eine ausreichende Ausstattung der Datenschutzaufsichtsbehörde mit den „personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen […], die sie benötigt, um ihre Aufgaben und Befugnisse auch im Rahmen der Amtshilfe, Zusammenarbeit und Mitwirkung im Ausschuss effektiv wahrnehmen zu können“, wie dies Artikel 52 Abs. 4 DSGVO fordert? Diese Frage wurde in zwei Gutachten bearbeitet, die beide trotz aller Unsicherheit über die zukünftige Entwicklung zum Schluss kommen, dass eine personelle Verstärkung der Datenschutzaufsicht notwendig sein wird.

Der ehemalige Bundesbeauftragte für den Datenschutz und ehemaliger Landesinnenminister Prof. Dr. Hans Peter Bull hat sein 74-seitiges Gutachten im Auftrag der Präsidentin des Landtages Brandenburg verfasst und bereits im August 2016 finalisiert. Dabei hat Prof. Bull speziell den Bedarf für die Dienststelle der Landesbeauftragten für den Datenschutz und das Recht auf Akteneinsicht aus diesem Bundesland in Bezug auf die neuen Aufgaben ermittelt und Aufstockungsbedarf herausgearbeitet. Allerdings lässt er offen, wie der tatsächliche Bedarf ab Mai 2018 aussehen wird. Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg, Dagmar Hartge, hat zudem ihre Kritik an dem Gutachten gegenüber ihrem Landtag kommuniziert.

Im Auftrag der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat der Rechtswissenschaftler Prof. Dr. Alexander Roßnagel sein Gutachten zum zusätzlichen Arbeitsaufwand für die Aufsichtsbehörden der Länder erarbeitet und im Januar 2017 vorgestellt. Auf 167 Seiten beschreibt er, welcher mutmaßliche Aufwand mit den zusätzlichen Aufgaben verbunden sein wird. Dabei unterscheidet Prof. Roßnagel zwischen den Aufgaben für Aufsicht, Kooperation, Kommunikation, Verfahrensmanagement und Justiziariat, die von Jurist(inn)en, Informatiker(inne)n, Öffentlichkeitsexpert(inn)en, Sachbearbeiter(inne)n sowie einem Sekretariat erfüllt werden sollen. Im Ergebnis kommt er auf einen Bedarf von mehr als 20 Stellen pro Datenschutzbehörde, die für die Erfüllung der hinzukommenden Aufgaben notwendig sein werden. Dieses Gutachten ist auf der Webseite des ULD verfügbar:

https://datenschutzzentrum.de/artikel/1136-1.html

Was ist zu tun?

Die Ausstattung aller Datenschutzbehörden muss mit den Aufgaben wachsen. Nur so kann rechtssicher vorgegangen werden, und nur so lassen sich die Ziele der europäischen Datenschutzreform erreichen.

02

KERNPUNKTE

Europäische Datenschutzreform
Fundament der Informationsgesellschaft
Datenschutz neu denken

2 Datenschutz – global und national

2.1 Europäische Datenschutz-Grundverordnung – von Europa über Deutschland nach Schleswig-Holstein

Alles neu macht der Mai, und zwar der 25. Mai 2018, denn ab diesem Datum gilt die europäische Datenschutz-Grundverordnung. Die Grundverordnung ist das Schwergewicht des EU-Datenschutzreformpakets, das den Datenschutz modernisieren und – nun ernsthaft – zwischen den Mitgliedstaaten der Europäischen Union harmonisieren soll. Hinzu kommt die E-Privacy-Verordnung, die bisher nur im Entwurfsstadium existiert, und die Datenschutz-Richtlinie für Justiz und Inneres (Tz. 2.2).

Jahrelang wurden über die Datenschutz-Grundverordnung zähe Verhandlungen geführt, um einen angemessenen und einheitlichen Schutz für die 500 Millionen Bürgerinnen und Bürger der EU zu erreichen. Die nun entstandenen 99 Artikel der DSGVO enthalten Neues und Bekanntes. Erreicht wurde mit der Anschlussfähigkeit an Bekanntes, dass der Aufwand zum Einhalten der DSGVO für diejenigen verantwortlichen Stellen, die schon immer Datenschutz ernst genommen und die Anforderungen der Datenschutz-Richtlinie von 1995 (95/46/EG) umgesetzt haben, nicht hoch ist. Die neuen Instrumente zur Risikoeindämmung und für einen verbesserten Datenschutz bergen einiges an Potenzial: Datenschutz-Folgenabschätzung (Artikel 35 DSGVO), Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Artikel 25 DSGVO), verbesserte Transparenzregelungen (Artikel 12 bis 15 DSGVO), Zertifizierung (Artikel 42 und 43 DSGVO; jetzt nicht mehr nur in Landesgesetzen wie im Landesdatenschutzgesetz Schleswig-Holstein). Das Erfüllen der Rechenschaftspflicht (Artikel 24 DSGVO) lässt sich mit einem Datenschutzmanagementsystem unterstützen.

Für einige Mitgliedstaaten sind betriebliche und behördliche Datenschutzbeauftragte ebenfalls ein neues Instrument. Neu ist daran für Schleswig-Holstein, dass behördliche Datenschutzbeauftragte nunmehr verpflichtend zu bestellen sind, was in der überwiegenden Zahl der Bundesländer ohnehin schon der Fall ist.

Neu ist die Betonung des Marktortprinzips der Datenschutz-Grundverordnung (Artikel 3 Abs. 2 DSGVO). Das Marktortprinzip besagt, dass auch dann, wenn ein Verantwortlicher oder Auftragsverarbeiter keine Niederlassung in der EU hat, die DSGVO für die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, anwendbar ist, wenn die Datenverarbeitung im Zusammenhang damit steht, den Personen in der Union Waren oder Dienstleistungen anzubieten oder ihr Verhalten zu beobachten. Das bedeutet: Wer im räumlichen Bereich der Europäischen Union Geschäfte macht und dabei personenbezogene Daten verarbeitet oder Daten über das Verhalten von Personen sammelt, unterliegt der DSGVO.

Das heutzutage eher stumpfe Schwert der Sanktionen mit Bußgeldern wird schärfer – bei dem Verstoß gegen einige der Bestimmungen mit einer Maximalstrafe von bis zu 4 % des Vorjahresumsatzes eines Unternehmens oder 20 Mio. Euro bzw. bei anderen Bestimmungen immer noch 2 % des Vorjahresumsatzes oder 10 Mio. Euro (Artikel 83 DSGVO). Seitdem diese Regelungen bekannt sind, scheinen erstmals einige Unternehmen das Datenschutzrecht ernst zu nehmen.

Dem Gesetzeswerk sieht man an, dass es das Ergebnis mühsamer Verhandlungen über einen längeren Zeitraum ist. Öffnungsklauseln ermöglichen es den Mitgliedstaaten, Anpassungen an ihre nationalen Vorstellungen zu schaffen, beispielsweise im Beschäftigtendatenschutz. Nicht nur gesetzliche Konkretisierungen werden angesichts der überwiegend recht abstrakten Regelungen in der DSGVO notwendig sein. Diese Abstraktheit ist so gewollt, um nicht nur für wenige Jahre, sondern für mehrere Jahrzehnte anpassungsfähig zu sein. Dem Flickenteppich soll der Europäische Datenschutzausschuss entgegenwirken, besetzt mit den Aufsichtsbehörden der Mitgliedstaaten, um eine einheitliche Anwendung des Datenschutzrechts zu gewährleisten. Außerdem ist schon absehbar, dass voraussichtlich für die notwendige Rechtssicherheit in Zweifelsfragen gerichtliche Klärungen bis zum Gerichtshof der Europäischen Union notwendig werden.

Es liegt wohl in der Natur der Sache, dass die DSGVO als Kompromiss zwischen den verhandelnden Akteuren nicht alle Wünsche einer Landesbeauftragten für Datenschutz festge-

schrieben hat. Dasselbe gilt für die nationale Umsetzung durch das Datenschutz-Anpassungs- und Umsetzungsgesetz – EU (DSAnpUG-EU), mit dem u. a. das Bundesdatenschutzgesetz reformiert wird. Kritikpunkte haben wir gemeinsam mit allen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder geäußert, großenteils leider vergebens. Nun gilt es, das Beste daraus zu machen. Es bleibt abzuwarten, ob die Umsetzung der DSGVO und der Datenschutz-Richtlinie für Justiz und Inneres ins nationale Recht rechtskonform gelungen ist und handhabbar sein wird.

In jedem Fall ist aber nun Eile für den Landesgesetzgeber geboten, der erst nach der Landtagswahl mit nunmehr weniger als einem Jahr Vorlauf nicht nur ein neues Landesdatenschutzgesetz zimmern soll, sondern eine Menge an bereichsspezifischem Recht auf die Kompatibilität mit der DSGVO abklopfen und anpassen soll. Im Zweifelsfall geht die DSGVO für ihren Anwendungsbereich vor.

Was ist zu tun?

Die Zeit bis zum Mai 2018 muss sowohl von Unternehmen als auch von der Verwaltung genutzt werden, um sich rechtskonform im Datenschutz aufzustellen. Der Landesgesetzgeber muss dafür sorgen, dass die Landesgesetze konform zur DSGVO gestaltet werden. Das ULD steht gerne beratend zur Seite.

2.2 EU-Richtlinie für den Datenschutz bei der Verfolgung und Verhütung von Straftaten

Im Paket mit der Datenschutz-Grundverordnung hat die EU im Jahr 2016 auch die Richtlinie 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI (JI-Richtlinie) verabschiedet. Sie muss bis zum 6. Mai 2018 in nationales Recht umgesetzt werden.

Vor große Schwierigkeiten stellt das EU-Reformpaket den Gesetzgeber bei der exakten Abgrenzung der Anwendungsbereiche der Datenschutz-Grundverordnung und der JI-Richtlinie. Die JI-Richtlinie nimmt ausdrücklich Bezug auf Straftaten, sodass sie für Gefahrenabwehrmaßnahmen der Polizei, die keinen Bezug zu einer Straftat haben, nicht gilt. Umstritten ist, ob die JI-Richtlinie nur für die Polizei gilt oder auch für die Gefahrenabwehr durch Ordnungsbehörden. Nach Auffassung des ULD gilt die JI-Richtlinie ausschließlich für die Polizei. Ordnungsbehörden fallen dagegen in den Anwendungsbereich der Datenschutz-Grundverordnung. Umstritten ist ebenfalls, ob zu den Straftaten im Sinne der JI-Richtlinie auch Ordnungswidrigkeiten gehören. Die europarechtliche Definition des Begriffs der Straftat ist in diesem Punkt nicht eindeutig. Da nach nationalem Recht die Verfolgung von Ordnungswidrigkeiten weitgehend der Verfolgung von Straftaten nachgebildet ist, befürwortet das ULD im Interesse der Einheitlichkeit des Rechts die Anwendung der JI-Richtlinie auch für die Verfolgung von Ordnungswidrigkeiten.

Für die Bereiche, die der Datenschutz-Grundverordnung unterfallen, gilt diese ab Mai 2018 als unmittelbar anwendbares Recht. Landesrecht kommt nur noch in einigen Punkten zur Anwendung, wo die Regelungen der Datenschutz-Grundverordnung durch nationales Recht konkretisiert werden dürfen. Die JI-Richtlinie muss hingegen vollständig in Landesrecht umgesetzt werden, denn EU-Richtlinien sind nicht unmittelbar anwendbar. Für diesen Bereich müssen landesrechtliche Regelungen erlassen werden. Schließlich gibt es noch einen dritten Bereich, der vom EU-Recht überhaupt nicht berührt wird, weil die EU in diesem Bereich keine Kompetenzen hat. Hierzu gehört in jedem Fall der Verfassungsschutz.

Für die der JI-Richtlinie unterfallenden Datenverarbeitungen und für diejenigen Behörden, für die die EU keine Regelungskompetenz hat, müssen daher vollständige Regelungen über

den Datenschutz getroffen werden. Bisher war das Landesdatenschutzgesetz Schleswig-Holstein für diese Bereiche Auffanggesetz für allgemeine Fragen wie technische und organisatorische Maßnahmen, behördliche Datenschutzbeauftragte, Verfahrensverzeichnis, Vorabkontrollen und gemeinsame Verfahren mit zentraler Stelle, Datenverarbeitung im Auftrag, Videoüberwachung zum Schutz des Hausrechts, Mitteilungen über Datenpannen, Bußgeldvorschriften und schließlich die Einrichtung und die Befugnisse des ULD. Das bestehende LDSG wird ab Mai 2018 durch die Datenschutz-Grundverordnung abgelöst. Eine parallele nationale Regelung ist neben einer EU-Verordnung nicht zulässig, sodass insoweit das Landesdatenschutzgesetz aufgehoben werden muss. Damit würde es jedoch auch als Auffangregelung für die der JI-Richtlinie unterfallenden oder die vom EU-Recht nicht erfassten Behörden wegfallen.

Der Bundesgesetzgeber hat dieses Problem dadurch gelöst, dass er im allgemein geltenden Bundesdatenschutzgesetz vier Teile vorgesehen hat: Ein Teil enthält Durchführungsbestimmungen für die Datenschutz-Grundverordnung, ein Teil enthält Regelungen zur Umsetzung der JI-Richtlinie, ein Teil enthält Regelungen für Bereiche, die weder der Datenschutz-Grundverordnung noch der JI-Richtlinie unterfallen, und ein vorangestellter Teil enthält gemeinsame Regelungen für alle drei Bereiche. Durch dieses Regelwerk wird sichergestellt, dass zum einen keine Regelungslücken entstehen und zum anderen für alle Bereiche ein einheitliches Datenschutzniveau gilt. Auch für Schleswig-Holstein halten wir es für unerlässlich, dass das Landesdatenschutzgesetz eine umfassende Regelung des allgemeinen Datenschutzrechts für die Bereiche der JI-Richtlinie und des Verfassungsschutzes sowie etwaiger anderer Bereiche, die nicht dem EU-Recht unterfallen, trifft. Nur so können Regelungslücken und Zersplitterungen vermieden werden.

Um die JI-Richtlinie vollständig umzusetzen, werden allgemeine Regelungen allerdings nicht ausreichen. Diese werden, wie dies auch jetzt der Fall ist, durch bereichsspezifische konkrete Regelungen ergänzt werden müssen. Dies betrifft in erster Linie das Landesverwaltungsgesetz für die polizeiliche Datenverarbeitung. Hier sind einige Anpassungen an das neue EU-Recht vorzunehmen:

- Beispielsweise verlangt die JI-Richtlinie, dass bei der Datenverarbeitung zwischen Verdächtigen einer Straftat, verurteilten Straftätern, Geschädigten einer Straftat und anderen Personen, wie etwa Zeugen, unterschieden wird. Für diese Personengruppen müssen unterschiedliche Rechtsfolgen gelten, die sich z. B. in unterschiedlichen Voraussetzungen für die Erhebung und Speicherung, aber auch in unterschiedlichen Löschfristen niederschlagen können.
- Differenziert werden muss außerdem zwischen Daten, die auf objektiven Tatsachen beruhen, und solchen, die auf persönlichen Einschätzungen basieren. Dies setzt voraus, dass der Charakter solcher Daten erkennbar ist, z. B. durch eine Kennzeichnung von Daten, die sich auf Einschätzungen stützen.
- Neu ist im Bereich der Strafverfolgung und polizeilichen Gefahrenabwehr, dass nun auch Einschränkungen für besondere Kategorien personenbezogener Daten vorzusehen sind, etwa für Gesundheitsdaten, aber auch für biometrische und genetische Daten. Da die frühere EG-Datenschutz-Richtlinie aus dem Jahr 1995, mit der solche besonderen Kategorien von Daten in das deutsche Recht eingeführt wurden, für den Bereich der Strafverfolgung und polizeilichen Gefahrenabwehr nicht galt, gibt es hier bislang solche Unterscheidungen nicht.
- Neu sind auch ausdrückliche Anforderungen an die Protokollierung von Verarbeitungsvorgängen in automatisierten Verarbeitungssystemen. Die JI-Richtlinie schreibt vor, dass die Erhebung, Veränderung, Abfrage, Offenlegung einschließlich Übermittlung, die Kombination und die Löschung der Daten protokolliert werden müssen.
- Bei Abfragen und Offenlegungen müssen außerdem die Begründung hierfür, das Datum und die Uhrzeit des Vorgangs, die abrufende oder übermittelnde Person und – bei Übermittlungen – der Empfänger der Daten erkennbar sein.

Was ist zu tun?

Allgemeine Datenschutzvorschriften sollten für alle der JI-Richtlinie unterfallenden Behörden und den Verfassungsschutz im Landesdatenschutzgesetz gemeinsam geregelt werden. Ergänzend sind punktuelle Änderungen in den Fachgesetzen vorzunehmen.

2.3 Informationssicherheit – von „I love you“ bis „WannaCry“

Alle haben dasselbe Ziel: mehr Informationssicherheit! Oder etwa nicht?

Entwickler von Schadsoftware sind kreativ – nicht nur, was das Ausnutzen von Sicherheitslücken angeht, sondern auch in der Namensgebung ihrer Erzeugnisse. Der Computerwurm „I love you“ verstopfte Anfang Mai 2000 das Netz, indem er sich massenhaft per E-Mail verbreitete. Dafür nutzte der Wurm das Adressbuch der E-Mail-Software. Dass es sich um ausführbaren Code handelte, konnten die meisten Windows-Nutzer nicht erkennen, die in ihrer empfangenen E-Mail die vermeintliche Liebesbotschaft einer ihnen bekannten Person öffneten. In solchen Fällen wird meistens recht schnell aufseiten der Antivirus-Tool-Anbieter nachgerüstet. Auch Hersteller von betroffener Anwendungssoftware oder von Betriebssystemen schließen bekannt gewordene Sicherheitslücken. Daher ist es wichtig, sicherheitsrelevante Updates durchzuführen – und natürlich nicht mit Systemen online zu gehen oder Daten auszutauschen, bei denen der Hersteller keine Aktualisierungen mehr anbietet, wie dies beispielsweise bei Windows XP der Fall ist.

Aber das Grundproblem ist ein anderes: Die Angreifer auf die Informationssysteme haben die Nase vorn. Eine Reaktion ist erst möglich, wenn die Probleme bemerkt werden. Abhilfe kommt also mit Zeitverzögerung.

In dem Fall von „WannaCry“ mit der Infektionswelle im Frühjahr 2017 merkten die Betroffenen ziemlich schnell, dass sie ein Problem hatten. Bei diesem Schadprogramm handelt es sich nämlich um erpresserische Ransomware, bei der Daten auf dem eigenen Rechner verschlüsselt werden und der Angreifer den Nutzer zur Zahlung eines „Lösegelds“ auffordert, um die Entschlüsselung zu ermöglichen. Gut, wenn man eine vollständige Datensicherung aus der

Zeit vor der Infektion hat. „WannaCry“ nutzt allerdings nicht irgendeine neue Sicherheitslücke, sondern das Einfallstor war einigen Akteuren schon länger bekannt, soll es doch aus dem Hacking-Arsenal des US-Geheimdienstes National Security Agency (NSA) stammen. Moment – dort werden Sicherheitslücken gesammelt? Und die Tools entwickelt, um die Sicherheitslücken auszunutzen? Ja, das ist nicht erst seit den Snowden-Enthüllungen bekannt. Mehrfach sind in der letzten Zeit Informationen über Sicherheitslücken und Hacking-Tools aus dem NSA-Fundus öffentlich geworden.

Offensichtlich führt ein (vermeintlich alleiniger) Wissensvorsprung bei der NSA nicht zu mehr Sicherheit, sondern spielt den Angreifern in die Hände. Statt für bessere Informationssicherheit zu sorgen, indem entdeckte Sicherheitslücken sofort geschlossen werden, will man sie selbst ausnutzen können – mit dem Risiko, dass auch andere Akteure diese Einfallstore für ihre Zwecke nutzen. Dass der Hersteller Microsoft in diesem Fall kurz vor der Infektionswelle wichtige Updates bereitstellte, weil sich eine Hacker-Gruppe mit den Informationen von der NSA brüstete, hat einen Teil des möglichen Schadens verhindert. Sogar für das gar nicht mehr gepflegte Betriebssystem Windows XP wurde als große Ausnahme ein Sicherheitsupdate ausgerollt. Aber eigentlich – so beurteilen es Sicherheitsforscher – hätte das Sicherheitsupdate schon früher verteilt werden können. Und man hätte deutlich auf die Wichtigkeit des Updates hinweisen müssen, weil es nur noch eine Frage der Zeit war, dass dieses Einfallstor ausgenutzt worden wäre. Oder sehr wahrscheinlich schon über längere Zeit ausgenutzt worden ist – mutmaßlich nicht nur, aber auch durch die NSA. Was wiederum ein zögerliches Schließen der Sicherheitslücken durch die jeweiligen Hersteller erklären würde.

Dieses Verhalten von Geheimdiensten und Herstellern muss uns wachrütteln. Angesichts der nicht mehr übersehbaren Sicherheitsrisiken ist es hochproblematisch, wenn die Datenver-

arbeitung unserer Informationsgesellschaft davon abhängig ist. Zumindest sind unabhängige Überprüfungen des Codes notwendig, damit die Fehler und Hintertüren im eingesetzten Verfahren schnell gefunden und beseitigt werden können. Am besten geschieht dies durch Veröffentlichung der Quelltexte – also des Programmcodes. Das Wissen der Entwickler, dass das Arbeitsergebnis einsehbar ist und nicht unter den Tisch gekehrt werden kann, ist der einzig wirksame Schutz vor Manipulation und Hintertüren.

Wenn zukünftig die Software in selbstfahrenden Autos nicht mehr nur über Abgaswerte, sondern in Gefahrensituationen sogar über Menschenleben entscheiden kann, muss transparent sein, wie eine solche Entscheidung abläuft. Die Quelldaten von Hard- und Software müssen überprüfbar sein.

Transparenz ist essentiell, wenn Algorithmen Annahmen über das Verhalten von Menschen treffen und sie zu einer wesentlichen Steuerungskomponente in wichtigen Lebensbereichen werden. Dies kann die Einschätzung der Kreditwürdigkeit betreffen, die Entscheidung über eine medizinische Behandlung, den verlangten Preis für eine Ware oder die Verweigerung einer Versicherung. Ohne Transparenz über die Funktion, die Parameter und deren Gewichtung ist es nicht möglich, Ergebnisse nachzuvollziehen und festzustellen, ob überhaupt ein geeignetes und faires Verfahren zugrunde liegt. Ohne Transparenz wird die Beherrschbarkeit der Technik infrage gestellt.

Besonders wichtig sind öffentliche Prüfbarkeit und unabhängige Überprüfung der eingesetzten Verfahren bei Sicherheitskomponenten wie Verschlüsselung und bei jeder Informationstechnik, die Einfluss auf unser Leben nimmt. Auch für Verfahren im E-Government gilt: Mit Geheimniskrämerei ist kein Staat zu machen.

Was ist zu tun?

Informationstechnik ist das Fundament der Informationsgesellschaft. Vorsätzlich eingebaute Hintertüren oder bewusst nicht beseitigte Sicherheitslücken darf es nicht geben. Ein Ausweg: Quelltextöffentlichkeit mit professioneller Qualitätssicherung.

2.4 Datenschutz neu denken!

Nach der Reform ist vor der Reform: Zwar hat es einige Jahre gedauert, bis die Datenschutz-Grundverordnung und das restliche Reformpaket auf europäischer Ebene umgesetzt wurde, aber man sieht schon jetzt, dass viele Regelungen unterkomplex sind oder den Anwender vollständig darüber im Unklaren lassen, wie mit neuen technischen Entwicklungen umgegangen werden kann. „Datenschutz neu denken!“ ist das Motto der Sommerakademien, die jährlich an einem Montag im Spätsommer von der DATENSCHUTZAKADEMIE Schleswig-Holstein ausgerichtet werden.

Im Berichtszeitraum lag der Schwerpunkt zunächst auf dem Thema „Vertrauenswürdige IT-Infrastruktur – ein (un?)erreichbares Datenschutzziel“ (2015), um sich mit dem brüchigen Fundament für unsere Informationsgesellschaft und dem IT-Sicherheitsgesetz auseinanderzusetzen (Tz. 2.3). Das „Datenschutz neu denken!“-Motto wurde im Folgejahr eingeführt, als „Werkzeuge für besseren Datenschutz“ im Mittelpunkt der Diskussion standen.

Noch ist es zu früh, die Wirksamkeit der Instrumente der Datenschutz-Grundverordnung (Tz. 2.1) zu evaluieren, die bislang nur auf dem Gesetzespapier stehen. In jedem Fall sind jedoch zusätzliche Werkzeuge sinnvoll, beispielsweise eine enge Kooperation mit den Verbraucherschützern, die über die Verbandsklage und den zivilrechtlichen Weg für Rechtsklarheit in verwandten Feldern sorgen und die Datenschutzdiskussion zusammen mit den Aufsichtsbehörden vorantreiben können. Die Rolle des Gerichtshofs der Europäischen Union (EuGH) wird künftig noch wichtiger, um einer Rechtszersplitterung entgegenzuwirken. Doch dürften sich die Verfahren dann nicht über Jahre und über mehrere Instanzen hinziehen. So wurde auf der Sommerakademie vorge-

schlagen, dass bereits erstinstanzliche Gerichte zunehmend von der Möglichkeit Gebrauch machen sollten, die Fragen dem EuGH vorzulegen. Dort solle ein beschleunigtes Verfahren ermöglicht werden, um Rechtssicherheit in Bezug auf die Auslegung der Datenschutz-Grundverordnung zu erreichen.

Die Sommerakademie 2017 im September wird das Thema der Herausforderung „Informationelle Nichtbestimmung“ beleuchten. Statt das Recht auf informationelle Selbstbestimmung, die Grundlage des Datenschutzes in Deutschland, auszuüben, scheinen sich mittlerweile viele Menschen für eine „Nichtbestimmung“ zu entscheiden – vielleicht weil Datenschutz nicht verständlich gemacht wird, weil die Technik zu komplex ist oder weil ihnen die Wahlmöglichkeiten nicht gefallen. Die Einwilligung – das wurde auch schon bei der vorjährigen Sommerakademie herausgearbeitet – funktioniert nicht, wenn man die Datenverarbeitung nicht mehr überblicken kann, beispielsweise wenn künftig „smarte“ Gegenstände ständig miteinander kommunizieren. Wir werden diskutieren, ob Datenschutz „by Default“ hier zu guten Lösungen verhilft oder dieses eigentlich sehr mächtige Prinzip aus der Datenschutz-Grundverordnung leerläuft oder ausgehebelt wird.

Für „Datenschutz neu denken!“ müssen viele Perspektiven zusammengeführt werden. Dies geschieht auch in dem Forum Privatheit (Tz. 8.1), an dem das ULD mitwirkt. Hier wird es in der nächsten Zeit um Vorschläge für eine zukunftsadäquate „Datenschutz-Governance“ gehen, d. h. um Kontroll- und Steuerungsstrukturen, die Politik, Gesetzgebung und Aufsichtsbehörden zu einer modernen Weiterentwicklung von Datenschutz befähigen.

Was ist zu tun?

Datenschutz neu zu denken bedeutet keinesfalls, dass alles über die letzten Jahrzehnte Errungene achtlos beiseitegewischt wird. Stattdessen ist zu prüfen, wie man Werte und Maßnahmen auf die digitalisierte Welt sinnvoll überträgt und dort weiterentwickelt.

03

KERNPUNKTE

Datenschutzgremium des Landtages

Auditierung der Videoüberwachung des Landeshauses

3 Landtag

3.1 Datenschutzgremium

Gemäß § 3 Abs. 4 Landesdatenschutzgesetz Schleswig-Holstein unterliegen der Landtag, seine Gremien, seine Mitglieder, die Fraktionen und deren Beschäftigte sowie die Landtagsverwaltung […] nicht den Bestimmungen dieses Gesetzes, soweit sie in Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeiten. Die Erfüllung von Verwaltungsaufgaben fällt dagegen unter das Landesdatenschutzgesetz. Der Landtag hat unter Berücksichtigung seiner verfassungsrechtlichen Stellung und der Grundsätze des Landesdatenschutzgesetzes eine Datenschutzordnung für die Verarbeitung personenbezogener Daten bei der Wahrnehmung parlamentarischer Aufgaben erlassen.

In der Datenschutzordnung werden die Zusammensetzung und die Aufgaben des Datenschutzgremiums geregelt: Das Datenschutzgremium des Landtages überwacht die Einhaltung der datenschutzrechtlichen Bestimmungen. Jede Fraktion ist mit einem Mitglied – in der Regel der oder dem datenschutzpolitischen Sprecher(in) – im Gremium vertreten. In der Legislaturperiode hat das Datenschutzgremium achtmal getagt. Die Landesbeauftragte für Datenschutz hat an den Sitzungen teilgenommen und das Datenschutzgremium auf Anfrage beraten.

Ein wichtiger Punkt im Berichtszeitraum war die Frage nach den Auswirkungen der Datenschutz-Grundverordnung auf die parlamentarische Tätigkeit. Die Antwort darauf lautet: Da die Wahrnehmung parlamentarischer Aufgaben nicht dem Unionsrecht unterfällt, gilt auch nicht die DSGVO. Dennoch bietet es sich an, mit Blick auf die DSGVO die Datenschutzordnung in der neuen Legislaturperiode daraufhin zu prüfen, ob Anpassungen oder Konkretisierungen sinnvoll sind.

Was ist zu tun?

Die Abgeordneten des Schleswig-Holsteinischen Landtages können bei Bedarf in allen Fragen des Datenschutzes die Landesbeauftragte für Datenschutz hinzuziehen.

3.2 Auditierung Zutrittsberechtigungssystem und Videoüberwachung des Landeshauses

Die vorerst letzte Reauditierung des Zutrittsberechtigungssystems und der Videoüberwachung des Landeshauses war 2014 (35. TB, Tz. 3.1). Seitdem wurden einige technische Erneuerungen an der Videoüberwachungsanlage vorgenommen; u. a. wurden Kameras, Serverhardware und Software aktualisiert. Grundsätzliche Änderungen der Funktionalität gab es nicht.

Die Landtagsverwaltung hat schon in der Projektierungsphase für diese Erneuerungen das ULD umfassend informiert und eingebunden sowie Hinweise für die Umsetzung aufgenommen. Bei einer bereits geplanten Reauditierung, bei der Umsetzung und Aktualisierung der Datenschutz- und Datensicherheitsmaßnahmen sind daher keine Überraschungen zu erwarten.

Was ist zu tun?

Stellen, die Zutrittsberechtigungssysteme und Videoüberwachungsanlagen einsetzen, sollten die Möglichkeit einer Auditierung prüfen.

04

KERNPUNKTE

Datenschutzgerechtes E-Government
Transparenz bei Funkzellenabfragen
Informationspflicht bei Datendiebstahl
Digitale Schule

4 Datenschutz in der Verwaltung

4.1 Allgemeine Verwaltung

4.1.1 Digitalisierung von Personalakten in der Landesverwaltung

Auf Landesebene besteht das Ziel, die Personalakten von Beschäftigten in Zukunft elektronisch zu führen. Hierfür wird die Staatskanzlei als zentrale Stelle tätig, die die Verantwortung für die Gewährleistung der Ordnungsmäßigkeit des automatisierten Verfahrens übernimmt. Näheres regelt eine Landesverordnung. Mit dem Digitalisieren der Aktenbestände wurde Dataport beauftragt, wobei wiederum Unteraufträge mit privaten Dienstleistern geschlossen wurden. Die Wahrnehmung der entsprechenden Aufgaben durch die Dienstleister kann im Wege einer Auftragsdatenverarbeitung erfolgen.

Das Oberverwaltungsgericht Schleswig hat im Jahr 2016 allerdings entschieden, dass für eine Auftragsdatenverarbeitung die Bestimmungen des Landesdatenschutzgesetzes nicht ausreichend sind. Das Landesbeamtenrecht ließ nach der Entscheidung des Verwaltungsgerichts eine Weitergabe von Personalaktendaten nur in eng begrenzten Ausnahmefällen zu. Die Einbindung von Dienstleistern war in diesen Vorschriften nicht vorgesehen. Der Landesgesetzgeber hat daraufhin das geltende Landesbeamtenrecht geändert und somit die Weitergabe von Personalakten an Dienstleister zum Zweck der Digitalisierung legitimiert. Fortan bedarf eine solche Auftragsdatenverarbeitung etwa der vorherigen Zustimmung durch die oberste Dienstbehörde.

Der Auftrag mit den Dienstleistern ist schriftlich zu verfassen, wobei u. a. die nach dem Landesdatenschutzgesetz zu treffenden technisch-organisatorischen Maßnahmen, die Berechtigung zur Begründung von Unteraufträgen, Kontroll- und Weisungsrechte des Auftraggebers sowie Details zur Abwicklung des Auftrags festzulegen sind. Die Beauftragung privater Dienstleister darf nur erfolgen, wenn beim Auftraggeber sonst Störungen im Geschäftsablauf auftreten können oder der Auftragnehmer die übertragenen Aufgaben erheblich kostengünstiger erledigen kann und die beim Auftragnehmer mit der Datenverarbeitung beauftragten Beschäftigten besonders auf den Schutz der Personalakten verpflichtet sind. Soweit private Dienstleister eingebunden werden, ist im schriftlichen Auftrag festzuhalten, dass die Dienstleister eine Kontrolle durch das ULD zu dulden haben.

Das ULD hat neben der inhaltlichen Prüfung von Personalakten auch im Gesetzgebungsverfahren zur Änderung des Landesbeamtenrechts Hinweise gegeben, Vertragsprüfungen vorgenommen und eine Beratung zur Umsetzung technisch-organisatorischer Sicherheitsmaßnahmen durchgeführt. Insbesondere dürfen die Digitalisate vom Dienstleister nur in verschlüsselter Form und unter Verwendung einer qualifizierten elektronischen Signatur versandt werden.

Qualifizierte elektronische Signatur

Mithilfe einer digitalen Signatur lassen sich Authentizität und Unverfälschtheit von Daten prüfen. Beispielsweise lassen sie sich bei elektronischen Akten einsetzen, um die Integrität sicherzustellen. Technisch funktioniert die Signatur auf Basis eines asymmetrischen Verschlüsselungsverfahrens. Das deutsche Signaturgesetz unterscheidet verschiedene Kategorien. Für eine qualifizierte elektronische Signatur sind ein qualifiziertes Zertifikat, ausgestellt von einem Zertifizierungsdiensteanbieter, und eine sichere Signaturerstellungseinheit nötig.

4.1.2 Neufassung des Landesmeldegesetzes

Im Jahr 2015 wurde das Landesmeldegesetz neu gefasst, nachdem das Bundesmeldegesetz in Kraft getreten war. Das ULD hat zu den beabsichtigten Neuregelungen eine Stellungnahme abgegeben (Landtagsumdruck 18/4501). Mit dem Gesetzentwurf sollte u. a. für Sicherheits- und Strafverfolgungsbehörden die Möglichkeit geschaffen werden, im Wege eines automatisierten Datenabrufs einen näher geregelten Datensatz zu bestimmten Personen zu erlangen. Zu diesem Datensatz zählten z. B. die letzte frühere Anschrift, Angaben zu einem gesetzlichen Vertreter, der Familienstand und das Sterbedatum.

Nach den bundesrechtlichen Vorgaben dürfen entsprechende erweiterte Datensätze durch die Sicherheits- und Strafverfolgungsbehörden abgerufen werden, soweit im Bundes- oder Landesrecht Anlass und Zweck der Übermittlungen und Abrufe, der Datenempfänger und die zu übermittelnden Daten festgelegt werden. Das ULD bat im Rahmen des Gesetzgebungsverfahrens um konkretisierende Formulierungen bezüglich der Anlässe und Zwecke der Datenübermittlungen. Im Ergebnis wurden die Identitätsfeststellung und die Adressvalidierung als mögliche Anlässe eines Datenabrufs geregelt. Hinsichtlich der Zwecke für eine Datenübermittlung wurde fortan in das Landesmeldegesetz aufgenommen, dass die Datenübermittlung nur zulässig ist, soweit dies im Einzelfall zum Zweck der Gefahrenabwehr, der Strafverfolgung, der Strafvollstreckung, des Strafvollzugs, der Unterrichtung der Landesregierung und anderer zuständigen Stellen über Gefahren für die freiheitliche demokratische Grundordnung, den Bestand und die Sicherheit des Bundes und der Länder oder der Ahndung von Ordnungswidrigkeiten erforderlich ist.

Der Gesetzentwurf (Landtagsdrucksache 18/2777) sah auch vor, dass die Meldebehörden im Falle der Abmeldung, Anmeldung oder des Todes u. a. Angaben zum Familienstand an den NDR übermitteln. Das ULD gab zu bedenken, dass die Kenntnis des Familienstands für die Beitragsveranlagung nicht erforderlich ist. Nach den rundfunkrechtlichen Bestimmungen ist für jede Wohnung von dessen Inhaber ein Rundfunkbeitrag zu entrichten. Als Inhaber wird jede Person vermutet, die dort nach dem Melderecht gemeldet ist oder im Mietvertrag für die Wohnung als Mieter genannt ist. Der Familienstand spielt also für diesen Zweck keine Rolle. Die entsprechende Änderung fand ungeachtet dessen Eingang im Landesmeldegesetz, wodurch nun eine nicht notwendige Datenübermittlung an den NDR vorgesehen ist.

Was ist zu tun?

Dem Landtag wird empfohlen, die Vorschrift des § 8 Abs. 1 Satz 1 Nr. 7 des Landesmeldegesetzes zu streichen, um eine künftige Übermittlung von Angaben zum Familienstand an den NDR zu vermeiden.

4.1.3 Regeln für E-Government im Landesverwaltungsgesetz – mit Datenschutz

Mittlerweile findet bereits das halbe Leben in digitalen Netzen statt. Auch Verwaltungsdaten werden bereits zu einem großen Teil automatisiert verarbeitet. Während Online-Einkauf und Online-Banking gängig geworden sind, stehen bislang erst wenige Verwaltungsdienstleistungen online zur Verfügung. Hier kommt es in besonderem Maße darauf an, dass die Angebote rechtskonform gestaltet sind und das notwendige – hohe – Niveau an Datenschutz und Informationssicherheit umsetzen.

Die allgemeinen Bedingungen für den elektronischen Behördengang in Schleswig-Holstein haben über den Gesetzentwurf zur Modernisierung der elektronischen Verwaltung Anfang 2017 in das Landesverwaltungsgesetz Eingang gefunden. So regelt beispielsweise § 52a die elektronische Kommunikation der Verwaltung, mit der elektronischen Aktenführung und Vorgangsverwaltung beschäftigt sich § 52d, und zur Frage der elektronischen Zahlungsverfahren und Rechnungen sind die Vorgaben in

§ 52g enthalten. Insgesamt sind zehn Paragrafen (§ 52a bis § 52j) hinzugekommen.

E-Government

Unter E-Government versteht man den Einsatz von Informations- und Kommunikationstechnik zur Erfüllung der Aufgaben der öffentlichen Verwaltung und der Regierung. Dies betrifft auch den Datenaustausch zwischen den öffentlichen Stellen und Bürgerinnen und Bürgern. Künftig soll mithilfe des E-Governments der Behördengang in vielen Fällen über das Internet ermöglicht werden.

Während des Gesetzgebungsverfahrens konnte das ULD zum Gesetzentwurf (Landtagsdrucksache 18/4663) Stellung nehmen (Landtagsumdruck 18/7178) und wesentliche Änderungen erreichen:

- Im Entwurf waren die Anforderungen an eine sichere Kommunikation mit Behörden per Verschlüsselung aus unserer Sicht zu unscharf formuliert gewesen. Insbesondere wurde in der Begründung zum Gesetzentwurf die Transportverschlüsselung für die Übertragung von Dokumenten mit personenbezogenen Daten genannt und betont, dass eine Ende-zu-Ende-Verschlüsselung „unter Umständen“ bei der Übermittlung von besonders sensitiven Daten angeboten werden könne. Dies reichte uns nicht, denn zumindest bei besonders schutzwürdigen Daten – beispielsweise Sozialdaten, Gesundheitsdaten oder Steuerdaten – darf eine Ende-zu-Ende-Verschlüsselung nicht optional sein.
  Im Ergebnis wurde der Passus in § 52a Abs. 8 geändert zu: „Die elektronische Kommunikation erfolgt unter Verwendung eines dem Stand der Technik entsprechenden und der Schutzbedürftigkeit der Kommunikation angemessenen Verschlüsselungsverfahrens.“ Wir werden darauf einwirken, dass es nicht zu Fehlinterpretationen dieser Vorschrift kommt, denn eindeutig sind mehrere Ende-zu-Ende-Verschlüsselungsverfahren dem Stand der Technik zuzuordnen. In den Fällen, in denen eine Behörde dies für besonders schutzwürdige Daten nicht anbieten kann, muss wegen eines zu hohen Risikos des Zugriffs auf die Daten auf die elektronische Übermittlung verzichtet werden.
- § 52g LVwG regelt die Anforderungen an elektronische Zahlungsverfahren, wenn Bürgerinnen und Bürger Gebühren oder sonstige Forderungen im Rahmen eines elektronisch durchgeführten Verwaltungsverfahrens entrichten müssen. Dort haben wir die – eigentlich für die Verwaltung selbstverständlichen, aber in der Praxis der weitverbreiteten Zahlungssysteme nicht immer umgesetzten – Anforderungen des Datenschutzes ergänzt. So heißt es nun: „[…] muss die Behörde die Einzahlung dieser Gebühren […] durch Teilnahme an mindestens einem im elektronischen Geschäftsverkehr üblichen Zahlungsverfahren ermöglichen, das die Anforderungen des Datenschutzes und der Datensicherheit nachweislich erfüllt.“ Auch in diesem Punkt werden wir der Verwaltung beratend zur Seite stehen.
- Mit § 52i LVwG wird eine Zentrale E-Governmentstelle eingeführt, die dazu dient, die Einheitlichkeit der elektronischen Verfahrenshandhabung in der öffentlichen Verwaltung sicherzustellen und die rechtliche und technische Kompetenz zu bündeln. Strategisch wird diese Stelle sehr wichtig sein, um nicht nur Sicherheit, sondern auch Datenschutz in die Prozesse einzubauen – so wie es Artikel 25 Datenschutz-Grundverordnung fordert. Daher wurde auf unseren Wunsch in § 52i LVwG der folgende Satz aufgenommen: „Dabei berücksichtigt sie die Anforderungen des Datenschutzes, insbesondere des Prinzips ‚Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen‘.“

Was ist zu tun?

Bei der Planung und Umsetzung von E-Government-Verfahren muss Datenschutz von Anfang an berücksichtigt und eingebaut werden. Das ULD bietet der Verwaltung und insbesondere der Zentralen E-Governmentstelle seine Beratung an, damit vorbildliche Lösungen geschaffen werden.

4.2 Polizei und Verfassungsschutz

4.2.1 Gefahrengebiete auch in Schleswig-Holstein

Im Berichtszeitraum hat sich das ULD mit der Regelung im Landesverwaltungsgesetz zur Ausweisung von und zu polizeilichen Kontrollen in Gefahrengebieten befasst. In einem Gefahrengebiet darf die Polizei Personen anhalten und Fahrzeuge in Augenschein nehmen. Gegenüber dem Landtag hat das ULD eine Stellungnahme zu einem Gesetzentwurf der Fraktion der PIRATEN (Landtagsdrucksache 18/1995) abgegeben, der auf eine Abschaffung der Gefahrengebiete abzielte. Eine vollständige Abschaffung der Befugnis zur Ausweisung von Gefahrengebieten und zur Durchführung von Polizeikontrollen in diesen Gebieten sieht das ULD nicht als verfassungsrechtlich zwingend geboten an. Für eine verhältnismäßige Ausgestaltung der Norm haben wir jedoch Einschränkungen und Präzisierungen der Befugnisnorm empfohlen. Diese sind nun durch einen Vorschlag der Fraktionen von SPD und BÜNDNIS 90/DIE GRÜNEN sowie der Abgeordneten des SSW umgesetzt worden (Landtagsumdruck 18/6941). Im Einzelnen handelt es sich um folgende Änderungen:

- Die vorherige Formulierung „Tatsachen, insbesondere dokumentierte polizeiliche Lageerkenntnisse“ hat das ULD als missverständlich kritisiert. Der Begriff „Lageerkenntnisse“ umfasst sprachlich nicht nur Tatsachen. Das ULD hat eine Präzisierung empfohlen, um eine andere Auslegung zweifelsfrei auszuschließen. Außerdem hat das ULD empfohlen, die Anforderungen an den Zusammenhang zwischen den Tatsachen und den in § 180 Abs. 3 Satz 1 Landesverwaltungsgesetz (LVwG) genannten Schutzgütern deutlicher festzulegen. Die nunmehr geltende erweiterte Formulierung trägt diesen Empfehlungen Rechnung: „[...] soweit Tatsachen, insbesondere dokumentierte polizeiliche Lageerkenntnisse, dies erfordern, weil sie auf einen Kriminalitätsschwerpunkt hindeuten und anzunehmen ist, dass eine Gefahr für die öffentliche Sicherheit vorliegt.“

Gefahrengebiet

Die sogenannten Gefahrengebiete sind in § 180 Abs. 3 Landesverwaltungsgesetz Schleswig-Holstein geregelt:

„Die Polizei darf im öffentlichen Verkehrsraum zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung, bei denen Schaden für Leib, Leben oder Freiheit oder gleichgewichtiger Schaden für Sach- oder Vermögenswerte oder die Umwelt zu erwarten sind, Personen kurzzeitig anhalten und mitgeführte Fahrzeuge einschließlich deren Kofferräume oder Ladeflächen in Augenschein nehmen. Maßnahmen nach Satz 1 werden [...] angeordnet, soweit Tatsachen, insbesondere dokumentierte polizeiliche Lageerkenntnisse, dies erfordern, weil sie auf einen Kriminalitätsschwerpunkt hindeuten und anzunehmen ist, dass eine Gefahr für die öffentliche Sicherheit vorliegt. In [...] Anordnung ist die Maßnahme in örtlicher, sachlicher und zeitlicher Hinsicht auf den für die vorbeugende Bekämpfung der in Satz 1 aufgeführten Kriminalität erforderlichen Umfang zu beschränken. Die Anordnung soll vorab in geeigneter Weise bekannt gemacht werden, es sei denn, ihr Zweck wird dadurch gefährdet. Die Anordnung ist zunächst auf maximal 28 Tage zu befristen. [...]“

- Des Weiteren hat das ULD empfohlen, die Ausweisung von Gefahrengebieten transparenter für die Betroffenen zu gestalten. Die Presseberichterstattung hat gezeigt, dass die Ausweisung von Gefahrengebieten sieben Jahre nach Inkrafttreten der Vorschrift in der Öffentlichkeit nahezu unbekannt war – selbst denjenigen, die seit geraumer Zeit in einem Gefahrengebiet wohnten. Daher hat das ULD empfohlen, dass eine Bekanntmachung der Ausweisung im Gesetz jedenfalls für den Regelfall vorgesehen werden sollte. Auch dieser Empfehlung ist der Änderungsantrag der Fraktionen gefolgt. Im Gesetz heißt es nun: „Die Anordnung soll vorab in geeigneter Weise bekannt gemacht werden, es sei denn, ihr Zweck wird dadurch gefährdet."

4.2.2 Prüfung der Falldatei Rauschgift

In einer gemeinsamen Prüfaktion der Datenschutzbeauftragten des Bundes und der Länder wurde die Speicherpraxis der jeweiligen Länderpolizeien in der Falldatei Rauschgift (FDR) unter die Lupe genommen.

Falldatei Rauschgift

Bei der „Falldatei Rauschgift" (FDR) handelt es sich um eine Bund-/Länderdatei des polizeilichen Informationssystems INPOL des Bundeskriminalamts. Sie dient insbesondere der Aufklärung oder Verhütung von Straftaten nach dem Betäubungsmittelgesetz, die von länderübergreifender, internationaler oder erheblicher Bedeutung sind.

Wir haben die Speicherungen der Landespolizei Schleswig-Holstein geprüft. Dabei haben wir folgende Feststellungen getroffen:

Fälle, die in der FDR gespeichert werden, sind in der Regel nach fünf Jahren – in besonders schweren Fällen nach zehn Jahren – zu löschen. Eine längere Speicherung ist nur erlaubt, wenn bei der Aussonderungsprüfung festgestellt wird, dass die Daten weiterhin erforderlich sind. Dies ist nachvollziehbar zu dokumentieren. Die Prüfung der Stichprobe in Schleswig-Holstein hat ergeben, dass 38 % der geprüften Fälle älter als zehn Jahre waren. Ein Fall lag bereits über 20 Jahre zurück. Eine dokumentierte Begründung für die lange Speicherung fehlte.

Eine Speichervoraussetzung nach dem Bundeskriminalamtgesetz ist die sogenannte Negativprognose. Es muss wegen der Art oder Ausführung der Tat, der Persönlichkeit des Betroffenen oder sonstiger Erkenntnisse Grund zu der Annahme bestehen, dass zukünftig weitere Strafverfahren gegen den Beschuldigten oder Tatverdächtigen zu führen sind. Diese Erkenntnisse müssen gerichtsfest dokumentiert werden. In der Hälfte der geprüften Fälle konnte keine dokumentierte Negativprognose vorgefunden werden.

Außerdem dürfen nur Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung in INPOL gespeichert werden. Die Prüfung hat gezeigt, dass in Schleswig-Holstein auch Fälle gespeichert wurden, für die diese Voraussetzungen offensichtlich nicht vorlagen. Dies betrifft insbesondere Straftaten ohne länderübergreifenden oder internationalen Bezug. Diese dürfen nur gespeichert werden, wenn sie von „erheblicher Bedeutung" sind. Solche Straftaten sind der mittleren Kriminalität zuzuordnen. Die Prüfung hat allerdings ergeben, dass beispielsweise auch Daten über Erstkonsumenten harter Drogen in der FDR gespeichert wurden, selbst wenn nur eine – nach dem Betäubungsmittelgesetz als Bagatellfall anzusehende – „geringe Menge" für den Eigengebrauch konsumiert wurde. Auch Fälle im Bereich der sogenannten Normalmenge wurden pauschal gespeichert. In keinem Fall wurde das Vorliegen einer Straftat von erheblicher Bedeutung nachvollziehbar dokumentiert.

Bei einigen der Stichproben war nicht ersichtlich, warum Fälle trotz Einstellung des Verfahrens weiter gespeichert wurden. In einem anderen Fall wurde der Name einer geschädigten Ärztin im recherchefähigen Freitext genannt. Dies wäre allenfalls mit Einwilligung der betroffenen Ärztin zulässig. Ob eine solche erteilt wurde, konnte im Rahmen der Prüfung nicht ermittelt werden.

Ähnliche Ergebnisse haben auch die Prüfungen in den anderen Bundesländern und beim Bund ergeben. Im Zuge der Migration der Fälle aus der FDR in das Verfahren PIAV (Polizeilicher Informations- und Analyseverbund, Tz. 4.2.4), die für Anfang 2018 geplant ist, hat das

Bundeskriminalamt (BKA) zusammen mit den Polizeien der Länder ein Konzept erarbeitet, um die hohe Zahl an unzulässig gespeicherten Datensätzen zu bereinigen. Es ist danach zu erwarten, dass bundesweit schätzungsweise 90 % der Fälle aus der FDR gelöscht werden.

Ein hoher Prozentsatz der unrechtmäßig gespeicherten Datensätze betrifft Erstkonsumenten harter Drogen sowie Drogentote. Daten über diese Personengruppen wurden bisher in erster Linie für statistische und Planungszwecke gespeichert. Auch wenn diese Daten nichts in einer für operative Zwecke geführten Bund-/Länderdatei zu suchen haben, so sind diese Daten natürlich von gesellschaftspolitischer und strategischer Bedeutung. Das ULD spricht sich daher dafür aus, diese Daten zukünftig – möglichst anonymisiert – in separaten Dateien oder als Bundesstatistik zu führen.

Das Landeskriminalamt (LKA) hat in einer Stellungnahme zum Prüfbericht mitgeteilt, dass in allen beanstandungsrelevanten Fällen eine Bereinigung erfolgt sei. Darüber hinaus würden die bei der Prüfung festgestellten Mängel nicht erst bei der Migration von Daten in PIAV, sondern bereits aktuell in der Datenpflege berücksichtigt. Hierdurch sowie durch den mittlerweile angestoßenen „Cleansing-Prozess“ des BKA zur Bereinigung der Altdaten sowie die klaren Vorgaben für die Speicherung neuer Fälle in PIAV ist für die Zukunft eine Verbesserung der Situation zu erwarten.

Was ist zu tun?

Im Hinblick auf zukünftige Speicherungen muss durch technische und qualitätssichernde Maßnahmen gewährleistet werden, dass nur relevante Fälle gespeichert werden und dass die Dokumentation der gesetzlichen Speichervoraussetzungen stets vorliegt. Löschfristen sind einzuhalten, Verfahrensausgänge müssen berücksichtigt werden.

4.2.3 Prüfung der Datei „Fußball SH“

Im Jahr 2016 hat eine Prüfung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit die vielfache illegale Speicherung von Fußballfans in einer polizeilichen Datei aufgedeckt. Das ULD hat daraufhin ebenfalls die fußballspielbezogene Speicherpraxis in Schleswig-Holstein untersucht.

Bei der Landespolizei Schleswig-Holstein wird die Datei „Fußball SH“ geführt. Diese Datei wird ausschließlich durch sogenannte szenekundige Beamte gepflegt. Sie dient als Grundlage für präventive gefahrenabwehrende Maßnahmen vor einem Spiel (z. B. Gefährderansprachen, Aufenthaltsverbote usw.) sowie der Entwicklung von Einsatzkonzepten, die Störungen oder Gefahren für die öffentliche Sicherheit verhindern sollen.

Gespeichert werden die Namen von Personen, die im Zusammenhang mit Fußballspielen durch Straftaten oder als Störer im Sinne des Landesverwaltungsgesetzes aufgefallen sind und gegen die polizeiliche Maßnahmen ergriffen wurden (z. B. ein Platzverweis). Die Daten werden offen bei den Betroffenen erhoben und für maximal zwei Jahre gespeichert. Fällt eine Person erneut auf, verlängert sich diese Frist jeweils um zwei weitere Jahre, ausgehend vom Zeitpunkt der letzten Speicherung. Kontakt- oder Begleitpersonen werden nicht gespeichert.

Eine unverhältnismäßige, rechtswidrige Speicherung konnte bei der Prüfung nicht festgestellt werden. Die Datei war zum Zeitpunkt der Prüfung gut gepflegt, und die Daten sind nur für einen eng begrenzten, fachlich zuständigen Personenkreis einsehbar. Die automatische Verlängerung der Speicherung birgt allerdings die Gefahr, dass zurückliegende Vorkommnisse beliebig lange gespeichert bleiben, obwohl sie für die aktuelle Lagebeurteilung nicht mehr relevant sind. Das ULD hält daher die Festlegung einer maximalen Speicherdauer für erforderlich.

Darüber hinaus bedarf es für die erstmalige Speicherung zukünftig einer dokumentierten Negativprognose. Es muss wegen der Art oder Ausführung und Schwere der Tat sowie der

Persönlichkeit des Betroffenen Grund zu der Annahme bestehen, dass der Betroffene zukünftig durch weitere Strafverfahren bzw. Störungen auffällig werden wird. Diese Hürde sieht der Landesgesetzgeber bereits für die Speicherung von Straftaten vor. Sie muss daher erst recht für die Speicherung niederschwelliger Handlungen gelten.

Die Landespolizei hat zwischenzeitlich reagiert und die Hinweise des ULD umgesetzt. Außerdem wurde der Katalog der vorhandenen Datenfelder noch einmal überprüft und auf das erforderliche Maß reduziert.

Was ist zu tun?

Der Landesgesetzgeber ist gefordert, eine Rechtsgrundlage zu schaffen, die die Speicherung von personenbezogenen Daten für den Zweck zukünftiger Gefahrenabwehr regelt. Im Gegensatz zu den Vorgaben im Bereich der Speicherung für zukünftige Strafverfolgung sind die Rechtsgrundlagen zur Speicherung für Fälle zukünftiger Gefahrenabwehr zu generell oder fehlen vollständig. Dabei erfordert gerade die Speicherung im Bereich unterhalb der Strafverfolgung eine normenklare und verhältnismäßige Regelung.

4.2.4 Polizeilicher Informations- und Analyseverbund im Betrieb

Im Mai 2016 wurde die erste Stufe des Polizeilichen Informations- und Analyseverbunds (PIAV, 35. TB, Tz. 4.2.2) in Schleswig-Holstein durch den Innenminister für den produktiven Einsatz freigegeben. In der Stufe 1 werden Informationen über Delikte mit Bezug zu Waffen und Sprengstoff an PIAV angeliefert. Die Erfahrungen aus dieser Stufe bilden die Grundlage für die Weiterentwicklung von PIAV sowie die Einführung weiterer Stufen.

Das ULD wird seit dem Start des Projekts regelmäßig durch das Landeskriminalamt über den Fortschritt informiert und bringt sich fachlich mit ein. Die bisherigen Erfahrungen aus der Stufe 1 zeigen, dass es durchaus Verbesserungen im Datenschutz im Vergleich zu den bisherigen INPOL-Falldateien gibt.

Durch die Festlegung sogenannter PIAV-Relevanzkriterien werden Sachbearbeiter IT-gestützt darauf aufmerksam gemacht, wenn ein Vorgang PIAV-relevant sein könnte. Dies trägt dazu bei, dass auf der einen Seite keine notwendige Erfassung übersehen wird; auf der anderen Seite ergibt sich daraus auch schnell, dass ein Vorgang gegebenenfalls nicht nach PIAV angeliefert werden soll oder darf. Natürlich kann die Informationstechnik nur eine unterstützende Rolle übernehmen. Letztlich entscheiden, ob die gesetzlichen Voraussetzungen für eine Anlieferung vorliegen, muss immer ein Mensch.

In diesem Zusammenhang stellt PIAV insbesondere deshalb eine Verbesserung dar, weil jeder Vorgang qualitätsgesichert angeliefert wird. Das bedeutet, dass in der Regel neben dem Sachbearbeiter und seinem Vorgesetzten noch eine weitere Qualitätssicherungsstelle den Vorgang vor der Anlieferung an PIAV auf Plausibilität und Vollständigkeit prüft. Dieses Vorgehen führt dazu, dass auch menschliche Fehler bei der Eingabe oder grobe Bewertungsfehler erkannt und korrigiert werden können.

Eine weitere Verbesserung besteht in der Kopplung der Speicherdauer an die Speicherung des zugrunde liegenden Vorgangs im Vorgangs- oder Fallbearbeitungssystem des Landes. Wird der Grundvorgang im Landessystem gelöscht, erfolgt automatisch die Löschung in PIAV. Gleichzeitig beachtet PIAV die maximalen Speicherfristen nach dem Bundeskriminalamtgesetz und signalisiert, wenn eine Aussonderungsprüfung notwendig ist. Über Jahrzehnte gespeicherte Altdatenbestände, wie sie z. B. bei der Prüfung der Falldatei Rauschgift (Tz. 4.2.2) vorgefunden wurden, werden dadurch in PIAV vermieden.

Da das Verfahren PIAV sehr komplex ist und sich nach wie vor im Aufbau befindet, sind noch

einige Baustellen im Datenschutz zu bearbeiten, und es werden sicherlich im Laufe der Zeit neue hinzukommen.

So hat die Prüfung der Falldatei Rauschgift (INPOL) z. B. Defizite in der Dokumentation der Speichervoraussetzungen ergeben. Insbesondere in Fällen, in denen es auf die Erheblichkeit einer Straftat als Speichervoraussetzung ankommt, gibt es Nachbesserungsbedarf. Der weitere Ausbau von PIAV wird zeigen, ob die allgemeinen und dateispezifischen PIAV-Relevanzkriterien, die zusätzlichen Qualitätssicherungsstufen und Schulungen zu einer Verbesserung beitragen werden.

Da sich PIAV in der Stufe 1 auf eine einzige Datei beschränkt, wird sich außerdem erst mit dem Start der weiteren Stufen und der Einführung weiterer Dateien zeigen, wie die Analyse- und Auswertefunktionen arbeiten und welche Auswirkungen dies für die Betroffenen hat.

Von Interesse werden auch die für die Erschließung der Daten erforderlichen Zugriffsberechtigungen sein. Diese legt jedes Land individuell fest. Theoretisch könnte also ein PIAV-Teilnehmer entscheiden, allen seinen Sachbearbeitern dateiübergreifend lesenden Zugriff zu gewähren. Die Einführung von sogenannten ermittlungsunterstützenden Hinweisen dient ebenfalls zur dateiübergreifenden Erschließung der Daten. Wie diese Möglichkeiten von den einzelnen Teilnehmern genutzt werden und wie sich dies mit den Prinzipien der Erforderlichkeit und der Zweckbindung der Daten vereinbaren lässt, wird genau zu prüfen sein.

Die nächste Ausbaustufe von PIAV ist für Anfang 2018 vorgesehen.

Was ist zu tun?

Im Rahmen der nächsten Ausbaustufen wird die Verknüpfung und Auswertung von unterschiedlichen Daten und Dateien eine immer größere Rolle spielen. Bei der Fortschreibung der Konzepte muss daher den Grundsätzen der Erforderlichkeit und der Zweckbindung eine besondere Bedeutung zukommen. Die Kooperation der Projektgruppe PIAV mit dem ULD hat sich bewährt. Sie sollte auch künftig weitergeführt werden.

4.2.5 Rechen- und Dienstleistungszentrum zur Telekommunikationsüberwachung

Über die Pläne der norddeutschen Küstenländer, die technische Durchführung der Telekommunikationsüberwachung (TKÜ) in einem gemeinsamen Zentrum – dem Rechen- und Dienstleistungszentrum (RDZ) – zu bündeln, hat das ULD im Jahr 2013 berichtet (34. TB, Tz. 4.2.3). In den Folgejahren war das Projekt zunächst nicht weiterverfolgt worden. Doch im Berichtszeitraum wurden nicht nur die Arbeiten am Projekt fortgesetzt, sondern auch wesentliche Grundsteine für das gemeinsame Zentrum gelegt. Es wurde ein Staatsvertrag über die Einrichtung und den Betrieb des gemeinsamen Zentrums geschlossen.

Hierzu haben die Datenschutzbeauftragten der beteiligten Länder gemeinsam Stellung genommen (Landtagsumdruck 18/6179). Der von ihnen angemeldete Änderungsbedarf wurde aufgegriffen. Der Staatsvertrag entspricht damit den datenschutzrechtlichen Anforderungen. Wichtig ist in diesem Zusammenhang jedoch, dass Einzelheiten der Datenverarbeitung bei Telekommunikationsüberwachungen nicht im Staatsvertrag geregelt werden. Der Staatsvertrag regelt lediglich die Struktur des RDZ und der Kontrolle der Länder, einschließlich der Datenschutzkontrolle, über das gemeinsame Zentrum.

Da das RDZ seine Leistungen im Wege der Datenverarbeitung im Auftrag für die Behörden der teilnehmenden Länder erbringen wird, ist ein Auftragsdatenverarbeitungsvertrag zwischen der Landespolizei Schleswig-Holstein und dem RDZ zu schließen. In diesem sind die Einzelheiten der Datenverarbeitung festzulegen, z. B. das genaue Leistungsspektrum des RDZ, Zugriffsrechte auf die gespeicherten Daten, Maßnahmen zur Gewährleistung einer Mandantentrennung zwischen den TKÜ-Daten der einzelnen Länder sowie Maßnahmen zur Gewährleistung der Kontrollierbarkeit und der Sicherheit der Datenverarbeitung.

Die Anlage für die Telekommunikationsüberwachung wird, wie es auch jetzt in den Landeskriminalämtern der Fall ist, von einem externen Diensteanbieter bereitgestellt werden. Bei der Ausschreibung der Leistung ist darauf zu achten, dass die Anforderungen an Datenschutz und Datensicherheit umfassend und präzise formuliert werden, damit diese Kriterien bei der Vergabe berücksichtigt und im Echtbetrieb erfüllt werden.

Das ULD begleitet die Einführung des RDZ federführend für die Länder in datenschutzrechtlichen Fragen und empfiehlt der Projektgruppe RDZ, auch für die anstehenden Schritte die Datenschutzbeauftragten eng einzubinden.

Was ist zu tun?

Nachdem der Staatsvertrag ratifiziert wurde, sind nun das Konzept für die Datenverarbeitung und der Vertrag zur Auftragsdatenverarbeitung festzulegen. Ebenso wie die Vergabe für die TKÜ-Anlage sollten diese Arbeiten in enger Abstimmung mit den Datenschutzbeauftragten der beteiligten Länder erfolgen.

4.2.6 Reichsbürger – Meldung von Behörden an die Polizei

Nach tödlichen Schüssen eines Reichsbürgers auf einen Polizeibeamten in Bayern befasste sich auch die Landespolizei Schleswig-Holstein intensiver mit dieser Gruppierung. Um ein Lagebild über Reichsbürger in Schleswig-Holstein zu erstellen, wandte sie sich an die Kommunen und bat um Informationen. Da die Anfragen nicht einheitlich formuliert waren, wurden unterschiedliche Informationen angefordert. Dies führte in einigen Kommunen zu Irritationen. Für die Lagebilderstellung wurden nur anonymisierte Daten benötigt. Bei einigen Kommunen wurden jedoch auch personenbezogene Daten abgefragt. Dabei wurde teilweise danach differenziert, ob die Person bereits als Störer im Sinne des Polizeirechts aufgefallen war oder nicht. Teilweise wurden ohne Differenzierung Meldungen über alle als Reichsbürger bekannten Personen verlangt. Das ULD hat zu diesen Anfragen gegenüber den Kommunen und dem Innenministerium Stellung genommen.

Die Übermittlung von personenbezogenen Daten über Reichsbürger kann in Einzelfällen nach dem Polizeirecht zulässig sein. Voraussetzung ist, dass sie für die Aufgabenerfüllung der übermittelnden oder empfangenden Stelle erforderlich ist und – soweit die Übermittlung zu einem anderen Zweck erfolgt als dem Zweck, der der Speicherung der Daten zugrunde liegt – auch die Änderung des Verarbeitungszwecks zulässig ist. Nach dem Landesdatenschutzgesetz dürfen personenbezogene Daten zweckändernd verarbeitet (hier: übermittelt) werden, wenn die Abwehr erheblicher Nachteile für das Allgemeinwohl oder von Gefahren für Leben, Gesundheit, persönliche Freiheit oder sonstiger schwerwiegender Beeinträchtigungen der Rechte Einzelner dies gebietet.

Reichsbürger

„Als ‚Reichsbürger' oder auch ‚Reichsregierungen' bezeichnen sich mehrere sektenartige Gruppen von Rechtsextremen und Verschwörungstheoretikern. Die Kernideologie der Reichsbürger ist antisemitisch, geschichtsrevisionistisch und demokratiefeindlich. Neben der Ablehnung der Demokratie gehört häufig die offensive Leugnung des Holocaust zur Agitation. Das Bundesinnenministerium geht bundesweit von mehreren Hundert Mitgliedern aus. [...] Als Konsequenz weigern sich die Reichsbürger, Steuern zu zahlen, und erkennen die deutsche Gesetzgebung nicht an. Manche stellen eigene Reisepässe und Führerscheine ihres Fantasie-Staates her und ernennen sich selbst zu ‚Ministern' verschiedener ‚Reichsregierungen'. Erste Gruppen dieser Art entstanden in den 1980er-Jahren. Seit 2010 treten sie verstärkt in Erscheinung."

Quelle: Bundeszentrale für politische Bildung, Dossier Rechtsextremismus

http://www.bpb.de/politik/extremismus/rechtsextremismus/173908/glossar?p=69

Sofern eine Übermittlung von Daten über Reichsbürger an die Polizei auf diese Grundlage gestützt werden soll, müssen solche Gefahren für die genannten Rechtsgüter für jede Person, die an die Polizei gemeldet wird, aus Sicht der übermittelnden Stelle schlüssig sein. Soweit die Kommunen nicht über eigene Erkenntnisse verfügen, die die von den jeweiligen Reichsbürgern ausgehende Gefährdung für die genannten Rechtsgüter begründen, ist diese von der Polizei darzulegen. Ein allgemeiner Hinweis auf frühere gefährliche Situationen mit Reichsbürgern reicht hierfür nicht aus. Denn es bleibt danach möglich, dass es einen oder wenige Reichsbürger gibt, die für eskalierende Situationen verantwortlich gemacht werden können, während andere Kontakte zu Reichsbürgern im Hinblick auf die Rechtsgüter Leben, Gesundheit und persönliche Freiheit ungefährlich bleiben.

Weniger strenge Anforderungen gelten für Übermittlungen durch die Ordnungsämter, da für diese eine andere Rechtsgrundlage Anwendung findet. Für diese gelten die bereichsspezifischen Regelungen des Polizeirechts. Danach können personenbezogene Daten zwischen Polizeidienststellen des Landes, zwischen Ordnungsbehörden sowie zwischen Ordnungsbehörden und der Polizei übermittelt werden, soweit dies zur Erfüllung polizeilicher oder ordnungsbehördlicher Aufgaben erforderlich ist. Die Abwehr von Gefahren für die öffentliche Sicherheit ist Aufgabe sowohl der Polizei als auch der Ordnungsbehörde. Es reicht nach dieser Rechtsgrundlage eine Gefahr auch für geringwertigere Rechtsgüter als Leben und Gesundheit. Auch eine besondere Eintrittswahrscheinlichkeit und -nähe, wie etwa eine konkrete Gefahr, werden nicht vorausgesetzt. Damit dürfte es für das Ordnungsamt möglich sein, dort gespeicherte eigene Erkenntnisse über Reichsbürger der Polizei mitzuteilen.

Strengere Anforderungen gelten hingegen für Sozialleistungsträger. Hier sind die allgemeinen Vorschriften des Sozialgesetzbuchs X zu beachten. Außerdem können sich aus anderen Sozialgesetzbüchern bereichsspezifische, oftmals noch weiter einschränkende Sonderregelungen ergeben.

Sonderregelungen sind außerdem für Daten des Gesundheitsamts zu berücksichtigen. Amtsärzte unterliegen dem strafbewehrten Berufsgeheimnis und der ärztlichen Schweigepflicht. Zum Schutz dieser Verpflichtungen verfügen sie außerdem nach der Strafprozessordnung über ein Zeugnisverweigerungsrecht.

Im Ergebnis hält das ULD Datenübermittlungen durch das Ordnungsamt an die Polizei über solche Reichsbürger vertretbar, die beim Ordnungsamt selbst bekannt sind und dort als gefährdend für jegliche Rechtsgüter der öffentlichen Sicherheit eingeschätzt werden. Dasselbe gilt, wenn andere Ämter – ausgenommen Gesundheitsamt und Sozialamt – Daten über solche Reichsbürger übermitteln, die dort als gefährdend für Leben, Gesundheit, persönliche Freiheit oder vergleichbare Rechtsgüter angesehen werden. Personenbezogene Daten aus Sozial- und Gesundheitsämtern dürfen in der Regel nicht übermittelt werden. Eine pauschale Übermittlung personenbezogener Daten über jegliche Reichsbürger, unabhängig von polizeilich relevanten Vorfällen, ist nicht zulässig.

Was ist zu tun?

Generell benötigen Ämter vor der Übermittlung personenbezogener Daten an die Polizei eine Rechtsgrundlage.

4.3 Justiz

4.3.1 IT-Gesetz für die Landesjustiz – Regeln für ein Outsourcing

Im Jahr 2016 ist das IT-Gesetz für die Justiz in Schleswig-Holstein in Kraft getreten. Das Gesetz bildet die Grundlage für die zentrale Verwaltung der Informations- und Kommunikationstechnik der Gerichte und Staatsanwaltschaften durch eine beim Justizministerium eingerichtete Gemeinsame IT-Stelle und die Betreuung der IT durch Dataport. Es enthält zahlreiche Vorgaben für technische und organisatorische Maßnahmen, die dem Schutz der richterlichen Unabhängigkeit dienen sollen.

Zu diesem Zweck sieht das Gesetz u. a. die Einrichtung einer IT-Kontrollkommission vor. Diese hat die Aufgabe, die Einhaltung des Gesetzes, der Verträge mit externen IT-Dienstleistern und aller sonstigen Bestimmungen, die der Bereitstellung von IT-Infrastrukturen, der Betreuung der eingesetzten IT und der Gewährleistung der IT-Sicherheit in den Gerichten und Staatsanwaltschaften dienen, zu kontrollieren. Um eine Kontrolle durchführen zu können, erhält sie umfassende Auskunfts-, Zutritts- und Einsichtsrechte. Ihre Aufgaben und Befugnisse ähneln denen des ULD oder behördlicher Datenschutzbeauftragter. Und auch wenn die Zielrichtung des Gesetzes und damit der Kontrolle durch die IT-Kontrollkommission eine andere ist, gibt es weitgehende Überschneidungen zum Datenschutz. Denn die Maßnahmen, mit denen die richterliche Unabhängigkeit sichergestellt werden soll, sind vielfach dieselben, mit denen die Datenschutzrechte der Betroffenen gewährleistet werden. Es geht um Vertraulichkeit der Datenverarbeitung gegenüber dem Ministerium und gegenüber Dataport genauso wie um die Revisionsfähigkeit der von Dataport getätigten Handlungen.

Folgerichtig sieht das Gesetz vor, dass das ULD die IT-Kontrollkommission bei ihrer Aufgabenwahrnehmung berät. Damit hat das ULD eine neue Aufgabe erhalten: Es berät nun nicht mehr nur im Hinblick auf den Datenschutz, sondern auch unter dem Blickwinkel der richterlichen Unabhängigkeit. Die IT-Kontrollkommission hat sich mittlerweile konstituiert und Kontakt mit dem ULD aufgenommen. Gemeinsam wurden Schulungen durch das ULD vereinbart.

4.3.2 Verantwortung für die Datenverarbeitung klarstellen – zentrale Stelle in der Justiz

Im letzten Tätigkeitsbericht (35. TB, Tz. 4.3.10) hatten wir darüber berichtet, dass Fachverfahren in der Justiz, wie z. B. forumSTAR, häufig zentral vom Justizministerium beschafft und eingerichtet werden. Auch Verträge mit Dienstleistern, wie z. B. Dataport, werden vom Justizministerium geschlossen. Die tatsächliche Nutzung der Fachverfahren erfolgt hingegen in den Gerichten, Staatsanwaltschaften, Vollzugsanstalten oder anderen Stellen der Justiz. Diese Konstellation entspricht der einer zentralen Stelle nach § 8 Abs. 2 Landesdatenschutzgesetz. Diese Regelung ist ausdrücklich für automatisierte Verfahren geschaffen worden, die gemeinsam von mehreren Stellen betrieben werden. Danach kann die Verantwortung für die Gewährleistung der Ordnungsmäßigkeit des automatisierten Verfahrens von der Verantwortung für die gespeicherten Daten abgetrennt und auf eine zentrale Stelle übertragen werden.

Dies ist für das Verfahren forumSTAR wie für andere Fachverfahren in der Justiz faktisch erfolgt. Damit diese Aufteilung der Verantwortung rechtlich wirksam werden kann, bedarf es nach § 8 Abs. 2 Landesdatenschutzgesetz jedoch einer Rechtsverordnung. In dieser Verordnung ist das Zusammenwirken der zentralen Stelle mit den datenverarbeitenden Stellen, hier den Gerichten, Staatsanwaltschaften, Vollzugsanstalten und anderen Stellen der Justiz, sowie die Aufteilung von Aufgaben und Verantwortlichkeiten zu regeln.

Auch im Berichtszeitraum ist die Verordnung über die Einrichtung einer zentralen Stelle nicht erlassen worden. Sie ist jedoch dringend erforderlich, um die datenschutzrechtliche Verantwortung für die Fachverfahren der Justiz den tatsächlichen Gegebenheiten entsprechend zu verteilen. Ohne diese Verordnung bleibt die datenschutzrechtliche Verantwortung vollständig bei den Gerichten, Staatsanwaltschaften und Vollzugsanstalten. Diese kennen weder die Funktionsweise des Verfahrens in allen Einzelheiten noch haben sie hinreichenden Einfluss auf Gestaltung und Konfiguration der Verfahren. Ihrer Verantwortung können sie naturgemäß nicht in vollem Umfang nachkommen.

Was ist zu tun?

Dem Justizministerium sollte dringend die Verantwortung für die Ordnungsmäßigkeit der Fachverfahren der Justiz durch Verordnung übertragen werden.

4.3.3 Kontrollmitteilungen an Finanzämter zu Geldauflagen bei Einstellung von Strafverfahren

Gegen eine Petentin wurde ein Strafverfahren geführt und durch das Gericht gegen Zahlung einer Geldauflage eingestellt. Als ihr Verteidiger Einsicht in die Gerichtsakte nahm, staunte er: Das Gericht hatte die Verfahrenseinstellung dem für die Petentin zuständigen Finanzamt als sogenannte Kontrollmitteilung übersandt. Das ULD hat diese Übermittlung als unzulässig beanstandet.

Wird ein Strafverfahren gegen Geldauflage eingestellt, dann wird dem Betroffenen in der Regel aufgegeben, einen vom Gericht festgelegten Betrag an eine vom Gericht festgelegte Einrichtung zu zahlen. Bei den Einrichtungen handelt es sich oftmals um solche, die gemeinnützige, mildtätige oder kirchliche Zwecke verfolgen. Geldzuwendungen an diese Einrichtungen können normalerweise von der Steuer abgesetzt werden. Dies gilt jedoch nicht für Zahlungen, die als Auflage einer Einstellung eines Strafverfahrens vorgenommen werden. Solche Zahlungen sind ausdrücklich nicht steuerbegünstigt. Damit die Zahlungen von den Betroffenen nicht als Zuwendung in der Steuererklärung angegeben werden können, informieren die Gerichte die Empfänger der Zahlungen darüber, dass es sich um eine Geldauflage im Rahmen der Einstellung eines Strafverfahrens handelt. Die Empfänger sollen dies berücksichtigen und für die Zahlung keine Spendenbescheinigung ausstellen.

So war es auch im Fall der Petentin. Die Zahlung hätte sie mangels Spendenbescheinigung steuerlich nicht geltend machen können. Die Höhe der Geldauflage überstieg die Grenze für Zuwendungen, die ohne Spendenbescheinigung von der Steuer abgesetzt werden können. Für eine gleichzeitige Information an das Finanzamt bestand also in diesem Fall kein Grund. Somit gab es für die Übermittlung der Daten auch keine gesetzliche Grundlage.

Diese Mitteilung ist nicht zu verwechseln mit Kontrollmitteilungen, die in anderen Fällen an Finanzämter versendet werden. Mit der typischen Kontrollmitteilung informiert eine Stelle das Finanzamt über steuerrelevante Sachverhalte, in der Regel über steuerpflichtige Einnahmen des Steuerpflichtigen. Hier handelt es sich um Sachverhalte und Informationen, auf deren Kenntnis das Finanzamt einen Anspruch hat und die das Finanzamt bei rechtmäßigem Verhalten des Steuerpflichtigen von diesem selbst ohnehin erfährt. Bei der Kontrollmitteilung im Fall der Petentin war es umgekehrt: Bei rechtmäßigem Verhalten der Petentin hätte das Finanzamt nichts von dem Strafverfahren gegen die Petentin erfahren und auch nicht erfahren dürfen.

Was ist zu tun?

Informationen über Geldauflagen in Strafverfahren dürfen in der Regel nicht an Finanzämter weitergegeben werden. Dies darf nur ausnahmsweise erfolgen, wenn im konkreten Einzelfall Anlass zu der Besorgnis besteht, dass der Betroffene die Zahlung rechtswidrig geltend machen wird.

4.3.4 Weitergabe von Familienfotos aus einer Durchsuchung an den Urheberrechtsverband GVU

Bei einer Durchsuchung der Wohnung eines Beschuldigten hat die Polizei neben tatrelevantem Material auch die Speicherkarte einer Digitalkamera sichergestellt. Die Kamera gehörte nicht dem Beschuldigten, sondern dessen Partnerin. Auf dieser Speicherkarte befanden sich Familienfotos, die für die Ermittlungen nicht von Bedeutung waren. Besonders irritiert hat die Petentin, dass die Polizei die Speicherkarte ungesehen an die Gesellschaft für Urheberrechtsverletzungen e. V. (GVU) zur Auswertung weitergab, obwohl schon eine kurze Durchsicht gezeigt hätte, dass diese keine ermittlungsrelevanten Daten enthielt.

Das ULD hat die Übermittlung der Daten an die GVU als Verstoß gegen Datenschutzvorschriften beanstandet. Für die Übermittlung gab es keine Rechtsgrundlage. Es bestehen schon erhebliche Zweifel, ob die GVU überhaupt zur Unterstützung der Ermittlungen als Sachverständige hinzugezogen werden darf, wie es vorliegend geschehen ist. Das ULD hat Übermittlungen an Interessenverbände von Rechteinhabern auch in früheren Fällen beanstandet (30. TB, Tz. 4.3.3), weil ein Interessenverband nicht als Sachverständiger im Strafverfahren in Betracht kommt. Hierfür fehlt ihm die erforderliche Neutralität.

Dies sah im vorliegenden Fall zunächst auch das Gericht so, das die Petentin mit einer Beschwerde angerufen hatte. Auf eine Gegenvorstellung der Staatsanwaltschaft änderte es seine Auffassung allerdings in diesem Punkt. Das Gericht stellte nunmehr fest, dass es neben der GVU nur einen einzelnen weiteren Sachverständigen für den Bereich der vorliegenden Ermittlungen gibt. Auch dieser würde zur Klärung von Zweifelsfragen hinsichtlich der Rechteinhaberschaft mit der GVU zusammenarbeiten. Daher erkannte das Gericht die GVU als Sachverständige an und wies die Beschwerde insoweit zurück. Das Risiko für die Rechte der Betroffenen erhöht sich jedoch erheblich, wenn private Stellen bei Durchsuchungen hinzugezogen werden oder Auswertungen sichergestellter Materialien übernehmen, statt dass die Strafverfolgungsbehörden selbst die Kompetenz dazu vorhalten oder aufbauen. Im Fall der GVU gilt sogar, dass sie eigene Interessen verfolgt und daher nicht von einer Unparteilichkeit ausgegangen werden kann.

Davon unabhängig war es im vorliegenden Fall unverhältnismäßig, da nicht erforderlich, der GVU ohne vorige Durchsicht sämtliches sichergestelltes Material zur Auswertung zu übermitteln. Hier hätte zunächst durch die Polizei eine erste Sichtung erfolgen müssen. Bei dieser Sichtung hätte vermutlich schnell festgestellt werden können, dass die Speicherkarte der Petentin keine ermittlungsrelevanten Daten, dafür aber zahlreiche persönliche Fotos ihrer Familie enthielt. Dies hat auch das Beschwerdegericht festgestellt.

Die fehlende Vorprüfung kann auch nicht durch eine Einwilligung des Betroffenen ersetzt werden. Eine Einwilligung in eine Datenübermittlung, die für die Ermittlungen nicht erforderlich ist, kann dem Betroffenen nicht abverlangt werden. Diese Möglichkeit scheidet praktisch bereits deshalb häufig aus, weil nicht alle von der Übermittlung betroffenen Personen den Ermittlungsbehörden bekannt sind und um ihre Einwilligung ersucht werden können. Gegen die Einwilligungslösung spricht aber vor allem das Wesen der Eingriffsverwaltung. Dieses ist durch gesetzlich bestimmte Eingriffsbefugnisse der Behörden gekennzeichnet, die den Behörden den für die Aufgabenerfüllung nötigen Handlungsspielraum eröffnen. Das Instrument der freiwilligen Einwilligung kann nicht dazu genutzt werden, die Eingriffsbefugnisse von Behörden zu erweitern oder sie von ihnen obliegenden Pflichten zu befreien (siehe auch 31. TB, Tz. 4.3.6 zur Einwilligung in die Datenübermittlung an die GVU).

Was ist zu tun?

Sichergestellte oder beschlagnahmte personenbezogene Daten dürfen nur in dem Umfang an Dritte zur Auswertung gegeben werden, wie es für die Ermittlungen erforderlich ist. Hierzu müssen die Ermittlungsbehörden die Daten nötigenfalls vorher sichten. Eine Einwilligung des Betroffenen kann diesen Schritt nicht ersetzen. Zusätzlich muss die Unabhängigkeit polizeilicher Ermittlungsarbeit gewährleistet werden. Risiken des Missbrauchs personenbezogener Daten durch das Einbeziehen von Dritten müssen unterbunden werden.

4.3.5 Akteneinsichtsrecht für Europaratsausschuss zur Verhütung von Folter

Der Europaratsausschuss zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe, abgekürzt CPT, führt regelmäßig Kontrollen in deutschen Vollzugs- und Gewahrsamseinrichtungen durch. Streitig ist dabei die Frage, ob er auch Einsichtsrechte in die Gefangenenpersonal- und Krankenakten hat. Rechtliche Grundlage für das Einsichtsrecht ist das Europäische Übereinkommen zur Verhütung von Folter. Es enthält eine Vorschrift zu den Auskunftsrechten des CPT. Doch diese Vorschrift erfüllt als Regelung des internationalen Rechts nicht die Maßstäbe, die nach deutschem Verfassungsrecht an die Bestimmtheit von Eingriffsbefugnissen anzulegen sind. Insbesondere die deutsche Sprachfassung ist sehr eng gefasst, denn sie gesteht dem CPT nur das Recht zu, Auskünfte zu verlangen. Akteneinsicht ist dort nicht genannt. Die englische Sprachfassung ist hingegen weiter gefasst. Danach ist dem CPT „other information available which is necessary“ („andere verfügbare Informationen, die erforderlich sind“) zur Verfügung zu stellen.

Commitee for the Prevention of Torture (CPT)

CPT ist der Name des Kontrollausschusses, der mit dem Europäischen Übereinkommen zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe eingesetzt wurde.

Das ULD hat in einer Stellungnahme gegenüber dem Justizministerium die Auffassung vertreten, dass die Vorschrift im Europäischen Übereinkommen ausreicht, um dem CPT Akteneinsicht zu gewähren. Dabei hat das ULD berücksichtigt, dass es sich um internationales Recht handelt, das üblicherweise weitaus weniger bestimmt ist als deutsches Recht. Bei der Auslegung der Vorschrift kann nicht nur die deutsche Sprachfassung betrachtet werden, sondern es müssen auch andere Sprachfassungen berücksichtigt werden. Auch die Entstehungsgeschichte der Regelung ist mit zu betrachten. Aus dieser ergibt sich ein klarerer Umriss des Kontrollauftrags des CPT und der korrespondierenden Unterstützungspflichten der kontrollierten Stellen. Wünschenswert wäre eine deutlichere Klarstellung im nationalen Recht. Da dies jedoch landesrechtlich zu regeln wäre, entstünde die Gefahr unterschiedlicher Rechtsvorschriften. Dies hätte zur Folge, dass ein internationales Kontrollgremium, das unter Beteiligung von Deutschland nach internationalem Recht eingesetzt wurde, in den einzelnen Ländern unterschiedliche Befugnisse hätte. Angesichts dieses bestehenden Risikos hält das ULD ergänzende, klarstellende nationale Regelungen nicht für zwingend erforderlich.

Auch eine Beschränkung des Akteneinsichtsrechts auf solche Akten, in deren Einsichtnahme die Betroffenen eingewilligt haben, ist kein gangbarer Weg. Dies würde die Kontrolle des CPT weitgehend einschränken. Eine anlasslose Kontrolle nach eigenen Kriterien, die sich auch auf Betroffene erstreckt, die nicht mehr in einer Vollzugs- oder Gewahrsamseinrichtung untergebracht sind, wäre damit nicht möglich.

Was ist zu tun?

Dem CPT ist auf sein Verlangen Einsicht in Akten zu erteilen, auch soweit personenbezogene Daten betroffen sind. Eine Einwilligung der Betroffenen ist hierfür nicht erforderlich. Gleichwohl sollte Schleswig-Holstein sich für eine bundesweit einheitliche Konkretisierung der Mitwirkungspflichten der kontrollierten Stellen einsetzen.

4.3.6 Fehladressierung von E-Mails bei Polizei und Justiz

Ein kommunaler Abgeordneter erhielt im Berichtszeitraum mehrere E-Mails von der Polizei und von der Staatsanwaltschaft. Manchmal handelte es sich um Mitteilungen unter Kollegen, in einem Fall wurden ihm Anträge für Durchsuchungen zugeschickt – sehr sensible Daten! Für ihn bestimmt war jedoch keine dieser E-Mails. Eigentlich hätten sie einen namensgleichen Polizeibeamten erreichen sollen. Grund für den Fehlversand war in allen Fällen eine Verwechslung. Beide Personen sind im globalen E-Mail-Adressverzeichnis der „+1“-Infrastruktur des Landes (Tz. 6.1) geführt. In der Listenansicht des Adressverzeichnisses sind Einträge für beide Personen untereinander aufgelistet, wobei der Eintrag des Abgeordneten mit einem Symbol versehen ist, das externe Empfänger kennzeichnet. Man hätte also an dem Symbol erkennen können, dass die Kommunikation an einen falschen Empfänger gehen würde. Doch in der Listenansicht wird nicht die zugehörige E-Mail-Adresse dargestellt, aus der deutlich hervorgeht, wer externer Empfänger ist. So kann es leicht zu Verwechslungen kommen.

Sowohl die Staatsanwaltschaften als auch die Polizei haben nach Bekanntwerden dieser Fehlversendungen angeordnet, dass das globale Adressverzeichnis als primäres Adressverzeichnis zu deaktivieren ist und stattdessen das lokale Adressverzeichnis der Staatsanwaltschaften oder der Polizei als primäres Adressverzeichnis einzustellen ist. Durch diese Maßnahme wird das Risiko eines versehentlichen E-Mail-Versands an Adressen außerhalb des eigenen Behördenkreises erheblich reduziert.

Das ULD hat auf die Risiken und den richtigen Umgang damit in einer Pressemitteilung hingewiesen:

https://datenschutzzentrum.de/artikel/1048-1.html

Was ist zu tun?

Generell ist beim Versand von E-Mails Umsicht geboten, denn hier kommt es leicht zu Fehladressierungen. Empfänger sind sorgfältig auszuwählen. Dies gilt nicht nur für die Auswahl aus Adressverzeichnissen, sondern auch für die Nutzung der „Antworten“-Funktion und für die Verwendung des CC- und des BCC-Feldes.

4.3.7 Mehr Transparenz bei Funkzellenabfragen

Im letzten Tätigkeitsbericht hat das ULD über die Ergebnisse einer Prüfung von nicht individualisierten Funkzellenabfragen in Strafverfahren berichtet (35. TB, Tz. 4.3.1). Der Prüfbericht des ULD ist im Berichtszeitraum veröffentlicht und im Innen- und Rechtsausschuss des Schleswig-Holsteinischen Landtages diskutiert worden (Landtagsumdruck 18/5038). Betont haben wir die Notwendigkeit, dass die erhobenen Verkehrsdaten spätestens zum Abschluss des Verfahrens gelöscht werden müssen.

Nicht individualisierte Funkzellenabfrage

Bei einer nicht individualisierten Funkzellenabfrage werden von Mobilfunkanbietern alle Verkehrsdatensätze erhoben, die an einem Ort in einem von der Ermittlungsbehörde festgelegten Zeitraum erzeugt worden sind. Dies können Telefonate, SMS oder Datenverbindungen zum Internet sein. Mit der Abfrage soll zumeist ermittelt werden, welche Anschlussinhaber sich in der Nähe eines Tatorts aufgehalten haben. Häufig wird dieses Mittel bei dem Verdacht einer Serienstraftat angewandt, um zu prüfen, ob an unterschiedlichen Tatorten dieselben Telefonnummern oder Mobilfunkgeräte auftauchen.

Die Rechtsgrundlage für nicht individualisierte Funkzellenabfragen ergibt sich aus § 100g Abs. 2 Satz 2 StPO. Laut Antwort der Landesregierung auf eine Kleine Anfrage der PIRATEN (Landtagsdrucksache 18/5172) wurden im Jahr 2016 in Schleswig-Holstein 866 nicht individualisierte Funkzellenabfragen durchgeführt.

In der Diskussion im Ausschuss ging es vor allem um die Transparenz für die Betroffenen. Durch eine Funkzellenabfrage werden oft zahlreiche Personen erfasst und deren Verkehrsdaten anschließend für die Dauer des Ermittlungsverfahrens und in vielen Fällen auch darüber hinaus gespeichert. Wenn sie nicht namentlich identifiziert werden, müssen sie über die Maßnahme nicht benachrichtigt werden. In ihre Grundrechte wurde dennoch eingegriffen, und das völlig ohne ihr Wissen. Diese Situation ist im Hinblick auf den Grundrechtsschutz für die Vielzahl von Betroffenen unbefriedigend. Das ULD hat daher Lösungsideen veröffentlicht, wie durch freiwillige Maßnahmen die Transparenz für die Betroffenen erhöht werden kann (Landtagsumdruck 18/7553).

Zu den im Bericht diskutierten Ansätzen für mehr Transparenz gehören die (verpflichtende) schriftliche Benachrichtigung der Betroffenen, wenn ihre Identität bekannt geworden ist oder sie sich mit ihrer Telefonnummer für eine Mitteilung registriert haben, die Information per SMS-Nachricht, die öffentliche Bekanntmachung sowie eine kombinierte Methode, in der die Nutzenden der Mobilgeräte entscheiden, ob und wie sie informiert werden möchten (siehe Abbildung).

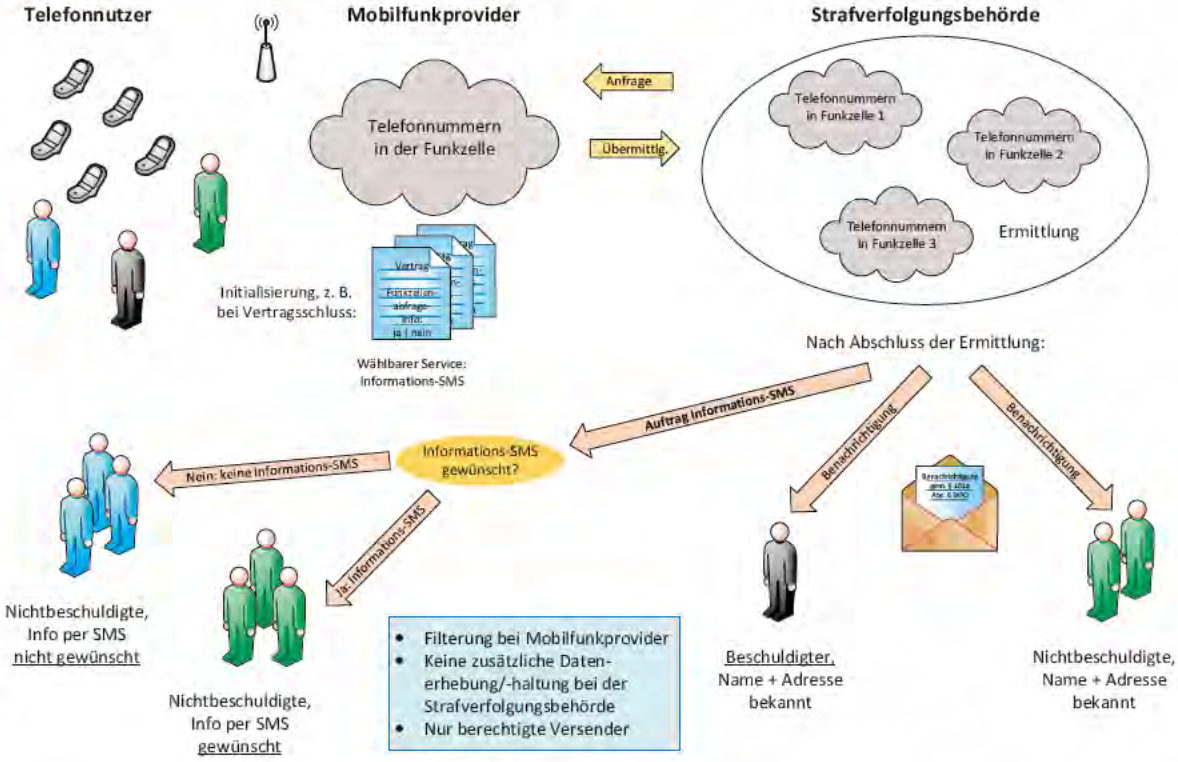


Abbildung: Kombination von Benachrichtigung und Informations-SMS

In dieser kombinierten Lösung ist es nicht notwendig, dass die Strafverfolgungsbehörden ein Register über diejenigen führen, die eine Information begehren, wenn sie von einer Funkzellenabfrage betroffen sind. Dies könnte stattdessen beim Mobilfunkanbieter oder bei Treuhändern (nicht in der Abbildung dargestellt) geschehen. Auch würden die Strafverfolgungsbehörden bei der Information über die Funkzellenabfrage die bisher unbekannten Identifikationsdaten nicht erhalten. In einer erweiterten Fassung könnte zusätzlich eine Information per (verschlüsselter) E-Mail an zu diesem Zweck von den Betroffenen ausgewählte Adressen versandt werden. Die Betroffenen hätten also die Wahl, ob und wenn ja auf welche Weise und unter welcher (gegebenenfalls wechselnden) Adresse sie informiert werden möchten.

Der Lösungsansatz berücksichtigt nicht nur die StPO mit der (verpflichtenden) Benachrichtigung, sobald die Identität bekannt wird, sondern ergänzt diese Anforderung um eine empfehlenswerte Information für alle anderen Betroffenen. In die Konzeption sind die Überlegungen eingeflossen, wie die Gewährleistungsziele aus dem Standard-Datenschutzmodell (Tz. 6.3) berücksichtigt werden können. Offensichtlich dient die Idee der verbesserten Transparenz, aber auch Datenminimierung und Nichtverkettbarkeit (es sollen keine überschießenden Informationen bei den Strafverfolgungsbehörden vorliegen) und die Intervenierbarkeit (die Betroffenen entscheiden selbst über das Ob und Wie und können bei Bedarf nachfragen) werden berücksichtigt.

Der Prüfbericht des ULD ist veröffentlicht unter:

http://www.landtag.ltsh.de/infothek/wahl18/umdrucke/5000/umdruck-18-5038.pdf

Der Bericht „Möglichkeiten für verbesserte Transparenz bei Funkzellenabfragen“ ist veröffentlicht unter:

http://www.landtag.ltsh.de/infothek/wahl18/umdrucke/7500/umdruck-18-7553.pdf

Was ist zu tun?

Verbesserte Transparenz bei Funkzellenabfragen ist möglich und sollte umgesetzt werden. Das ULD hat einen Lösungsansatz in die Diskussion eingebracht und unterstützt gerne bei der Verfeinerung des Konzepts und der Umsetzung.

4.4 Ausländerverwaltung

4.4.1 Quartiersmanagement für Geflüchtete

Der Zustrom von Geflüchteten hat im Berichtszeitraum die Verwaltung auch im Hinblick auf die Datenverarbeitung vor große Herausforderungen gestellt. Dabei musste vieles zunächst improvisiert werden, denn zeitgemäße Strukturen und IT-Verfahren waren häufig nicht vorhanden. Betroffen waren vor allem die Erstaufnahmeeinrichtungen für Geflüchtete. Nachdem die meisten Geflüchteten die Erstaufnahmeeinrichtungen nun wieder verlassen haben, ist es an der Zeit, die eingerichteten Verfahren datenschutzgerecht zu gestalten und zu dokumentieren.

In den Erstaufnahmeeinrichtungen fehlte anfangs der Überblick: Es gab kein geeignetes System, um die aufgenommenen Personen, die Belegung der Zimmer, die ausgegebenen Mahlzeiten oder die durchgeführten Gesundheitsuntersuchungen zu erfassen. Schnell war klar, dass sich hieran etwas ändern musste, und es wurde ein IT-Verfahren mit der Bezeichnung Quartiersmanagement (QMM) eingerichtet. Dieses basiert auf einer Chipkarte, die jeder Bewohner der Einrichtung erhält und mit der Berechtigungen zum Zutritt zum Gebäude oder zur Geld- und Essensausgabe nachgewiesen werden. Gleichzeitig können Zutritt und Verlassen des Gebäudes, Essensausgabe, anstehende und wahrgenommene Termine mit dem Bundesamt für Migration und Flüchtlinge und weitere Ereignisse mit der Karte erfasst werden. Im System können Informationen über die Identität der untergebrachten Personen

sowie Angaben z. B. zur Herkunft, Volks- und Religionszugehörigkeit gespeichert werden. Auch Gesundheitsdaten, wie z. B. durchgeführte Untersuchungen und dabei getroffene Feststellungen, können gespeichert werden. Dabei handelt es sich großenteils um besonders sensible personenbezogene Daten.

Hierbei ist eine Vielzahl datenschutzrechtlicher Fragen zu klären, angefangen mit der Rechtsgrundlage für die jeweiligen Datenkategorien über Zugriffsrechte von beteiligten Stellen und Personen bis hin zur Löschung der Daten. Die Staatskanzlei hat für die Koordinierung der IT-Verfahren im Ausländerbereich ein Projekt eingerichtet und bindet das ULD eng in die Erstellung der Verfahrensdokumentation ein. Ferner berät das ULD zu Fragen der Datensicherheit.

Was ist zu tun?

Gerade in diesem besonders sensiblen Bereich ist eine sorgfältige Gestaltung und Dokumentation von IT-Verfahren wichtig. Dass zunächst andere Aufgaben vorrangig waren, ist nachvollziehbar. Nun müssen diese Arbeiten schnellstmöglich nachgeholt werden. Die enge Kooperation der Staatskanzlei mit dem ULD hat sich bewährt. Wir bieten weiterhin unsere Unterstützung an.

4.4.2 Hinweise für ehrenamtliche Helferinnen und Helfer für Geflüchtete

Kommunikation zwischen Geflüchteten und Ehrenamtlichen, die Geflüchtete unterstützen, in Deutschland Fuß zu fassen, muss reibungslos und schnell funktionieren. Dafür sind elektronische Kommunikationsmittel wie E-Mail, SMS und Messenger-Dienste für viele unerlässlich. Genauso unerlässlich ist es, dabei die personenbezogenen Daten der Betroffenen ausreichend zu schützen. Ein Zugriff durch Dritte auf die ausgetauschten Informationen kann dazu führen, dass der neue Aufenthaltsort und die Lebensumstände der Geflüchteten bekannt werden. Dies kann nicht nur die Geflüchteten selbst gefährden, sondern auch Angehörige, die noch im Herkunftsland leben oder sich ebenfalls auf der Flucht befinden. Beispielsweise haben staatliche Organisationen, darunter auch ausländische Geheimdienste, die Möglichkeit, elektronische Kommunikation mithilfe modernster Technologien zu durchsuchen.

Das ULD hat daher ein Hinweisblatt veröffentlicht, in dem nicht nur auf die Risiken aufmerksam gemacht wird (siehe auch Tz. 7.3 zu WhatsApp), sondern vor allem praktische Tipps zu deren Vermeidung gegeben werden. Es ist abrufbar unter:

https://datenschutzzentrum.de/artikel/1137-1.html

Was ist zu tun?

Alle Helferinnen und Helfer sollten beim Einsatz elektronischer Kommunikationsmittel Risiken für die Betroffenen vermeiden.

4.5 Soziales

4.5.1 Die Dauerbrenner im Sozialleistungsbereich

Jobcenter, Sozial- und Jugendamt oder Wohngeldstelle – mangelnde Datenschutzkenntnisse führen immer wieder zu den gleichen Fragen und Beschwerden. Das ULD gibt die wichtigsten Antworten auf die häufigsten Fragen:

Anforderung von Kontoauszügen: Grundsätzlich darf nur die Vorlage von Kontoauszügen der letzten ein bis drei Monate angefordert werden. Antragsteller haben ein (begrenztes) Recht, Texte einzelner Sollbuchungen zu schwärzen. Über dieses Recht sind die Betroffenen zu informieren.

Anfertigung von Kopien (Kontoauszüge, Mietverträge, Personalausweis usw.): Unterlagen dürfen in Kopie nur dann auf Dauer zur Akte genommen werden, wenn dies für die Aufgabenerfüllung der Behörde zwingend erforderlich ist. Personalausweise, EC-Karten oder die Krankenversichertenkarte dürfen grundsätzlich nicht kopiert werden. Das ULD kann im Einzelfall prüfen, wenn Behörde und Betroffener unterschiedliche Auffassungen zur „Erforderlichkeit von Kopien“ haben.

Diskretion bei Gesprächen (am Empfang, bei offenen Bürotüren …): Jeder hat Anspruch darauf, seine Anliegen geschützt vor neugierigen Augen und Ohren vortragen zu können. Das ULD kann vor Ort beraten, aber auch Prüfungen durchführen.

Recht auf Akteneinsicht, Auskunft, Korrektur oder Löschung: Wer Sozialleistungen bezieht oder beantragt, darf grundsätzlich in seine Akte einsehen. Wird die Auskunft darüber, welche Daten zu welchem Zweck gespeichert sind, woher die Daten stammen und an wen diese Daten eventuell weitergegeben wurden, verweigert, kann sich jeder Betroffene an das ULD wenden. Sind Daten falsch, müssen diese berichtigt werden. Werden Daten nicht mehr benötigt, ist eine Löschung zu prüfen.

Kommunikation per E-Mail und die Nutzung sozialer Medien wie WhatsApp: Sozialdaten unterliegen dem Sozialgeheimnis. Die Behörden müssen sicherstellen, dass auch bei einem Datenaustausch Unbefugte keine Kenntnis von diesen Daten nehmen können. Besondere Vorsicht ist daher geboten, wenn Sozialdaten über E-Mail, Textnachricht oder Cloud-Dienste ausgetauscht werden (zu WhatsApp: Tz. 7.3). Wer sicher Daten übermitteln will, kann den Postweg nutzen oder fragt das ULD um Rat.

Datenaustausch zwischen Jobcenter und Maßnahmeträger: Wer einer Eingliederungsmaßnahme zustimmt, muss akzeptieren, dass sich Jobcenter und Maßnahmeträger untereinander austauschen. Dieser Informationsaustausch darf jedoch nicht grenzenlos erfolgen. Betroffene sollten stets über den Informationsaustausch unterrichtet werden.

Verlust von Unterlagen, unsichere Briefkästen: Wenn Bürgerinnen und Bürger Unterlagen einreichen, diese aber nicht beim Sachbearbeiter ankommen, muss sich die Behörde auf die Fehlersuche begeben. Ist z. B. der Briefkasten zu klein und nicht ausreichend gesichert?

Medizinische Daten und Unterlagen im Verwaltungsbereich: Angaben über die Gesundheit sind besonders sensibel. Medizinische Unterlagen wie Atteste und Arztbriefe oder Angaben über Diagnosen gehören daher grundsätzlich nicht in die Verwaltungsakten, sondern sind gesondert im amtsärztlichen Bereich zu verarbeiten.

Anrufe beim Vermieter, der Krankenkasse, den Stadtwerken …: Der Gesetzgeber fordert, dass Sozialdaten grundsätzlich beim Betroffenen zu erheben sind. Eine direkte Nachfrage bei Dritten darf ohne Wissen und Einwilligung des Betroffenen nur erfolgen, wenn eine Rechtsvorschrift dies erlaubt oder anordnet oder in begründeten Einzelfällen.

Veraltete, unverständliche Vordrucke und unwirksame Einwilligungserklärungen: Hier ist zu klären, ob die Vordrucke verständlich sind und der aktuellen Rechtslage entsprechen. Werden nur Daten abgefragt, die auch wirklich erforderlich sind? Hat der behördliche Datenschutzbeauftragte die Vordrucke überprüft?

Achtung! Einwilligungserklärungen können unwirksam sein, wenn diese keine ausreichenden Informationen über die sich austauschende Stellen, den Zweck sowie den Umfang der beabsichtigten Datenübermittlung und keinen Hinweis auf die Freiwilligkeit und die Möglichkeit des Widerrufes beinhalten. Das ULD hilft

Behörden bei der datenschutzgerechten Gestaltung ihrer Vordrucke.

Aufforderung zur Angabe der Telefonnummer: Die Angabe von Telefon-, Fax- und Handynummern, aber auch der E-Mail-Anschrift ist grundsätzlich freiwillig. Die Behörde muss diese Daten auf Verlangen löschen.

Fehlgeleitete Briefe und Faxe: Eine Namensverwechslung, zwei Briefe in einem Umschlag oder ein Tippfehler beim Faxen und schon erhält der falsche Empfänger Post von der Behörde. Die Folgen für die Betroffenen sind möglicherweise gravierend. Zwar können solche Fehler nie vollständig ausgeschlossen werden, doch die Mitarbeiterinnen und Mitarbeiter in den Behörden müssen an jedem Tag achtsam bleiben.

Informationspflicht bei einer Datenpanne: Wenn ein Datenschutzverstoß zur Folge hat, dass Unbefugte Kenntnis von sensiblen Sozialdaten erhalten, hat die Behörde unter Umständen die gesetzliche Pflicht, die Betroffenen und die Aufsichtsbehörden zu unterrichten.

Unter *www.datenschutzzentrum.de/uploads/blauereihe/blauereihe-alg2.pdf* hat das ULD eine umfassende Informationsbroschüre mit den häufigsten Fragen und den wichtigsten Antworten zum Datenschutz in der Sozialhilfe, Grundsicherung und beim Arbeitslosengeld II veröffentlicht.

Was ist zu tun?

Behörden müssen ihre Mitarbeiterinnen und Mitarbeiter regelmäßig schulen, damit auch im normalen Tagesgeschäft Datenschutzverstöße unterbleiben. Das ULD berät gerne Behörden sowie Bürgerinnen und Bürger, kann aber auch prüfend tätig werden.

4.5.2 Personaldaten der Jugendhilfe – das Online-Meldeportal des Landesjugendamts

Sind Jugendhilfeeinrichtungen verpflichtet, dem Landesjugendamt mitzuteilen, wenn Mitarbeiterinnen und Mitarbeiter entlassen oder eingestellt werden? Welche Personaldaten darf das Landesjugendamt über das Online-Portal „Schleswig-Holstein-Service – Heimaufsicht-Meldeservice“ erheben? Das ULD wurde um Prüfung und Beratung gebeten.

Das Landesjugendamt als Teil des Sozialministeriums ist die oberste Landesjugendbehörde in Schleswig-Holstein und zuständig für die Erteilung der Betriebserlaubnis für über 1.800 Einrichtungen der Jugendhilfe. Die Erteilung einer Erlaubnis für den Betrieb einer Jugendhilfeeinrichtung kann erfolgen, wenn u. a. die dem Zweck und der Konzeption der Einrichtung entsprechenden personellen Voraussetzungen erfüllt sind. Die Erlaubnis ist zurückzunehmen, wenn sich die Personalausstattung derart verändert, dass eine Kindeswohlgefährdung zu befürchten ist, weil die Betreuung der Kinder und Jugendlichen nicht oder nicht mehr ausreichend sichergestellt werden kann.

Betreiber von Jugendhilfeeinrichtungen sind daher gesetzlich verpflichtet, Änderungen in der Personalausstattung aktiv dem Landesjugendamt mitzuteilen. Das Landesjugendamt ist berechtigt, diese Personalmeldungen in einer Datenbank zu speichern.

Das Landesjugendamt darf Daten der Mitarbeiterinnen und Mitarbeiter der Einrichtungen jedoch nur in dem Umfang erheben und speichern, wie dies für die Aufgabenerfüllung erforderlich ist, also um z. B. prüfen zu können, ob eine Betriebserlaubnis zurückzunehmen ist. Mit Unterstützung des ULD hat das Landesjugendamt sowohl die Hinweise und die Vorlagen für die Anträge auf Erteilung einer Betriebserlaubnis als auch die Personalmeldebögen überprüft, angepasst und im Meldeportal neu hinterlegt. Beispielsweise wird zukünftig nicht mehr die private Anschrift der Mitarbeiterinnen und Mitarbeiter abgefragt. Zudem wurden bereits erhobene, aber nicht für diesen Zweck erforderliche Daten aus der Datenbank gelöscht.

Was ist zu tun?

Das Landesjugendamt ist berechtigt, die für seine Aufgabenerfüllung erforderlichen Personalmeldungen der Jugendhilfeeinrichtungen über ein Meldeportal zu erheben und in einer Datenbank zu speichern. Das Landesjugendamt muss sicherstellen, dass im Online-Meldeportal „Schleswig-Holstein-Service – Heimaufsicht-Meldeservice“ nur die für die Aufgabenerfüllung erforderlichen Daten erhoben werden.

4.6 Schutz des Patientengeheimnisses

4.6.1 Der neue Selbst-Check für Arztpraxen

Das ULD hat gemeinsam mit der Ärztekammer und der Zahnärztekammer Schleswig-Holstein einen neuen Datenschutz-Selbst-Check für Arzt- bzw. Zahnarztpraxen mit den wichtigsten Datenschutz-Kontrollfragen erarbeitet.

Bei der Verarbeitung von Patientendaten in einer Arzt- bzw. Zahnarztpraxis sind nicht nur die allgemeinen datenschutzrechtlichen Vorschriften, sondern zudem die besonderen Anforderungen der ärztlichen Schweigepflicht zu beachten. Die Anforderungen an den Schutz des Patientengeheimnisses sind hoch. Es gilt, viele mögliche Fehlerquellen zu bedenken. Nicht nur Ärzte bzw. Zahnärzte, sondern auch die Mitarbeiterinnen und Mitarbeiter in der Arztpraxis tragen die Verantwortung.

Basierend auf den Erfahrungen unserer jahrelangen Prüf- und Beratungstätigkeit wurde ein neuer Fragenkatalog erstellt und mit der Ärzte- und Zahnärztekammer Schleswig-Holstein abgestimmt. Gemeinsam wurden praxisnah und verständlich die wichtigsten Datenschutz-Kontrollfragen zu folgenden Themen zusammengetragen:

- Empfang/Anmeldung
- Wartebereich
- Behandlungsbereich
- Datenübermittlung
- Informationstechnik
- Praxisverwaltung
- Patientenrechte
- Outsourcing/Beauftragung von Dienstleistern
- Möglichkeiten einer Videoüberwachung von Patienten und Praxispersonal

Ärzte- und Zahnärztekammer Schleswig-Holstein waren von diesem neuen Selbst-Check für Arztpraxen so angetan, dass sie monatlich in ihren Kammermitteilungen über die Entwicklung dieses neuen Selbst-Checks für Arztpraxen berichteten. Selbstverständlich enthält der neue Selbst-Check für Arztpraxen auch Antworten, Hilfestellungen und weiterführende Informationen.

Der neue Datenschutz-Selbst-Check für Arztpraxen ist veröffentlicht unter:

https://datenschutzzentrum.de/artikel/1068-1.html

Was ist zu tun?

Arzt- und Zahnarztpraxen sollten den neuen Selbst-Check für Arztpraxen nutzen, um zu überprüfen, ob in ihrer Praxis das Patientengeheimnis geschützt wird. Bei Fragen können sich Ärzte und Zahnärzte an das ULD wenden.

4.6.2 Outsourcing in Kliniken und Arztpraxen – künftig auch ohne Einwilligung möglich

Ärzte müssen genauso wie Apotheker, Sozialpädagogen oder Rechtsanwälte ein besonderes Berufsgeheimnis beachten. Dieses Patientengeheimnis soll davor schützen, dass Unbefugte Kenntnis von Patientendaten erhalten. Es kann aber sinnvoll sein, dass sich eine Klinik oder Arztpraxis bei der Einrichtung, dem Betrieb oder der Wartung der Informationstechnik qualifizierter externer Unternehmen bedient. Ähnliches gilt für den Bereich der Aktenvernichtung oder -archivierung. Was ist in solchen Fällen zu beachten?

Bislang benötigen Kliniken und Arztpraxen in Schleswig-Holstein die Einwilligung der Patienten, wenn nicht auszuschließen ist, dass der Auftragnehmer Patientendaten zur Kenntnis nehmen könnte. Ärzte machten sich strafbar, wenn sie keine Schweigepflichtentbindungserklärung des Patienten einholten!

Doch dies wirft Probleme auf: Patienten berichteten uns immer wieder von nicht verständlichen Erklärungen, die sie kurz vor der Behandlung unterschreiben sollten. Kliniken verweigerten die Behandlung, wenn Patienten ihre Einwilligung nicht erteilten. Seit Jahren fordern die Datenschutzaufsichtsbehörden in Deutschland, dass die Beauftragung externer Dienstleister rechtssicher gestaltet wird.

Mit dem Entwurf eines Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen soll zukünftig die Beauftragung externer Dienstleister nicht mehr strafbar sein. Zugleich sieht dieser Gesetzentwurf Befugnisnormen für Rechtsanwälte, Patentanwälte und Notare vor. Was noch fehlt, sind gesetzliche Regelungen mit entsprechenden Offenbarungsbefugnissen für Berufsgeheimnisträger wie z. B. Ärzte, Apotheker, Kranken- und Altenpfleger, Sozialpädagogen und -arbeiter. Hier ist der Landesgesetzgeber gefordert, entsprechende Befugnisnormen zu schaffen. Sobald diese Normen geschaffen sind, muss in diesen Fällen die Einwilligung der Patienten endgültig nicht mehr eingeholt werden.

Aber Achtung: Auch wenn die Beauftragung von externen Dienstleistern zukünftig nicht mehr strafbar ist und auch wenn es zukünftig nicht mehr erforderlich sein wird, die Patienten vorab um ihre Einwilligung zu bitten, so bleibt es doch dabei, dass die Berufsgeheimnisträger weiterhin für den Schutz der sensiblen Daten verantwortlich bleiben und gewährleisten müssen, dass es nicht zu einem Missbrauch kommt. Dies geschieht über das Konstrukt der Auftragsdatenverarbeitung: Der Auftraggeber (Berufsgeheimnisträger) muss mit dem Auftragnehmer (Dienstleister) einen schriftlichen Vertrag schließen. In diesem Vertrag sind insbesondere Festlegungen zu treffen über:

- den Gegenstand und die Dauer des Vertrages,
- den Umfang, die Art und den Zweck der vorgesehenen Datenverarbeitung,
- die zu treffenden technischen und organisatorischen Maßnahmen,
- die Berichtigung, Löschung und Sperrung von Daten,
- die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
- die Kontrollrechte und Weisungsbefugnisse des Auftraggebers sowie
- die Rückgabe überlassener Datenträger.

Das ULD stellt unter www.datenschutzzentrum.de umfangreiche Informationen zur Verfügung und wird die datenschutzgerechte Gestaltung sogenannter Auftragsdatenverarbeitungsverhältnisse verstärkt prüfen.

Was ist zu tun?

Der Landesgesetzgeber ist gefordert, auch für Ärzte und weitere Berufsgruppen, die ein besonderes Berufsgeheimnis zu beachten haben, eine gesetzliche Offenbarungsbefugnis zu schaffen. Dabei gilt es, auch bei Einbindung von Dienstleistern das der Sensibilität der Daten angemessene Schutzniveau zu gewährleisten. Insbesondere sind Auftraggeber weiterhin verpflichtet, schriftliche Verträge mit ihren Auftragnehmern zu schließen. Das ULD berät gerne im Vorfeld und wird in diesem sensiblen Bereich verstärkt prüfen.

4.6.3 Speicherung von Patientendaten – bitte verschlüsseln!

Ein Fall aus der Praxis zeigt, warum auch digitale Sicherungskopien von Patientendaten grundsätzlich zu verschlüsseln sind und welche Folgen ein Diebstahl für Arztpraxen und Patienten haben kann.

Der Einbrecher kam um Mitternacht. Auch der Tresor der Gemeinschaftspraxis für Neurologie, Psychiatrie, Psychosomatik und Psychotherapie wurde aufgebrochen. Entwendet wurden Medikamente und die Datenträger der Datensicherung. Auf den Speichersticks waren Namen, Behandlungsdaten und Arztbriefe von weit über 40.000 Patientinnen und Patienten aus über 20 Jahren unverschlüsselt gespeichert.

Die Praxisinhaber konnten den Einbruch nicht verhindern, aber sie hätten sich darauf vorbereiten müssen. Nicht nur die digitalen Daten des laufenden Praxisbetriebs, sondern auch die digitalen Sicherungskopien müssen verschlüsselt gespeichert werden. Der Gesetzgeber fordert technische und organisatorische Maßnahmen, damit gewährleistet wird, dass personenbezogene Daten gegen zufällige Zerstörung bzw. Verlust und gegen einen Zugriff durch Unbefugte, also auch gegen Diebstahl, geschützt sind.

Die Kriminalpolizei ermittelte, aber die Datenträger blieben verschwunden. Es ist also nicht ausgeschlossen, dass irgendwann irgendwer die Patientendaten anschauen, auswerten oder weitergeben wird. Man mag sich nicht vorstellen, welche Folgen dies für die betroffenen Patientinnen und Patienten haben könnte.

Aber auch für die Arztpraxis hat diese Datenpanne gravierende Folgen. Der Gesetzgeber sieht vor, dass alle betroffenen Personen unverzüglich über den Vorfall unterrichtet werden und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen erhalten. In diesem Fall hätte die Praxis also über 40.000 Briefe verschicken müssen! Wenn Briefe einen unverhältnismäßigen Aufwand darstellen, tritt an ihre Stelle die Information der Öffentlichkeit. Dies kann durch Anzeigen geschehen, die mindestens eine halbe Seite umfassen und in mindestens zwei bundesweit erscheinenden Tageszeitungen abgedruckt sind, oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen geeignete Maßnahme. Wären die Patientendaten auf den Datenträgern doch nur verschlüsselt gespeichert worden!

Was ist zu tun?

Arztpraxen müssen auch ihre digitalen Sicherungskopien von Patientendaten verschlüsseln. Gelangen Patientendaten Dritten unrechtmäßig zur Kenntnis und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, müssen die Betroffenen und das ULD informiert werden.

4.7 Wissenschaft und Bildung

4.7.1 Planungen für eine einheitliche Schulverwaltungssoftware nehmen Fahrt auf

Im letzten Tätigkeitsbericht (35. TB, Tz. 4.7.2) hatte sich das ULD für die Beschaffung einer einheitlichen Software für die Verarbeitung der Schülerdaten in den Schulverwaltungen ausgesprochen. Das Bildungsministerium ist diesem Vorschlag mittlerweile nachgekommen. Dem inzwischen gebildeten Lenkungsausschuss ist das ULD beigetreten und unterstützt die Planungen aktiv. Da sich zwischenzeitlich auch der überwiegende Teil der Schulträger und viele Schulen sowie der Bildungsausschuss des Landtages für ein einheitliches IT-Verfahren ausgesprochen haben, besteht Anlass zur Hoffnung, dass diese Planungen zeitnah umgesetzt werden. Das ULD wird die Einführung intensiv begleiten, damit in dem IT-Verfahren auch die datenschutzrechtlichen Vorgaben umgesetzt werden.

4.7.2 Die digitale Schule – aber bitte mit eingebautem Datenschutz

Das Bildungsministerium setzt für den Unterricht verstärkt auf den Einsatz digitaler Medien unter Zuhilfenahme von z. B. Tablets, Notebooks und die Nutzung von sogenannten Cloud-Diensten.

Der Einsatz solcher digitalen Hilfsmittel führt jedoch auch zu einer Fülle von datenschutzrechtlichen Fragen. Diese hatten wir bereits in unserem letzten Tätigkeitsbericht (35. TB, Tz. 4.7.3 und 4.7.4) dargestellt.

In Kenntnis dessen hat das Bildungsministerium zusammen mit dem ULD die datenschutzrechtlichen Vorschriften für die Verarbeitung personenbezogener Daten von Schülerinnen, Schülern und Eltern überarbeitet. Ziel ist es, eindeutige Rahmenbedingungen zu schaffen, unter denen informationstechnische Geräte und Verfahren (z. B. Cloud-Dienste) genutzt werden können.

Verantwortlich für die Datenverarbeitung in den Schulen sind die Schulleiterinnen und Schulleiter. Dass diese zunehmend das ULD um Beratung ersuchen, lässt eine erhöhte Sensibilisierung für Datenschutzbelange erkennen. Offenbar wird den Schulleiterinnen und Schulleitern bewusst, dass der Einsatz von Informationstechnik im Unterricht nur erfolgreich sein kann, wenn eine strukturierte Herangehensweise bei der Einführung solcher IT-Verfahren verfolgt wird, die auch Datenschutzaspekte einschließt.

In Kooperation mit dem Bildungsministerium begleitet das ULD die Schulleiterinnen und Schulleiter durch Handlungsempfehlungen und konkrete Hinweise beim datenschutzkonformen Einsatz digitaler Anwendungen in der Schule. Angesichts der dynamischen Entwicklung ist es jedoch nicht möglich, allen Anfragen zu der Vielzahl digitaler Lernmedien und den damit im Zusammenhang stehenden IT-Verfahren nachzugehen und diese Verfahren im Detail zu untersuchen.

Das ULD hält es deshalb für dringend erforderlich, möglichst schnell eine eindeutige Leitlinie für den Einsatz digitaler Medien und die Nutzung von IT-Geräten und IT-Verfahren zu schaffen. Damit soll eine strukturierte Planung des Einsatzes digitaler Medien vor der Verwendung im Unterricht erreicht werden.

Die Leitlinie muss zumindest einen orientierenden Rahmen geben, welche digitalen Instrumente in der Schule für den Unterricht eingesetzt werden können. Sie sollte die Schulleiterinnen und Schulleiter in die Lage versetzen, Angebote von Anbietern von Software und IT-Verfahren anhand definierter Kriterien, etwa in Form einer Checkliste, zu prüfen.

Neben dem pädagogisch-didaktischen Wert der IT-Verfahren müssen im nächsten Schritt die Fragen zur Verarbeitung personenbezogener Daten untersucht werden. Dabei ist zu prüfen, ob und welche personenbezogenen Daten der Schülerinnen und Schüler unbedingt verarbeitet werden müssen. Häufig ist eine Nutzung anonym oder unter Pseudonym möglich. Weiterhin müssen eindeutige Festlegungen zur Nutzung und Verarbeitung der personenbezogenen Daten der Schülerinnen und Schüler getroffen werden.

Bereits im letzten Tätigkeitsbericht hatten wir das Bildungsministerium aufgefordert, verbindliche Rahmenbedingungen für den Einsatz von Lern- und Kommunikationsplattformen festzulegen (35. TB, Tz. 4.7.3). Leider sind solche Rahmenbedingungen bisher nicht geschaffen worden.

Was ist zu tun?

Das Bildungsministerium sollte dringend eine Leitlinie für den Einsatz digitaler Medien erstellen. Datenschutz gehört in die Praxis des Unterrichts, auch bei der Nutzung von Lernsoftware oder anderer Technik. Das ULD stellt seine Expertise dabei gerne zur Verfügung.

4.7.3 Aktuelle Messenger-Dienste – für die schulische Kommunikation tabu

Die Kommunikation der Schule mit ihren Schülerinnen, Schülern und Eltern fand bisher auf Wegen statt, die datenschutzrechtlich meist unbedenklich waren. Neben den klassischen analogen Hilfsmitteln für die Kommunikation (Briefpost, Elternbriefe, Mitteilungshefte, „Ranzenpost“ usw.) trat in den letzten Jahren vermehrt die E-Mail-Kommunikation. Nicht nur die Schulverwaltung kommuniziert hierüber, sondern auch die Lehrkräfte nutzen E-Mails für den Kontakt mit ihren Schülerinnen, Schülern und Eltern.

In den letzten zwei Jahren hat das ULD festgestellt, dass einige Lehrkräfte Messenger-Dienste – und hier meist den Dienst WhatsApp (Tz. 7.3) – für die Kommunikation mit ihren Schülerinnen und Schülern verwenden. Nach den Erkenntnissen des ULD geht es dabei nicht nur darum, kurz Termine oder Ähnliches abzusprechen. Es werden anscheinend auch Unterrichtsmaterialien und Hausaufgaben darüber verteilt.

Natürlich soll die Schule auch neue elektronische Kommunikationswege nutzen. Dies kann jedoch nur unter der Voraussetzung erfolgen, dass dies nicht zu einem Rechtsbruch führt.

Obwohl es sich bei Messenger-Diensten um Telekommunikationsdienste handelt, die bei einem Angebot in Deutschland dem hiesigen Recht unterfallen, werden die europäischen und die deutschen Regelungen von einigen Diensteanbietern nicht beachtet.

Viele Anbieter ermöglichen nicht einfach nur Telekommunikation, sondern werten diese Telekommunikationsvorgänge auch zur Nutzeranalyse aus. So werden u. a. Standortdaten und Daten darüber, wer mit wem wann kommuniziert, für Werbezwecke oder Ähnliches ausgewertet. Da mit der Nutzung dieser Dienste die Nutzungsbedingungen anerkannt werden müssen, die einen Ausschluss solcher Vorgänge nicht möglich machen, würde man die personenbezogenen Daten der Schülerinnen und Schüler und der Eltern im Rahmen der dienstlichen Kommunikation diesen Analysen preisgeben.

Ein weiterer Faktor darf dabei nicht unberücksichtigt bleiben: Die Nutzung eines Messenger-Dienstes erfordert immer ein informationstechnisches Gerät (in der Regel ein Smartphone), in dem die Telefonnummern der Kontaktpersonen (hier die Schülerinnen und Schüler) gespeichert sind. Da es sich um dienstliche Datenverarbeitung handelt, wären diese Smartphones nach der Schul-Datenschutzverordnung genehmigungspflichtig. Darüber hinaus ist zu bedenken, dass die dienstlichen Telefonnummern im Kontakttelefonbuch des Smartphones der Lehrkraft üblicherweise nicht getrennt von den privaten Telefonnummern gespeichert sind. Da bei der Nutzung von den meisten Messenger-Diensten, beispielsweise WhatsApp, stets eine automatische Synchronisierung der Telefonbuchdaten mit dem Server des Messenger-Dienstes erfolgt, können sowohl Telefonnummern von Schülerinnen und Schülern als auch von Dritten (insbesondere private Kontakte der Lehrkraft) dem Anbieter bekannt und ausgewertet werden. Es ist zu bedenken, dass die Lehrkräfte immer nur in dienstlicher Funktion mit ihren Schülerinnen und Schülern in Kontakt treten. Durch die Nutzung von Messenger-Diensten besteht die Gefahr, dass eine Grenzziehung zwischen dienstlich und privat allein durch die technischen Gegebenheiten nicht mehr möglich ist.

Ferner ist zu beachten, dass die dienstliche Kommunikation der Lehrkraft gegebenenfalls auch aktenrelevant werden muss, wenn es beispielsweise darum geht, ein Fehlverhalten von Schülerinnen und Schülern nachträglich zu dokumentieren und zu bewerten. Diese Dokumentation ist mit über Messenger-Dienste verschickte Botschaften nicht ohne Weiteres möglich.

Weitere Ausführungen des ULD zu diesem Thema:

https://datenschutzzentrum.de/artikel/1052-1.html

Was ist zu tun?

Schulverwaltung und Lehrkräfte dürfen nur datenschutzgerecht mit den Schülerinnen, Schülern und Eltern kommunizieren. Für Messenger-Kommunikation ist es nötig, dass datenschutzkonforme Lösungen entwickelt und bereitgestellt werden. Das Bildungsministerium sollte hierzu Festlegungen treffen.

4.7.4 Die digitale Fotowelt in der Schule wirft Fragen auf

Schon immer wurden in der Schule Fotos aufgenommen. Ereignisse wie die Einschulung, der Abschlussball, die Sportfeste oder sonstige schulische Veranstaltungen werden im Foto festgehalten. Nicht nur Familienangehörige, sondern auch Lehrkräfte fertigen Fotos dieser Ereignisse. Vor dem Einzug der Digitalfotografie und immer besserer Aufnahmemöglichkeiten von Smartphones standen die datenschutzrechtlichen und persönlichkeitsrechtlichen Fragestellungen nicht so sehr im Fokus.

Das ULD erreichen nun vermehrt Anfragen von Schulleiterinnen und Schulleitern zu diesem Themenbereich. Diese beobachten, wie z. B. Eltern bei schulischen Veranstaltungen wie Theateraufführungen Fotos und Videos vom Geschehen auf der Bühne machen. Dabei mögen die eigenen Kinder im Zentrum des Interesses stehen. Andere Schülerinnen und Schüler werden jedoch naturgemäß mit aufgenommen.

Was geschieht nun mit den Bildern und Aufzeichnungen? Da es heute möglich ist, alles sofort im Internet zu veröffentlichen, sorgen sich viele Schulleiterinnen und Schulleiter um die Persönlichkeitsrechte der Schülerinnen und Schüler. Eine erste datenschutzrechtliche Einschätzung des ULD finden Sie unter:

https://datenschutzzentrum.de/artikel/1089-1.html

Eine abschließende Antwort auf alle in solchen Konstellationen auftauchenden Fragestellungen wird es kaum geben können. Es würde den Schulleiterinnen und Schulleitern jedoch schon helfen, wenn das Bildungsministerium eine Handreichung entwickelte, die die häufigsten Konstellationen und mögliche Lösungsansätze aufzeigt. Das ULD ist natürlich gerne zur Mitarbeit hieran bereit.

4.7.5 Digitales Klassenbuch im Pilotversuch getestet

Bereits im 35. Tätigkeitsbericht (Tz. 4.7.4) hatten wir darüber berichtet, dass das Bildungsministerium die Einführung und Nutzung elektronischer Klassenbücher und Notizbücher für die Lehrkräfte in einem Pilotversuch, der vom ULD datenschutzrechtlich begleitet wurde, voranbringen möchte. Das ULD hat im Rahmen dieser Beratung zwei Verfahren zusammen mit dem Bildungsministerium datenschutzkonform ausgerichtet. Dabei war es hilfreich, dass die beiden von den Schulen ausgesuchten Anbieter der Verfahren bereit waren, die vom ULD aufgestellten datenschutzrechtlichen Anforderungen umzusetzen.

Mittlerweile werden diese Verfahren in mehreren Schulen verschiedener Schularten in weiteren Pilotversuchen erprobt. Mit dem Erkenntnisgewinn aus den Rückmeldungen der Pilotschulen werden die vom ULD und dem Bildungsministerium erstellten organisatorischen und technischen Verfahrensregeln weiterentwickelt.

Der in der Schul-Datenschutzverordnung festgelegte Genehmigungsvorbehalt des Bildungsministeriums für die Nutzung solcher digitalen Klassen- und Notizbücher kann sicherstellen, dass die Schulen nur datenschutzkonforme IT-Verfahren einsetzen.

4.7.6 Risiken: Lehrer-Apps ersetzen den klassischen Lehrerkalender

Immer mehr Lehrkräfte installieren auf ihren privaten Smartphones und Tablets Programme, mit denen sie ihre Unterrichtsplanung organisieren. Hiergegen ist aus datenschutzrechtlicher Sicht zunächst nichts einzuwenden. Jedoch werden in diesen sogenannten Lehrer-Apps auch die personenbezogenen Daten der Schülerinnen und Schüler wie z. B. die Namen, die Klassenzugehörigkeit und die Leistungen im Unterricht (Noten von Klassenarbeiten, mündliche Leistungen) bis hin zu Fehlzeiten gespeichert.

Aufgrund zahlreicher Anfragen von Lehrkräften und Schulleiterinnen und Schulleitern zur Zulässigkeit des Einsatzes solcher Lehrer-Apps und zu deren Sicherheit hat sich das ULD damit näher befasst.

Die datenschutzrechtliche Bewertung unter Berücksichtigung auch von schulrechtlichen Aspekten hat das ULD unter dem folgenden Link ausgeführt:

https://datenschutzzentrum.de/artikel/1053-1.html

Leider hat sich das Bildungsministerium bisher gegenüber den Schulen nicht geäußert, ob und unter welchen Bedingungen die Nutzung solcher Lehrer-Apps aus Sicht des Bildungsministeriums als zulässig erachtet wird.

4.8 Steuerverwaltung

4.8.1 Zusammenarbeit der Steuerverwaltungen der norddeutschen Länder

Die Steuerverwaltungen der Länder Schleswig-Holstein, Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen und Sachsen-Anhalt planen, künftig beim Betrieb von IT-Verfahren enger zusammenzuarbeiten. Im Wege einer länderübergreifenden gebündelten Verfahrensbetreuung (LGVB) soll für jeweils ein IT-Fachverfahren ein Land für alle anderen beteiligten Länder die Einführung und die Betreuung des laufenden Betriebs übernehmen. Hierdurch sollen personelle Ressourcen sowie das erforderliche Spezialwissen gebündelt werden.

Die Verfahrensbetreuung soll nach den Planungen der Finanzverwaltungen auch die Betreuung der Anwender umfassen. Verfahrensbetreuer sollen sich z. B. in die Bearbeitung von Steuerfällen einschalten und die Steuersachbearbeiter bei konkreten Problemen in der Nutzung des Fachverfahrens unterstützen und anleiten. Damit geht zwangsläufig eine Kenntnisnahme von Steuerdaten einher, die mit dem jeweiligen Fachverfahren verarbeitet werden. Da dies rechtlich als Offenbarung des Steuergeheimnisses anzusehen ist, bedarf es hierfür einer besonderen Erlaubnis. Diese kann sich aus einer gesetzlichen Regelung ergeben. Für die Einführung der länderübergreifenden Verfahrensbetreuung ist ein Staatsvertrag geplant. Das ULD hat empfohlen, dass die Datenverarbeitung, gerade im Hinblick auf Steuerdaten, durch das verfahrensbetreuende Land darin klar geregelt wird. Unter dieser Voraussetzung kann der Staatsvertrag als gesetzliche Grundlage für die Offenbarung von Steuerdaten angesehen werden.

Was ist zu tun?

Die länderübergreifende gebündelte Verfahrensbetreuung sollte durch einen Staatsvertrag geregelt werden. Darin sollten auch Regelungen über die Verarbeitung von Steuerdaten getroffen werden.

4.8.2 Immer Ärger mit der Zweitwohnungssteuer

Ob eine Zweitwohnungssteuer anfällt, hängt von der Art der Nutzung der Wohnung ab. Mit Formularen erheben die Kommunen die aus ihrer Sicht relevanten Daten bei den Eigentümern. Manche Frage gehen aber zu weit.

Zweitwohnungssteuer

Bei der Zweitwohnungssteuer handelt es sich um eine örtliche Aufwandsteuer, die die Kommunen erheben dürfen (§ 2 Abs. 1 i. V. m. § 3 Abs. 1 Kommunalabgabengesetz SH – KAG). Sie kann von den Gemeinden für das Innehaben einer Zweit- bzw. Nebenwohnung im Gemeindegebiet erhoben werden. Besteuert wird die in der Einkommensverwendung zum Ausdruck kommende wirtschaftliche Leistungsfähigkeit des Inhabers. Die Einzelheiten müssen in einer kommunalen Satzung festgelegt werden.

Im Berichtszeitraum hat das ULD vermehrt Eingaben im Zusammenhang mit der Datenerhebung bei der Festsetzung der Zweitwohnungssteuer erhalten. Viele Betroffene haben den Eindruck, dass die Kommunen zu viele Daten abfragen.

Die Zweitwohnungssteuerpflicht wird ausgelöst, wenn und soweit die Wohnung für den persönlichen Bedarf genutzt oder vorgehalten wird. Für Zeiten der kommerziellen Vermietung entsteht im Grundsatz keine Zweitwohnungssteuerpflicht. Nicht steuerpflichtig sind auch Zeiträume, in denen sich die Eigentümer nur kurz, z. B. zu Renovierungsarbeiten, in der Zweitwohnung aufhalten.

Zunächst gilt allerdings die Vermutung, dass jeder, der eine zweite Wohnung besitzt, diese für seine persönliche Lebensführung vorhält und damit steuerpflichtig ist. Die Eigentümer haben dann die Möglichkeit, diese Vermutung zu widerlegen, indem sie entsprechende Angaben machen und diese auch belegen.

Das ULD ist der Auffassung, dass es zulässig ist, wenn die Gemeinde regelmäßig Angaben zu den Namen der Mieter, der Dauer des Aufenthalts der Mieter und dem gezahlten Mietentgelt verlangt. Hierzu müssen in der Regel nicht die Mietverträge vorgelegt werden; eine Auflistung („Belegungsplan“) ist an dieser Stelle ein milderes Mittel.

Hält sich der Eigentümer beispielsweise zu Renovierungszwecken in der Wohnung auf, so ist dies zu belegen. Die Kommune darf vom Eigentümer fordern, die Renovierung durch entsprechende Mittel (Belege, Fotografien) nachzuweisen.

Zu weit geht es allerdings, wenn, wie auch geschehen, der Eigentümer aufgefordert wird, jedes einzelne Datum anzugeben, an dem er oder Freunde und Verwandte in der Wohnung genächtigt haben.

Weitere Information, auch dazu, ob die Eigentümer die Daten der Mieter an die Kommune weitergeben dürfen, finden sich auf der Webseite des ULD:

https://datenschutzzentrum.de/artikel/1120-1.html

Was ist zu tun?

Die Kommunen sollten sich bei der Erhebung der Zweitwohnungssteuer an die oben aufgestellten Grundsätze halten, die auch vom Verwaltungsgericht Schleswig bestätigt sind.

05

KERNPUNKTE

Prüfungen von Safe-Harbor-Datentransfer
Kundendatenschutz
Videoüberwachung in Urlaub und Freizeit

5 Datenschutz in der Wirtschaft

5.1 ULD prüft Datentransfer nach Safe-Harbor-Urteil

Nachdem der Gerichtshof der Europäischen Union (EuGH) in seinem Urteil vom 6. Oktober 2015 die Safe-Harbor-Entscheidung der Europäischen Kommission für unwirksam erklärt hatte (Tz. 11.1), leitete das ULD im März 2016 bei neun Unternehmen in Schleswig-Holstein Prüfverfahren ein. Bei der Übermittlung personenbezogener Daten an Handelspartner in den USA können sich europäische Unternehmen nach den Vorgaben des EuGH nicht auf die Safe-Harbor-Entscheidung berufen. Auf Basis dieser Entscheidung sollte den US-Unternehmen seit dem Jahr 2000 eine Selbstzertifizierung anhand festgelegter Kriterien (Informationspflicht, Wahlmöglichkeit, Weitergabe, Sicherheit, Datenintegrität, Auskunftsrecht, Durchsetzung) ermöglicht werden, um hierdurch den Nachweis für das Bestehen eines angemessenen Datenschutzniveaus zu erbringen. Ein angemessenes Datenschutzniveau im Drittland, in das personenbezogene Daten übermittelt werden sollen, bildet eine der Voraussetzungen dafür, dass ein entsprechender Datentransfer zulässig ist.

Die Angemessenheit des Datenschutzniveaus, das ein Drittland bietet, wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen Bedeutung haben. Insbesondere werden die Art der Daten, die Zweckbestimmung sowie die Dauer der geplanten Verarbeitung, die in dem Drittland geltenden allgemeinen und speziellen Rechtsvorschriften sowie die dort geltenden Standesregeln und Sicherheitsmaßnahmen berücksichtigt. Der EuGH wies in seiner Begründung zur Nichtigerklärung des Safe-Harbor-Beschlusses darauf hin, dass aus diesem Beschluss nicht deutlich wird, ob es in den USA staatliche Regeln gibt, die dazu dienen, etwaige Eingriffe in Grundrechte der Personen, deren Daten aus der EU in die USA übermittelt werden, zu begrenzen. Weiterhin wurde moniert, dass keine Feststellungen der Europäischen Kommission zum Bestehen eines wirksamen gerichtlichen Rechtsschutzes gegen derartige Eingriffe erkennbar sind. Ferner führte der EuGH aus, dass die Zuverlässigkeit eines Systems zur Durchführung von Selbstzertifizierungen voraussetzt, dass wirksame Überwachungs- und Kontrollmechanismen geschaffen werden.

Die eingeleiteten Verfahren dienen der Prüfung, ob laufende Datenübermittlungen in unzulässiger Weise noch auf die ungültige Safe-Harbor-Entscheidung gestützt werden. Die Artikel-29-Datenschutzgruppe, ein Gremium der Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten, hatte bereits in einer Stellungnahme vom 16. Oktober 2015 deutlich gemacht, dass nach dem 31. Januar 2016 aufsichtsbehördliche Prüfungen stattfinden können. Die Stellungnahme ist unter dem folgenden Link abrufbar:

http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

Acht der Prüfverfahren konnten ohne die Feststellung eines Verstoßes abgeschlossen werden, da keine Daten auf Basis der ungültigen Safe-Harbor-Entscheidung in die USA übermittelt werden. Bei einem der Verfahren dauern die Ermittlungen noch an.

Was ist zu tun?

Die europäischen Unternehmen dürfen sich bezüglich der Übermittlung personenbezogener Daten in die USA nicht mehr auf die Safe-Harbor-Entscheidung (2000/520/EG) berufen. Ein entsprechender Datentransfer wäre rechtswidrig. Die Unternehmen tragen die Verantwortung dafür, die datenschutzrechtlichen Vorgaben einzuhalten. Dies erfordert auch interne Überprüfungen.

5.2 Mindestlohngesetz und Datenschutz

Im Berichtszeitraum wurden an das ULD Fragen zur Einhaltung datenschutzrechtlicher Vorschriften im Zusammenhang mit der Erfüllung der Vorgaben nach dem Mindestlohngesetz (MiLoG) herangetragen. Nach § 20 MiLoG sind Arbeitgeber mit Sitz im In- oder Ausland verpflichtet, ihren im Inland beschäftigten Arbeitnehmerinnen und Arbeitnehmern ein Arbeitsentgelt mindestens in Höhe des Mindestlohns zu zahlen. Ordnungswidrig handelt derjenige Arbeitgeber, der Werk- oder Dienstleistungen in erheblichem Umfang ausführen lässt, indem er als Unternehmer einen anderen Unternehmer oder Nachunternehmer beauftragt, von dem er weiß oder fahrlässig nicht weiß, dass dieser entgegen dem MiLoG den Mindestlohn nicht erbringt. Hinzu tritt eine verschuldensunabhängige Haftung des Arbeitgebers als Generalunternehmer für Auftrag nehmende Unternehmen und weitere Nachunternehmer. Als weitere Sanktion droht dem Arbeitgeber im Fall eines Verstoßes seiner Auftragnehmer ein Ausschluss von der Vergabe öffentlicher Aufträge.

Zur Begrenzung des Haftungsrisikos wurden von den Datenschutzaufsichtsbehörden Vertragsstrafenregelungen und Bürgschaften vorgeschlagen, die der Generalunternehmer mit seinen Auftragnehmern vereinbaren könnte. Entsprechende Leitlinien wurden vom Bundesarbeitsgericht in einer Entscheidung zum Recht der Arbeitnehmerentsendung entwickelt (BAG, Beschluss vom 06.11.2002, Az.: 5 AZR 617/01). Weiterhin wird empfohlen, dass hinsichtlich der Beauftragung weiterer Subunternehmer ein Zustimmungsvorbehalt für den Generalunternehmer vereinbart wird. In Betracht kommt auch, sich von Forderungen Beschäftigter der Subunternehmer auf Zahlung des Mindestlohns freistellen zu lassen.

Wichtig ist aus datenschutzrechtlicher Sicht, dass der Generalunternehmer in diesem Kontext keine Befugnis hat, die Personalakten der Beschäftigten bei seinen Auftragnehmern einzusehen. Die Einsicht in die Personalakten bezieht sich auf ein höchstpersönliches Recht, das nach der Rechtsprechung des BAG nur vom Beschäftigten selbst wahrgenommen werden darf. Ebenso darf dem Generalunternehmer kein umfassender Zugriff auf die automatisierten Personalsysteme bei den Auftragnehmern gestattet werden. Die Datenschutzaufsichtsbehörden halten eine Übermittlung nicht anonymisierter Verdienstbescheinigungen für unzulässig, da auch Angaben zur Konfessionszugehörigkeit, zum Familienstand, zur Steuerklasse, zur Anzahl der Kinder, zum vollständigen Geburtsdatum und zur Privatanschrift enthalten sein können. Als Lösung bietet sich eine stichprobenartige Kontrolle geschwärzter Verdienstbescheinigungen an. Näheres ergibt sich aus dem Beschluss der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18./19. März 2015, der unter folgendem Link abrufbar ist:

www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/89DSK-MindestlohngesetzUndDatenschutz.pdf

Was ist zu tun?

Generalunternehmer sollten bestehende Möglichkeiten für eine vertragliche Haftungsbegrenzung ausschöpfen. Vor der Kontrolle von Verdienstbescheinigungen müssen Schwärzungen durch den Auftragnehmer erfolgen.

5.3 Keine juristischen Personen als betriebliche Datenschutzbeauftragte nach dem BDSG

In der Beratungspraxis des ULD wurde mehrfach die Frage gestellt, ob juristische Personen, wie etwa eine GmbH oder eine AG, als betriebliche Datenschutzbeauftragte bestellt werden dürfen, um so der Verpflichtung aus § 4f BDSG nachzukommen. Das ULD lehnt dies aus den folgenden Erwägungen ab. Zunächst besteht das gesetzliche Erfordernis, als bestellte Person die erforderliche Zuverlässigkeit und Fachkunde zu besitzen. Diese Anforderung bezieht sich im Kern auf natürliche Personen, da diese ihre erworbene Fachkunde etwa in

Form von Nachweisen zu einer abgeschlossenen Berufsausbildung und einer absolvierten Fortbildung erbringen können. In diesem Kontext ist zu bemerken, dass auch Personengesellschaften, wie die OHG oder die KG, nicht als betriebliche Datenschutzbeauftragte bestellt werden können. Letzterem wird teilweise entgegnet, dass nach den Vorschriften der Wirtschaftsprüferordnung offene Handelsgesellschaften und Kommanditgesellschaften als Wirtschaftsprüfungsgesellschaften anerkannt werden, wenn sie wegen ihrer Treuhandtätigkeit als Handelsgesellschaften in das Handelsregister eingetragen worden sind. Nach den Vorschriften des Handelsgesetzbuchs können Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften als Abschlussprüfer agieren. Damit hat der Gesetzgeber eine deutliche Aussage getroffen, die im BDSG für die betrieblichen Datenschutzbeauftragten gerade fehlt. Eine entsprechende Einsetzung von Personengesellschaften wurde im BDSG nicht normiert.

Andererseits legt der Wortlaut des § 4f BDSG nahe, dass nur eine Bestellung natürlicher Personen in Betracht kommt, denn auf solche beziehen sich die Aussagen zum Benachteiligungsverbot, zur Unterstellung des betrieblichen Datenschutzbeauftragten beim Leiter der nichtöffentlichen Stelle, zur entsprechenden Anwendung der Vorschrift zur Kündigung von Arbeitsverhältnissen (§ 626 BGB) bezüglich des Widerrufs der Bestellung, zur Übernahme von Fortbildungskosten zur Erhaltung der für die Aufgaben erforderlichen Fachkunde (§ 4f Abs. 3 BDSG) sowie zur Geltendmachung eines Zeugnisverweigerungsrechts (§ 4f Abs. 4a BDSG). Gerade die Geltendmachung eines Zeugnisverweigerungsrechts gilt speziell für natürliche Personen. Zeugen sollen bekanntlich vor einem Gewissenskonflikt bewahrt bleiben. Die Zeugnisverweigerung erfolgt wegen persönlicher Gründe, die bei einer natürlichen Person vorhanden sein können. Letzteres gilt etwa nach Maßgabe von § 383 Abs. 1 ZPO.

Was ist zu tun?

Für die Bestellung von betrieblichen Datenschutzbeauftragten (§ 4f BDSG) kommen nur natürliche Personen in Betracht.

5.4 Einwilligung per Unterschriften-Pad nicht wirksam

Im Frühjahr 2016 wandte sich eine Online-Publikation aus dem Bereich des Versicherungswesens mit einem Fragenkatalog an verschiedene Aufsichtsbehörden. Darin ging es um datenschutzrechtliche und allgemein vertragsrechtliche Fragen zu Abschlüssen von Verträgen mit digitaler Unterschrift auf Tablet-Computern oder Unterschriften-Pads. Insbesondere die Frage der Formgültigkeit einer auf einem Touchscreen gezeichneten Unterschrift war mit Hinblick auf das Schriftformerfordernis der Einwilligung ein Thema.

Unterschriften auf Touchscreens von Tablet-Computern und Unterschriften-Pads genügen nicht den Anforderungen der Schriftform einer datenschutzrechtlichen Einwilligung. Diese derzeitige Rechtslage wird sich jedoch durch die ab Mai 2018 geltende Datenschutz-Grundverordnung voraussichtlich ändern.

Ein Großteil der Aufsichtsbehörden entschloss sich, zu den Fragen in einer gemeinsamen Antwort Stellung zu nehmen. Das ULD übernahm dabei in seiner Rolle des Vorsitzes der Arbeitsgruppe Versicherungswirtschaft die Koordination der Rückmeldung.

Nach einhelliger Auffassung der beteiligten Aufsichtsbehörden erfüllt eine solche Unterschrift nicht die Anforderungen der Schriftform. Voraussetzung für die Schriftform ist im Datenschutzrecht wie auch im Zivilrecht im Allgemeinen, dass die Unterschrift in einer Weise geleistet wird, die zur dauerhaften Wiedergabe ebenjener Unterschrift geeignet ist, die tatsächlich geleistet wurde. Sofern die Unterschrift jedoch nicht dauerhaft in das Display des Tablet-Computers geritzt oder gekratzt würde, entspricht die bloße Digitalisierung einer Finger- oder Stiftbewegung nicht der Schriftform. Entsprechend erklärte Einwilligungen sind – wie alle Erklärungen, die der Schriftform unterliegen –

also formunwirksam. Dies wurde der anfragenden Online-Publikation mitgeteilt.

Mit Blick auf die ab Mai 2018 geltende Datenschutz-Grundverordnung gehen die Aufsichtsbehörden jedoch davon aus, dass sich diese Bewertung ändern könnte. Einwilligungen unterliegen in der Datenschutz-Grundverordnung nicht mehr in gleicher Strenge der Schriftform und können daher grundsätzlich auch in anderer Form erteilt werden, solange den übrigen Anforderungen an eine wirksame Einwilligung Genüge getan wird. Ob dies durch Handzeichnungen auf Touchscreens von Mobilgeräten möglich ist, wird derzeit sowohl auf deutscher wie auf europäischer Ebene diskutiert.

5.5 Einzelfälle aus der Praxis

5.5.1 Kundenkarten und Werbeeinwilligungen

Das ULD erhielt eine Beschwerde über ein Kundenkartensystem. In den zugehörigen Nutzungsbedingungen wurde eine Einwilligung zur Nutzung der Daten (gekaufte Waren, Ort und Zeit des Einkaufs, Warenwert und Ähnliches) auch zu Werbezwecken vorausgesetzt. Die dazu nötige Einwilligungserklärung sollte jedoch laut dem der Kundenkarte beiliegenden Schreiben durch Unterschrift auf der Kundenkarte und erstmalige Nutzung der Karte erfolgen.

Das ULD leitete daraufhin ein Aufsichtsverfahren ein, in dessen Rahmen klargestellt wurde, dass die Schriftform der Einwilligung eine hinreichend feste Verbindung zwischen geleisteter Unterschrift und Erklärungsinhalt voraussetzt. Die isolierte Unterschrift auf der Kundenkarte einerseits und der eigentliche Inhalt der Einwilligungserklärung auf dem beiliegenden Schreiben andererseits erfüllte diese feste Verbindung nicht. Stattdessen wäre es im Nachhinein kaum noch nachvollziehbar, welcher Datenverarbeitung Kundinnen und Kunden – etwa nach Änderung der AGB – mit ihrer Unterschrift ursprünglich tatsächlich zugestimmt haben.

Nachdem diese Rechtslage klargestellt wurde, argumentierte das verantwortliche Unternehmen sodann, dass ein Großteil der beabsichtigten Datenverarbeitung auch ohne Einwilligung allein aufgrund des Vertrags über die Nutzung der Kundenkarte zulässig sei. Das ULD trat dieser Sichtweise im Verfahren damit entgegen, dass ein Unternehmen, das sich einmal auf die Einwilligung und die damit einhergehenden Widerrufsrechte der Kundinnen und Kunden eingelassen hat, bei fehlerhafter Einholung der Einwilligung nicht ohne Weiteres auf die gesetzliche Rechtsgrundlage umschwenken könne. Das Verfahren endete mit einer Anpassung des Kundenkartensystems, ohne dass weitere aufsichtsrechtliche Maßnahmen nötig waren.

Das ULD rät jedem Unternehmen, bei der Gestaltung und Inbetriebnahme von Datenverarbeitungsverfahren nicht voreilig auf die Einwilligung als Rechtsgrundlage zu setzen, sondern die gesetzlichen Erlaubnistatbestände zunächst gründlich zu prüfen (siehe dazu auch 35. TB, Tz. 5.7.3). So lassen sich Probleme bei der Gestaltung formgültiger und inhaltlich konformer Einwilligungserklärungen vermeiden. Gleichzeitig ist der Rahmen des Zulässigen bei Zugrundelegung einer gesetzlichen Grundlage für alle Beteiligten rechtssicher, transparent und nachvollziehbar und wird nicht selten den Interessen der Kundinnen und Kunden sowie dem Unternehmen sogar eher gerecht als die Einholung einer Einwilligung.

5.5.2 Datenlecks in Online-Zugangssystemen

Im Verlauf des Jahres 2016 ging beim ULD eine Meldung über ein Datenleck in einem Online-Zugangssystem ein. Nach Änderungen der zugrunde liegenden Software sorgte für einige Stunden ein Softwarefehler dafür, dass Nutzerinnen und Nutzer einer Webseite in das Kundenkonto anderer Kundinnen und Kunden gelangten. Nachdem der Fehler bekannt wurde, informierte das Unternehmen unverzüglich das ULD gemäß § 42a BDSG, woraufhin gemeinsam mit dem Unternehmen eine Untersuchung der Ursachen erfolgte. Es stellte sich heraus, dass bei besonders hohen Zugriffszahlen ein bisher nicht erkannter Programmierfehler zu dem unberechtigten Zugang zu den Konten anderer Personen führte.

Das vom ULD eingeleitete Aufsichtsverfahren wurde nach mehrmonatiger Begleitung schließlich eingestellt, da das betroffene Unternehmen die Ursachen aufklären und beheben sowie durch Anpassung der Testverfahren zukünftig zusätzliche Absicherungen herbeiführen konnte.

Dem ULD ist bewusst, dass derartige Fehler in der Regel nicht mit absoluter Sicherheit ausgeschlossen werden können. Mit Blick auf die längst erfolgte Digitalisierung vieler Geschäftsfelder und die Verlagerung der Kundenkommunikation und -verwaltung in den Online-Bereich sind Vorfälle wie der geschilderte jedoch keine Seltenheit mehr und müssen aufseiten der verantwortlichen Unternehmen daher mit größter Priorität und auch Einsatz angemessener Ressourcen behandelt werden. Eingriffe in die Rechte Betroffener, Imageschaden, Vertrauensverlust bei Kundinnen und Kunden und letztlich auch wirtschaftliche Schäden für Unternehmen, die die technischen Herausforderungen von E-Commerce und Online-Kommunikation nicht ernst nehmen, können immens sein.

5.5.3 Personalausweiskopien – Identifizierungspflichten im Bankenbereich

Das ULD erreichte in den letzten Jahren eine Vielzahl an Eingaben, die sich gegen das Vorgehen von Banken oder Kreditinstituten wandten, bei Eröffnung von Konten oder anderen Kundenkontakten ohne nachvollziehbare Begründung Kopien von Ausweisdokumenten zu verlangen. Die Petentinnen und Petenten äußerten in vielen Fällen Unsicherheit über die Rechtmäßigkeit dieser Verlangen und baten um Beratung oder Einschreiten.

Das Kopieren und teilweise auch digitale Einscannen von Ausweisdokumenten ist nur in einigen wenigen Unternehmensbereichen ausnahmsweise rechtlich zulässig, wenn damit spezifische Identifizierungspflichten erfüllt werden. Zu diesen Bereichen gehört ohne Zweifel der Bereich des Kreditwesens. Aber auch obwohl das deutsche Geldwäschegesetz in einigen Fällen erlaubt, dass Kopien vom Personalausweis oder anderen Ausweisdokumenten angefertigt werden, darf dies nicht dazu führen, dass Kundinnen und Kunden auf Nachfrage nur mit allgemeinen Pauschalerklärungen abgefertigt werden.

Das deutsche Datenschutzrecht sieht vor, dass Betroffene darauf hinzuweisen sind, wenn Daten aufgrund einer Vorschrift erhoben werden müssen. Auf Verlangen sind die entsprechenden Vorschriften konkret zu benennen. Nur so können die Kundinnen und Kunden beurteilen, ob im jeweiligen Fall zu Recht Ausweisdokumente kopiert werden dürfen, und nur so wird das Unternehmen in die Lage versetzt, das eigene Handeln zu hinterfragen und gegebenenfalls auf Kompatibilität mit den rechtlichen Vorgaben zu überprüfen.

In gleicher Weise dürfen die Vorgaben des Kreditwesengesetzes und des Geldwäschegesetzes nicht dazu benutzt werden, um vollständige Kopien ohne Prüfung der Erforderlichkeit anzulegen. Identifizierungspflichten beziehen sich in aller Regel auf konkrete Merkmale wie Name oder Adresse der Kundinnen und Kunden, nicht jedoch auf andere Daten (z. B. Zugangsnummer, Seriennummer), die ebenfalls auf Ausweisdokumenten zu finden sind. Hier besteht das Recht der Kundinnen und Kunden, einzelne Bereiche der Ausweiskopie entsprechend zu schwärzen.

Die Nichtbeachtung dieser Vorgaben ist ein Verstoß, der sowohl bei Kundinnen und Kunden zu unnötigem Vertrauensverlust und Unmut führt als auch aufgrund der Vielzahl der Eingaben die knappen Ressourcen der Aufsichtsbehörden unnötig belastet.

Was ist zu tun?

Unternehmen aus dem Bereich des Kreditwesens sind zur Identifizierung ihrer Kundinnen und Kunden verpflichtet. Dazu dürfen auch Kopien von Ausweisdokumenten angefertigt werden, sofern sie sich auf das erforderliche Maß beschränken. Die Kundinnen und Kunden haben das Recht, dass nicht benötigte Daten geschwärzt werden. Pauschales und zu weit gehendes Vorgehen führt in großem Maß zur Verunsicherung.

5.5.4 Weitergabe der vollständigen IBAN an Zahlungsempfänger

Im Frühjahr 2015 kontrollierte das ULD die Praxis eines Kreditinstituts, das im Bereich des elektronischen SEPA-Zahlungsverkehrs den Zahlungsempfängern die vollständige IBAN des Zahlungsversenders anzeigte. Das verantwortliche Kreditinstitut verwies dabei auf die Vorgaben des Art. 248 EGBGB (Einführungsgesetz zum Bürgerlichen Gesetzbuche) sowie § 675r BGB (Bürgerliches Gesetzbuch), wonach die Übermittlung bestimmter Identifikationsnummern zulässig sei. Diese Vorgaben beziehen sich jedoch nur auf die Abwicklung des Zahlungsverkehrs zwischen den Kreditinstituten selbst, nicht hingegen auf eine Datenweitergabe an andere Kundinnen und Kunden. Bereits 2011 hatten sich die Aufsichtsbehörden einhellig auf diese Bewertung verständigt. Im Rahmen der Sitzung der Arbeitsgruppe Kreditwirtschaft im Jahr 2015 wurde diese Frage erneut mit den übrigen Aufsichtsbehörden diskutiert. Die in der Arbeitsgruppe Kreditwirtschaft vertretenen Behörden bleiben daraufhin bei ihrer Auffassung, dass aus Art. 248 EGBGB sowie § 675r BGB keine Rechtsgrundlage für die Weitergabe der IBAN an Kunden abgeleitet werden kann. Denkbar wäre stattdessen eine entsprechende Regelung in den allgemeinen Geschäftsbedingungen der Kreditinstitute, die ihrerseits aber nach geltendem Vertragsrecht auf Wirksamkeit überprüft werden müsste.

Aufgrund einer fehlenden gesetzlichen Rechtsgrundlage für die Weitergabe der Daten und mangels entsprechender Regelung in den AGB des Kreditinstituts musste das ULD das Vorgehen daher als rechtswidrig kritisieren. Das verantwortliche Kreditinstitut änderte seine Praxis sodann im Laufe des Aufsichtsverfahrens und stellte die Übermittlung der IBAN an Zahlungsempfänger ein, sodass das ULD das Verfahren ohne formelle Beanstandungen beendet hat.

Das ULD findet immer wieder Verfahren vor, die auf Vorschriften gestützt werden, die mangels Bestimmtheit oder Reichweite nicht die von den Unternehmen beabsichtigte Datenverarbeitung rechtfertigen. In derartigen Fällen müssen alternative Rechtsgrundlagen geprüft werden und die Datenverarbeitung ist gegebenenfalls anzupassen.

Was ist zu tun?

Unternehmen, deren Datenverarbeitung sich auf eine gesetzliche Grundlage stützt, sollten Ausmaß, Zweck und erfasste Daten genau prüfen, um sicherzustellen, dass die gewählte Rechtsgrundlage den geplanten Zweck legitimiert. Andernfalls darf die Datenverarbeitung nicht erfolgen.

5.5.5 Begehung von Mietwohnungen und Veröffentlichung von Fotos ohne Einwilligung

Immer wieder erreichen das ULD Eingaben von Mieterinnen und Mietern, die nach einer Kündigung ihres Mietvertrags im Internet Bilder des Inneren ihrer Wohnung finden. Vermieterinnen und Vermieter oder beauftragte Personen haben sich in diesen Fällen oft ohne Wissen und Einverständnis der Betroffenen Zutritt zur noch bewohnten Wohnung verschafft und Bilder angefertigt, um die Wohnungsanzeige online zu bewerben. Zwar ist der Wunsch, Mietobjekte möglichst schnell attraktiv im Internet zur Neuvermietung zu präsentieren, ein berechtigtes Interesse. Dies rechtfertigt aber nicht, die Wohnung ohne Wissen und Einverständnis der Mietparteien zu betreten und Aufnahmen von den privaten Lebensbedingungen zu machen.

Ähnlich urteilte auch das Amtsgericht Steinfurt im April 2014 (Urteil vom 10.04.2014 – 21 C 987/13) und entschied im dortigen Fall, dass der Vermieter keinen Anspruch auf Duldung der Fertigung von Fotos der an den Mieter vermieteten Innenräume habe. Das Recht auf Achtung der Persönlichkeitsrechte ging den durch Art. 14 des Grundgesetzes geschützten Interessen des Vermieters im entschiedenen Fall vor. Das Gericht stellte dabei richtigerweise fest, dass derartige Fotos intime Einblicke in die Lebensgewohnheiten, Hobbys und die Persönlichkeit der Mieterinnen und Mieter sowie deren Familienangehörigen und sonstigen Mitwohnenden zulassen. Demgegenüber sei das Verwertungsrecht des Vermieters in der Regel nicht unangemessen beeinträchtigt.

Was ist zu tun?

Bevor Fotos des Innenraums von Mietwohnungen angefertigt werden, müssen stets die mietenden Personen um Einwilligung gebeten werden. Ohne eine Einwilligung dürfen Fotos in der Regel erst nach Auszug der Mietpartei angefertigt und veröffentlicht werden.

5.5.6 Briefkastenaufbrüche bei Sparkassen

Im Herbst 2015 erreichten das ULD mehrere Meldungen über aufgebrochene Briefkästen von Sparkassen aus verschiedenen Teilen Schleswig-Holsteins. Unbekannte hatten offenbar systematisch außen gelegene Briefkästen aufgebrochen, um an die darin liegenden ausgefüllten Überweisungsträger der Sparkassenkundinnen und -kunden zu gelangen.

Das ULD weist darauf hin, dass eine den Anforderungen des deutschen Datenschutzrechts genügende Datenverarbeitung nicht nur rechtlichen, sondern auch technisch-organisatorischen Vorgaben genügen muss. Daher müssen technische und organisatorische Maßnahmen stets im Blick behalten werden. Abhängig von dem Schutzbedarf der verarbeiteten Daten sind unterschiedliche Maßnahmen erforderlich. Kann ein angemessenes Schutzniveau nicht hergestellt werden, ist im Einzelfall auch nicht auszuschließen, dass die Verarbeitung der Daten nicht weiter durchgeführt werden kann.

Im Fall der gemeldeten Briefkastenaufbrüche wurde durch die betroffenen Sparkassen dementsprechend geprüft, ob der Briefkasten verstärkt oder an anderen Orten – auch innerhalb der Filialräume – neu aufgestellt werden musste. Zusätzlich wurde in allen Fällen die anschließende Bearbeitung der Überweisungsträger im Umfeld der Vorfälle hinsichtlich Auffälligkeiten intensiviert. Die betroffenen Kundinnen und Kunden wurden in geeigneter Weise informiert.

Das ULD weist zudem darauf hin, dass die Meldepflicht des § 42a BDSG auch deshalb sinnvoll ist, weil wiederholte und gleichartige Vorfälle so bei den Aufsichtsbehörden erkannt werden können. Im Rahmen der Briefkastenaufbrüche konnte sich das ULD so dafür einsetzen, dass die betroffenen Filialen die auffällige Häufung von Vorfällen im Gesamtverband bekannt gaben.

Was ist zu tun?

Wo Post mit schutzwürdigen Daten in Briefkästen von Unternehmen eingeworfen wird, ist von den verantwortlichen Stellen zu prüfen, ob ein ausreichender Schutz dieser Informationen besteht. Gegebenenfalls müssen Maßnahmen getroffen werden, die einen ausreichenden Schutz gegen Aufbrechen oder Herausgreifen der Briefe bieten.

5.5.7 Weitergabe von Beschäftigtendaten im Rahmen eines Personalabbaukonzepts

Ein Arbeitgeber hat zum Nachweis der Sozialauswahl in der Anlage der von ihm versendeten Kündigungsschreiben eine Liste der zur Entlassung vorgesehenen Arbeitnehmer beigefügt. Auf dieser Liste waren neben dem Namen der Betroffenen u. a. deren Geburtsdatum, Familienstand und Staatsangehörigkeit vermerkt. Die Petentin, die zum Zeitpunkt der Übermittlung der Liste noch keine konkrete Kenntnis von der Kündigungsabsicht ihres Arbeitgebers hatte, deren Name und Daten aber auf der Liste aufgeführt waren, rügte die Übermittlung ihrer personenbezogenen Daten an die gekündigten Kollegen.

Der Arbeitgeber vertrat die Auffassung, dass er aufgrund der Vorgaben nach § 1 Abs. 3 Kündigungsschutzgesetz (KSchG) zum Nachweis der Sozialauswahl neben dem Namen auch die Qualifikation und die Sozialdaten der als vergleichbar angesehenen Mitarbeiter offenzulegen hatte. Er begründete dies damit, dass er im Falle eines arbeitsgerichtlichen Verfahrens diese Daten hätte ebenfalls offenlegen müssen. Daher habe man nicht nur eine Namensliste, sondern auch die Kriterien der Auswahl und deren Erfüllung übermittelt.

§ 1 Abs. 3 Satz 1 2. Hs. Kündigungsschutzgesetz

(3) […] auf Verlangen des Arbeitnehmers hat der Arbeitgeber dem Arbeitnehmer die Gründe anzugeben, die zu der getroffenen sozialen Auswahl geführt haben. […]

Werden Arbeitnehmer, denen gekündigt werden soll, gemäß § 1 Abs. 5 Satz 1 KSchG namentlich bezeichnet, erfasst diese Rechtsgrundlage lediglich die bloße Namensliste und keine Informationen, die darüber hinausgehen. Gemäß § 1 Abs. 3 Satz 1 2. Hs. KSchG hat der Arbeitgeber dem Arbeitnehmer seine Überlegungen zur Sozialauswahl nur auf Verlangen mitzuteilen. Erst dann muss der Arbeitgeber dem Arbeitnehmer die Gründe angeben, die ihn zu der getroffenen sozialen Auswahl geführt haben.

Als bereichsspezifische Norm zum Umgang mit personenbezogenen Daten geht die Regelung des § 1 Abs. 3 Satz 1 2. Hs. KSchG den allgemeinen Regelungen des Bundesdatenschutzgesetzes (BDSG) gemäß § 1 Abs. 3 Satz 1 BDSG zwar vor. Jedoch entbindet sie die verantwortliche Stelle nicht von dem Erfordernis einer gesetzlichen Erlaubnis für die Übermittlung der Daten gemäß § 4 Abs. 1 Satz 1 BDSG. Eine Übermittlung der Sozialdaten ist in § 1 Abs. 3 Satz 1 2. Hs. KSchG nicht ohne Verlangen eines Arbeitnehmers vorgesehen. Eine gesetzliche Erlaubnis zur Übermittlung ist daher nur unter dieser Bedingung gegeben.

Die unaufgeforderte Übermittlung einer Liste mit den Namen der zur Entlassung vorgesehenen Arbeitnehmer, deren Wohnort, Geschlecht, Staatsangehörigkeit, Familienstand, Anzahl der Kinder, Geburtsdatum, Alter, Anstellungsstatus, Schwerbehinderung, Vertragsbeginn und Beruf erfolgte daher ohne Rechtsgrundlage. Das ULD hat in diesem Fall einen Verstoß durch Übermittlung personenbezogener Daten ohne vorheriges Verlangen festgestellt.

5.5.8 Umgang mit privaten Daten beim Ausscheiden aus dem Unternehmen

Das ULD erhielt im Berichtszeitraum Anfragen zum Umgang mit privaten Daten Beschäftigter, wenn diese das Unternehmen verlassen haben. Im vorgelegten Fall bestand in einem Unternehmen eine Betriebsvereinbarung, die das Ablegen von privaten Daten auf Dienstrechnern erlaubte. Daraus ergab sich die Frage, wie im Kündigungsfall des Beschäftigten mit dessen privaten Daten zu verfahren ist.

Entscheidet sich ein Unternehmen, die private Nutzung von Dienstgeräten zuzulassen, sollte in einer Betriebsvereinbarung geregelt werden, dass private Daten als solche zu kennzeichnen und besser noch in einem gesonderten Bereich abzulegen sind.

Bei einer Speicherung der privaten Daten in einer gesonderten oder gekennzeichneten Ablage ist eine Einsichtnahme durch das Unternehmen grundsätzlich nicht zulässig, da diese Daten für die Beendigung des Beschäftigungsverhältnisses nicht erforderlich sind. Die gekennzeichneten Daten müssen dem Beschäftigten zugeleitet werden. Soweit die Zuordnung einzelner Dateien unklar ist, kann schrittweise eine Einsichtnahme durch die Personalabteilung in Beisein des Betriebsrats, des Datenschutzbeauftragten und bestenfalls auch des Beschäftigten erfolgen. Die Erforderlichkeit der Einsichtnahme ist für jede Datei gesondert zu prüfen.

Grundsätzlich ist die Ablage privater, persönlicher Daten auf einem Dienstrechner aber immer problematisch und zu vermeiden. Das ULD rät anderenfalls zu einer technischen Containerlösung mit einem verschlüsselten Datenbereich in speziellen Verzeichnissen oder zu einer Verschlüsselung der einzelnen Dateien, wenn eine Erlaubnis zur Speicherung privater Informationen auf dem Dienstrechner erteilt wird.

Was ist zu tun?

Erlaubt der Arbeitgeber den Beschäftigten die Speicherung privater Daten auf dienstlichen Betriebsmitteln, so sollten die Daten als „privat“ gekennzeichnet sein und verschlüsselt werden.

5.6 Videoüberwachung

5.6.1 Urlaubsland Schleswig-Holstein – Einsatz von Webcams

Das Übertragen von bewegten Bildern im Internet mithilfe von Webcams erfreut sich steigender Beliebtheit. Die Qualität der eingesetzten Kameras hat sich kontinuierlich verbessert, und geringe Kosten sorgen für einen verstärkten Einsatz – sowohl im gewerblichen als auch im privaten Umfeld.

Webcams bieten eine komfortable Möglichkeit, sich über das Wetter und andere örtliche Begebenheiten zu informieren. Problematisch wird ihr Einsatz im öffentlichen Raum, wenn Personen auf den Bildern identifiziert werden können. Immer wieder wenden sich besorgte Bürger an das ULD, weil sie befürchten, dass jedermann sie z. B. im Urlaub, am Strand, in der Schwimmhalle, im Restaurant oder beim Shoppen beobachten kann. Immer häufiger handelt es sich um hochaufgelöste, fließende Bilder. Durch die Übertragung ins Internet steht es praktisch jedem offen, diese Aufnahmen aufzuzeichnen oder auszuwerten.

Können Personen auf den Bildern identifiziert werden, bedarf es sowohl für die Erhebung als auch für die Veröffentlichung der Bilder einer Rechtsgrundlage. Für die Erhebung sind in der Regel die Voraussetzungen des § 6b Bundesdatenschutzgesetz (BDSG) einzuhalten. Die Veröffentlichung im Internet kommt nur mit Einwilligung der Betroffenen oder bei Vorliegen der gesetzlichen Voraussetzungen des § 23 Kunsturhebergesetz (KunstUrhG) in Betracht.

Die Identifizierbarkeit einer Person ist grundsätzlich dann gegeben, wenn deren Gesicht auf

den Aufnahmen erkennbar wird. Allerdings können auch zusätzliche Kriterien zu einer Bestimmbarkeit führen. Dies gilt vor allem für das sonstige Körperbild einer Person, wie die Körperhaltung, die Kleidung, die mitgeführten Gegenstände oder Fahrzeuge. Darüber hinaus sind auch Zeitpunkt und Ort der Aufnahme geeignet, um Rückschlüsse auf eine Person ziehen zu können. Eine Identifizierung muss zumindest mit weiteren Hilfsmitteln mit noch verhältnismäßigem Aufwand möglich sein. Nicht notwendig ist, dass ein Abgebildeter tatsächlich von bestimmten Personen erkannt wurde. Das Recht am eigenen Bild ist bereits dann verletzt, wenn der Abgebildete begründeten Anlass zu der Annahme hat, er könne identifiziert werden. Nicht erforderlich ist, dass schon der flüchtige Betrachter den Abgebildeten auf dem Bild erkennen kann; es genügt die Erkennbarkeit durch einen mehr oder minder großen Bekanntenkreis.

Werden Personen identifizierbar abgebildet, so ist in der Regel bereits die Erhebung der Daten nach dem BDSG unzulässig. Das BDSG setzt voraus, dass die verantwortliche Stelle ein berechtigtes Interesse an der Erhebung der personenbezogenen Daten hat. Dies fehlt in der Regel beim Betrieb einer Webcam. Zwar dient der Betrieb der Webcam meist einem berechtigten Interesse der verantwortlichen Stelle, z. B. der Werbung oder Kundenbindung. Die Erhebung und Veröffentlichung personenbezogener Daten ist für den jeweiligen Zweck in der Regel jedoch nicht erforderlich. Der Veröffentlichung stehen des Weiteren zumeist auch die berechtigten Interessen der Betroffenen entgegen, sodass nach dem KunstUrhG eine Veröffentlichung nicht zulässig ist.

Der rechtssichere Betrieb einer Webcam im öffentlichen Raum ist daher nur möglich, wenn sichergestellt ist, dass Personen nicht ohne Weiteres identifiziert werden können.

Was ist zu tun?

Webcam-Betreiber sollten den Bildausschnitt, die Auflösung, den Zoom und die Bildwiederholrate so wählen, dass Personen nicht identifizierbar sind.

5.6.2 Wolfsmonitoring mit Wildkameras

Bereits der 35. Tätigkeitsbericht (35. TB, Tz. 5.6.1) befasste sich mit der Frage, inwieweit Jagdausübungsberechtigte zur Unterstützung ihrer Tätigkeit auf sogenannte Wildkameras zurückgreifen dürfen. Der Einsatz solcher Kameras in öffentlich zugänglichen Räumen ist nur unter Einhaltung strenger Voraussetzungen möglich.

Einen besonderen Fall der systematischen Beobachtung von Wildtieren in Schleswig-Holstein stellt das sogenannte Wolfsmonitoring dar. Im Auftrag des Ministeriums für Energiewende, Landwirtschaft, Umwelt und ländliche Räume (MELUR) untersuchen Fachleute die Rückkehr des Wolfes und die damit verbundenen Auswirkungen. In diesem Zusammenhang werden auch Wildkameras eingesetzt, um mehr über die Anzahl, das Verhalten und die Verbreitung der Tiere zu erfahren. Zur Entwicklung von Lösungen für ein Wolfsmonitoring, das einen unverhältnismäßigen Eingriff in die Rechte der Bürgerinnen und Bürger vermeidet, wurde das ULD von den Verantwortlichen schon frühzeitig eingebunden.

Im Ergebnis wurde durch verschiedene Maßnahmen sichergestellt, dass ungewollte Eingriffe in die Persönlichkeitsrechte auf ein Minimum reduziert werden. U. a. wurden die mit der Aufstellung und Auswertung der Wildkameras beauftragten Wolfsbetreuer im Rahmen einer Schulung in Bezug auf die datenschutzrechtlichen Anforderungen besonders sensibilisiert.

Das Vorhaben zeichnet sich insbesondere durch seine Transparenz aus. Über die Webseite http://www.wildkamera-sh.de/ kann sich jeder über den Zweck der Wildkameras sowie die getroffenen Maßnahmen zum Datenschutz informieren. Auf den Kameras sowie auf Schildern in der unmittelbaren Umgebung wird auf die Beobachtung und die verantwortliche Stelle aufmerksam gemacht. Auf der Webseite ist darüber hinaus der Standort aller Kameras verzeichnet. Für Betroffene und Interessierte stehen persönliche Ansprechpartner zur Verfügung. Seit dem Start des Projekts im März 2016 hat es weder bei den Verantwortlichen noch beim ULD Datenschutzbeschwerden gegeben.

5.6.3 Videoüberwachung im Fitnessstudio

Im letzten Tätigkeitsbericht hat das ULD über die Videoüberwachung in einer Fitnessstudiokette berichtet (35. TB, Tz. 5.6.2). Da der Betreiber nicht freiwillig bereit war, auf die Videoüberwachung von Umkleidebereichen, Trainingsflächen und Aufenthaltsbereichen zu verzichten, hat das ULD die Deaktivierung der auf diese Bereiche ausgerichteten Videokameras angeordnet. In diesen Bereichen überwiegen die schutzwürdigen Interessen der Kundinnen und Kunden, die Umkleideräume zu nutzen, an den Geräten zu trainieren oder im Aufenthaltsbereich zu verweilen, ohne dass dies aufgezeichnet und für mehrere Tage gespeichert wird.

5.6.4 Videoüberwachung in Schwimmbädern

Aufgrund verschiedener Eingaben hat sich das ULD mit der Videoüberwachung in einigen Schwimmbädern befasst. Videoüberwachung wird in Schwimmbädern häufig eingesetzt, um Sachbeschädigungen zu verhindern oder aufzuklären, aber auch um die Sicherheit der Badegäste zu gewährleisten.

Jedoch ist der Eingriff in die Persönlichkeitsrechte Betroffener in Schwimmhallen besonders groß, da die Besucher häufig nur leicht bekleidet sind und dort ihre Freizeit verbringen. Bei der Videoüberwachung in Schwimmbädern müssen daher die Erforderlichkeit und Verhältnismäßigkeit jeder einzelnen Kameraeinstellung gut begründet werden. Dies ist besonders schwierig, wenn sogenannte Dome-Kameras zum Einsatz kommen, deren Blickwinkel und Zoom verändert werden können und deren Blickrichtung für Besucher in der Regel nicht erkennbar ist.

Neben der Frage, ob ein Bereich überhaupt mit einer Kamera beobachtet werden sollte, muss man sich auch damit auseinandersetzen, ob eine Aufzeichnung der Bilder erforderlich ist. Um für die Badeaufsicht die Einsicht in besonders gefährliche Bereiche zu verbessern und ihr ein Eingreifen in Gefahrensituationen zu ermöglichen, reicht in der Regel eine Livebeobachtung aus. Die Gefährlichkeit eines bestimmten Bereiches muss sich dabei aufgrund objektiver Anhaltspunkte ergeben, beispielsweise weil es bereits konkrete Vorfälle gegeben hat oder Erfahrungswerte für eine erhöhte Gefährlichkeit (wie z. B. bei Sprungtürmen, Rutschen, Kinderbecken) sprechen. Nicht ausreichend ist die allgemein erhöhte Unfallgefahr wegen des Aufenthalts im Wasser. Der Einsatz von Videoüberwachungstechnik kann kein Ersatz für Aufsicht durch Personal sein!

Eine Videoaufzeichnung ausschließlich zum Ausschluss des Haftungsrisikos gegenüber Ansprüchen von Badegästen ist aufgrund der überwiegenden schutzwürdigen Interessen der von der Videoüberwachung Betroffenen unzulässig. Sie ist auch nicht erforderlich, da in solchen Fällen der Geschädigte in der Beweispflicht ist.

In textilfreien Bereichen, wie z. B. Saunen, haben Kameras grundsätzlich nichts zu suchen. Besonderes Augenmaß ist auch in Umkleidebereichen erforderlich. Hier erfolgt häufig eine Videoüberwachung mit der Begründung, dass ein Aufbrechen von Spinden verhindert oder aufgeklärt werden soll. Allerdings sind die Betroffenen oft nur leicht oder gar nicht bekleidet. Eine Überwachung von Spinden kann nur dann zulässig sein, wenn damit nicht gleichzeitig Bänke oder Ablageflächen erfasst werden, die zum Umkleiden genutzt werden. Ist eine isolierte Überwachung der Spinde zulässig, liegt die Herausforderung häufig darin, den Aufnahmewinkel so zu wählen, dass die Spinde vom Bild erfasst werden, aber niemand beim Umkleiden gefilmt wird.

Die Betroffenen müssen über die Videoüberwachung informiert werden. Doch nicht immer ist es leicht, den videoüberwachten Bereich transparent zu machen. Nach Möglichkeit sollten außerdem überwachungsfreie Bereiche angeboten werden, damit Betroffene der Überwachung ausweichen können. Bei der Entscheidung bezüglich einer Videoüberwachung und ihrer Ausgestaltung helfen die Orientierungshilfe „Videoüberwachung durch nichtöffentliche Stellen“ sowie der Zusatz „Videoüberwachung in Schwimmbädern“. Beide Dokumente stehen auf der Webseite des ULD zum Download zur Verfügung:

https://www.datenschutzzentrum.de/uploads/video/Orientierungshilfe_Videoueberwachung.pdf

https://datenschutzzentrum.de/uploads/video/2015-Duesseldorfer-Kreis-Videoueberwachung_in_Schwimmbaedern.pdf

Was ist zu tun?

Bei der Videoüberwachung ist stets die Erforderlichkeit zu hinterfragen. Jede Kameraeinstellung muss sorgfältig geprüft werden.

5.6.5 Videoüberwachung auf Toiletten

Das ULD hat sich wiederholt mit der Videoüberwachung in Toilettenräumen beschäftigt. Die Überwachung bezog sich auf die Waschbecken oder den Toilettenraum, ohne dass in den einzelnen Kabinen gefilmt wurde.

Häufig sind es Diskotheken oder Bildungseinrichtungen, die in diesen Bereichen regelmäßig mit Vandalismus und groben Verschmutzungen zu kämpfen haben. Die Schäden sind nicht unerheblich, und oft gehen sie zulasten derer, die die Räume ordnungsgemäß nutzen möchten. Das Interesse daran, die Sanitäranlagen in gutem Zustand zu halten, ist absolut nachvollziehbar. Allerdings ist die Videoüberwachung dafür kein zugelassenes Mittel.

Bei jeder Videoüberwachung muss zwischen den zu schützenden Gütern und dem Eingriff in das Persönlichkeitsrecht der Betroffenen abgewogen werden. Die Eingriffsintensität ist dabei abhängig von der Art der erfassten Informationen (Informationsgehalt), dem Umfang (Informationsdichte, zeitliches und räumliches Ausmaß), dem betroffenen Personenkreis, der Interessenlage der betroffenen Personengruppen, dem Vorhandensein von Ausweichmöglichkeiten sowie von Art und Umfang der Verwertung der erhobenen Daten.

In Situationen, in denen Menschen privat Zeit mit Freunden verbringen, wie z. B. in einem Restaurant, überwiegt deshalb in der Regel das Persönlichkeitsrecht der Betroffenen, sodass eine Beobachtung mittels Videokamera unzulässig ist.

Videoüberwachung in Toilettenräumen ist aber noch viel eingriffsintensiver. Bereits der Umstand des Aufsuchens einer Toilette, die Verweildauer sowie übliche Verhaltensweisen, wie z. B. das Waschen, das Richten der Frisur oder der Kleidung oder das Reinigen der Zähne, sind dem Bereich der Intimsphäre eines Menschen zuzuordnen. Aus diesem Grund ist die Videoüberwachung von Toilettenräumen in jedem Fall unzulässig.

06

KERNPUNKTE

Standard-Datenschutzmodell
Datenschutz-Folgenabschätzung
Vorabkontrollen

6 Systemdatenschutz

6.1 Zusammenarbeit für IT-Sicherheit und technischen Datenschutz

IT-Sicherheit und technischer Datenschutz gehören in die Infrastrukturen für Informationstechnik. Um diese zu erreichen, ist eine regelmäßige Koordinierung der unterschiedlichen Akteure im Land notwendig.

Die Informationstechnik (IT) der Landesregierung wird durch die Abteilung „Zentrales IT Management“ (ZIT) der Staatskanzlei unter Leitung des Chief Information Officer (CIO) organisiert. Neben den Ministerien und nachgeordneten Behörden des Landes nutzen weitere Institutionen wie die Landtagsverwaltung und der Landesrechnungshof Teile der technischen Infrastruktur der Landesregierung. Beispiele sind der Standard der Bürokommunikation (genannt „+1“), das Landesnetz oder die Systeme für die eAkte. Auch der kommunale Bereich kann Verfahren oder Systeme des Landes nutzen, etwa den zentralen De-Mail-Zugang.

Diese Tätigkeiten sollen in verschiedenen Gremien mit teils operativem, teils strategischem Charakter koordiniert werden: im Landes-IT-Rat, in der IT-Beauftragten-Konferenz und im Integrierten Sicherheitsmanagement.

Das Spiegelgremium des (Bundes-)IT-Planungsrats, in dem Bund und Länder die bundesweite IT-Planung vorantreiben, ist in Schleswig-Holstein der **Landes-IT-Rat**. Neben den Vertretern Schleswig-Holsteins im IT-Planungsrat (CIO und Staatskanzlei) sind Landesinstitutionen (u. a. Ressorts, Landtag, Landesrechnungshof) und KOMFIT (Kommunales Forum für Informationstechnik e. V.) als Vertretung der Kommunen beteiligt. Hier war in der Vergangenheit das ULD eingebunden und wird auch derzeit mit Informationen versorgt.

Die **IT-Beauftragten-Konferenz (ITBK)** ist die regelmäßige Besprechung der Abteilung ZIT mit den IT-Leitungen der Ressorts und einigen nachgeordneten Behörden und finden nach ursprünglich monatlichem Rhythmus mittlerweile je nach Bedarf in mehrmonatigem Abstand statt.

Für das Thema „IT-Sicherheit“ gibt es ein eigenes Gremium, das als **Integriertes Sicherheitsmanagementsystem (ISMS)** die Tätigkeit des IT-Sicherheitsbeauftragten des Landes (angesiedelt im ZIT) und der IT-Sicherheitsbeauftragten der Ressorts und einiger nachgeordneter Behörden koordiniert. Vertreten ist auch der kommunale Bereich durch das KOMFIT sowie Dataport. Im Gegensatz zu den Treffen der ITBK und des Landes-IT-Rats tritt dieses Gremium in gewohnter Regelmäßigkeit in zweimonatlichen Arbeitstreffen zusammen.

Ein regelmäßiger Tagesordnungspunkt ist der Bericht des CERT Nord („Computer Emergency Response Team“), das im Auftrag der Länder Schleswig-Holstein, Bremen, Hamburg und Sachsen-Anhalt bei Dataport gebildet wurde. Seine Aufgabe ist die Beobachtung und Abwehr von Angriffen auf die IT-Sicherheit. Dazu werden Softwareschwachstellen und Angriffe auf fremde IT-Infrastrukturen analysiert (beispielsweise anhand von Publikationen, aber auch in Zusammenarbeit mit anderen CERTs auf Landes- und Bundesebene sowie dem BSI). Auch die Beobachtung und Abwehr von konkreten Angriffen auf die von Dataport bereitgestellte IT-Infrastruktur gehört zu den Aufgaben des CERT. Hilfreich ist hier die Gesamtschau auf die verschiedenen Bundesländer, denn je nach Konfigurationsvorgaben sind Angriffe in einigen Bundesländern erfolgreich, während sie in anderen Ländern durch eine geeignete Konfiguration unterbunden werden. Hier besteht die Chance, voneinander lernen und erfolgreiche Verteidigungsstrategien kopieren zu können. Daher ist eine weitere Aufgabe des CERT, Warnungen und Gegenmaßnahmen zu publizieren, die zielgerichtet auf Hardware, Software und Konfiguration der öffentlichen Verwaltung zugeschnitten sind. Dies richtet sich zunächst an die Landes-IT, ist aber auch hilfreich für andere öffentliche Bereiche wie Kommunen oder kommunale Dienstleister.

Im Projekt SiKoSH (Sicherheit für Kommunen in Schleswig-Holstein) des KOMFIT werden Hilfsmittel erarbeitet, um IT-Sicherheit im kommunalen Bereich auch mit geringen Ressourcen ausreichend gewährleisten zu können. Ziel ist es, durch die Bereitstellung von anpassbaren Musterdokumenten wie Leitlinien, Rahmenkonzepten, spezifischen Richtlinien und anderen Hilfsmitteln den Aufwand für die Erarbeitung dieser Dokumente zu verkürzen und gleichzeitig praxistaugliche Anforderungen zu formulieren, die dann umzusetzen sind.

Was ist zu tun?

IT-Sicherheit und technischer Datenschutz, wie dies im Land notwendig ist, erfordern ein Handeln mit vereinten Kräften. Die Zusammenarbeit im ISMS und seine Schlagkraft sind zu verbessern. Eine frühzeitige Information und Einbindung des ULD als beratendes Mitglied ist sinnvoll.

6.2 Länderübergreifende Zusammenarbeit der Datenschutzbeauftragten

Die Zusammenarbeit der Datenschutzbeauftragten zu technisch-organisatorischen Fragen erfolgt insbesondere über den Arbeitskreis Technik, der auch allen Facharbeitskreisen und -arbeitsgruppen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) durch die Bewertung technisch-organisatorischer Fragen zuarbeitet. Daneben gibt es regionale und Ad-hoc-Kooperationen sowie eine Vertretung der Datenschutzbeauftragten in externen Gremien, die sich mit Datenschutz und IT-Sicherheit in der Verwaltung und der Wirtschaft befassen.

6.2.1 Arbeitskreis Technik

Im Arbeitskreis Technik (AK Technik) beraten sich Vertreter der Technikabteilungen bzw. Technikreferate der Datenschutzbeauftragten der Länder und des Bundes. Mitglieder sind ebenfalls Vertreter des kirchlichen Datenschutzes sowie der Datenschutzbehörden aus der Schweiz und aus Liechtenstein. Der Arbeitskreis bereitet Kommentare, Orientierungshilfen und Entschließungen zu technischen Themen für die DSK vor. Einen weiteren Schwerpunkt bilden die gegenseitige Information und Koordination von Prüfungen und Bewertungen.

Relevante Themen im Berichtszeitraum waren Cloud-Dienste und ihre Prüfbarkeit aus technisch-organisatorischer Sicht, das Standard-Datenschutzmodell (Tz. 6.3) sowie die Wiedererkennung von Kfz bei streckenbasierten Geschwindigkeitskontrollen („Section Control“) und Verkehrsflussmessungen. Derzeit liegt der Arbeitsschwerpunkt auf der Überarbeitung und Anpassung bestehender Orientierungs- und Arbeitshilfen an die EU-Datenschutz-Grundverordnung.

6.2.2 Arbeitsgruppe der Datenschutzbeauftragten der Dataport-Trägerländer

Der Dienstleister Dataport hat insgesamt sechs Trägerländer: Schleswig-Holstein, Hamburg, Bremen, Niedersachsen, Mecklenburg-Vorpommern und Sachsen-Anhalt. Für diese führt Dataport insbesondere Auftragsdatenverarbeitungen durch, wobei das für die Auftraggeber jeweils geltende Recht zu beachten ist. Bei der Auftragsdatenverarbeitung für die Trägerländer oder deren Kommunen muss Dataport für einzelne Verfahren bis zu sechs verschiedene landesspezifische Regelungen beachten und wird durch bis zu sechs Datenschutzaufsichtsbehörden kontrolliert. Daneben verarbeitet Dataport eigenverantwortlich Daten, z. B. Personaldaten. Diese Verarbeitung richtet sich gemäß dem Staatsvertrag nach dem LDSG Schleswig-Holstein; die zuständige Aufsichtsbehörde ist das ULD.

Erklärtes Ziel der Gründung von Dataport war, durch Zusammenarbeit Synergieeffekte zu nutzen. Dies gelingt, wenn Verfahren länderübergreifend oder möglichst einheitlich, z. B. durch Nutzung der gleichen Software, betrieben werden können. Beispiele hierfür sind Verfahren für das Personenstandswesen und der Zentrale Meldedatenbestand, in dem die Meldedaten der Meldebehörden auf Landesebene gebündelt und für Auskunftsverfahren bereitgestellt werden.

Die Grenzen der übergreifenden Zusammenarbeit bilden die jeweiligen landesrechtlichen Regelungen. Daher sind bei länderübergreifenden Verfahren zumindest die Bundesländer als eigene Mandanten zu betreiben. Bei Flächenländern wie Sachsen-Anhalt und Schleswig-Holstein kommen häufig noch kommunale Mandanten hinzu. Auch aufgrund der Behördenorganisation in den Ländern unterscheiden sich Verfahren und Verfahrensweise insbesondere zwischen Stadtstaaten und Flächenländern – ein Umstand, der Anpassung der Verfahren erfordert.

Da bis zu sechs Aufsichtsbehörden zuständig sind, sind Absprachen bei Prüfungen und Beratungen notwendig. Zu diesem Zweck treffen sich die Datenschutzaufsichtsbehörden regelmäßig auf Arbeits- und Leitungsebene und nehmen Informationstermine durch Dataport wahr. 2017 wird erstmals eine gemeinsame Prüfung der Datenschutzaufsichtsbehörden im technischen Bereich erfolgen.

Was ist zu tun?

Dataport und seine Auftraggeber sollten die Datenschutzbeauftragten weiterhin frühzeitig einbinden. Dadurch können bereits in der Planungsphase unterschiedliche landesrechtliche Regelungen erkannt und passende Lösungen erarbeitet werden.

6.2.3 Standardisierung von Datentransporten im E-Government (XTA)

Das ULD berät stellvertretend für die Datenschutzaufsichtsbehörden der Länder eine Arbeitsgruppe der Koordinierungsstelle für IT-Standards (KoSIT), die als operativer Arm des IT-Planungsrats arbeitet. Sie erstellt u. a. die Spezifikation eines „fachunabhängigen Standards für Transportverfahren“ (XTA) für die öffentliche Verwaltung.

Aufgabe des Standards XTA

Die Sachbearbeitung in einer öffentlichen Verwaltung erfolgt meist mithilfe von Fachverfahren, z. B. für das Einwohnermeldewesen. Diese Fachverfahren kommunizieren mit anderen Fachverfahren derselben Verwaltung, aber auch mit Fachverfahren anderer Behörden (etwa Einwohnermeldeverfahren bei Umzügen). Dabei kommen verschiedene Transportmechanismen für die Daten zum Einsatz. XTA ist ein Programmbestandteil, der zwischen den Fachverfahren und den verfügbaren Transportmechanismen (z. B. OSCI-Transport, Direkteintrag in Datenbanken, örtliche Clearingstellen usw.) vermittelt und beispielsweise bestimmen kann, welche Transportmechanismen zum Einsatz kommen dürfen.

Die Datenübertragung entspricht in der papierbasierten Welt der Weitergabe von Papieren oder Akten, entweder innerhalb einer Verwaltung oder an andere Verwaltungen. Die Transportmechanismen setzen die verschiedenen Formen der Weitergabe bzw. des Versands (etwa persönliche Übergabe, Einlegen in örtliche Ablagefächer, Postversand, Einschreiben, Kurier für Verschlusssachen usw.) um. Mit dem Standard XTA lassen sich Verfahren beschreiben, mit denen die Modalitäten der Weitergabe der Daten festgelegt werden können, etwa: „Personalakten innerhalb der Verwaltung in geschlossenen Umschlägen oder von Hand zu Hand, an andere Verwaltungen nur per Post und Einschreiben weitergeben.“

Der Hintergrund zur Notwendigkeit dieser Standardisierung der elektronischen Kommunikation in der öffentlichen Verwaltung sowie der Begleitung der XTA-Entwicklung durch Datenschutzexperten wurde bereits im letzten Tätigkeitsbericht (35. TB, Tz. 6.2.4) dargestellt. Im Januar 2017 wurde nun die Spezifikation von XTA (Version 3) veröffentlicht, dazu die „Service Profile Schemata (V1.1)“ und die „XTA-WS-Schemata (V2.1.1)“ (http://www.xoev.de/downloads-2316#XTA). Dataport ist als einer der führenden Entwickler und Nutznießer von XTA beteiligt.

Die Standardisierung der Datenübertragung (genauer: des „Nachrichtentransports“) durch XTA geschieht auf zwei Ebenen: auf der nor-

mativen und auf der technisch-operativen Ebene:

Auf normativer Ebene wird den Auftraggebern – das ist aktuell der IT-Planungsrat, der deutschlandweit die Kommunikation zwischen den Behörden beim Bund und bei den Ländern und Gemeinden plant und abstimmt – das Modul „Service Profile“ bereitgestellt. Mit diesem Werkzeug können Anforderungen an Funktionalität, Datenschutz und IT-Sicherheit sowohl für den Transport als auch die dabei beteiligten Instanzen definiert und damit einheitlich konfigurierbar gemacht werden. Dies erfordert, dass der Gesetzgeber die rechtlichen Anforderungen an die Kommunikation und Sicherheit so formuliert, dass deren Rechtskonformität prüfbar und die technische Umsetzung eindeutig spezifizierbar und betriebswirtschaftlich kalkulierbar wird.

Auf technischer Ebene wird durch das Modul des „XTA-Webservice“ (XTA-WS) der Transport von Daten standardisiert. Die Spezifikation von Webservices vereinheitlicht die Schnittstellen zwischen Fachverfahren und Transportverfahren. Für die rechtskonforme Steuerung der dabei zu wählenden Adressierungen, Schutzfunktionen und Überwachungen sorgt XTA anhand der zuvor genannten Service Profile.

Die Spezifikation und Entwicklung des XTA-Standards wurde anhand der sieben Gewährleistungsziele des Standard-Datenschutzmodells (Tz. 6.3) modelliert. Seit 2014 hat diese Spezifikation eine zusätzliche Konkretion, insbesondere im Bereich der Dokumentation und Protokollierung, erfahren.

Mithilfe von Protokollierungen auf verschiedenen Ebenen kann beispielsweise der Nachweis erbracht werden, dass ein Nachrichtentransport erfolgreich war (z. B. Zustellungsquittung) und dass er in einer geforderten Art und Weise (z. B. unter Nutzung eines vorgegebenen Transportmechanismus unter Nutzung verbindlicher Verschlüsselungs- und Quittierungsfunktionen) erfolgt ist. Auf diese Weise lässt sich überprüfen, ob die Anforderungen eines Service Profiles umgesetzt wurden.

Offen ist noch, ob und inwieweit die Anforderungen an die übrige Infrastruktur eines Rechenzentrums (etwa Speichersysteme, Netzanbindungen, Administrationsverfahren) so standardisiert werden können, dass man von einem „XTA-konformen Rechenzentrum“ sprechen kann, dessen Nutzung per XTA gefordert oder sogar erzwungen werden könnte. Dieser Aspekt dürfte mit zunehmender Nutzung der Service Profile und Standardisierung von Datenübermittlungen von Fachverfahren einen immer größeren Nutzerkreis (Verwaltungsbereiche) betreffen. Potenziell sind damit auch zunehmend mehr private und öffentliche Rechenzentren betroffen, die sich als „XTA-konform“ ausweisen können sollten. Noch nicht hinreichend spezifiziert sind außerdem Testverfahren, um XTA-Konformität von Services und Servicebetreibern feststellen zu können.

Was ist zu tun?

Die Spezifikation sollte insbesondere im Hinblick auf Aspekte des Konformitätsnachweises weiterentwickelt werden. Die datenschutzrechtlichen Anforderungen an Funktionalität und Schutzmaßnahmen sollten gezielter formuliert und automatisiert durchgesetzt werden.

6.3 Das Standard-Datenschutzmodell (SDM)

Die 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) hat im November 2016 die Version 1.0 des Standard-Datenschutzmodells zustimmend zur Kenntnis genommen. Die DSK empfiehlt, die Nutzung des Modells bei Beratungs- und Prüfungstätigkeiten zu evaluieren und damit die Praxistauglichkeit zu erproben. Seit Januar 2017 liegt ein erster Entwurf der Englisch-Übersetzung des Standard-Datenschutzmodells vor, der in die europäischen Datenschutzgremien eingespeist werden wird.

Das Dokument zum Standard-Datenschutzmodell beschreibt die Methodik, um rechtliche Anforderungen und technische und organisatorische Eigenschaften in ein systematisches Verhältnis setzen zu können. Das Standard-Daten-

schutzmodell berücksichtigt auch die Anforderungen der DSGVO im Bereich der technisch-organisatorischen Maßnahmen. Die im März 2013 gegründete Unterarbeitsgruppe zum SDM hatte im Jahr 2015 damit begonnen, neben der Methodik einen Katalog mit Schutzmaßnahmen zu entwickeln. Als methodisches Vorbild dienen die Grundschutzmethode und die Grundschutz-Kataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI). Allerdings betont das Standard-Datenschutzmodell im Unterschied zum IT-Grundschutz, der vornehmlich die Perspektive der datenverarbeitenden Stellen in den Vordergrund stellt, die Sicht der betroffenen Personen und ihre Rechte. Dies wirkt sich auch auf den „Baustein 1.5 – Datenschutz“ in den IT-Grundschutz-Katalogen des BSI aus, in den nunmehr das Standard-Datenschutzmodell knapp eingeführt werden soll. In diesem Text wird deutlich, dass Datenschutz einerseits ohne Maßnahmen der Informationssicherheit nicht umsetzbar ist und andererseits die Maßnahmen der Informationssicherheit wiederum datenschutzgerecht zu gestalten sind.

Zusätzlich werden übergreifende Datenschutzmaßnahmen wie die Datenschutz-Folgenabschätzung und Datenschutz-Zuständigkeiten (Datenschutzbeauftragter) ebenso wie Maßnahmenbündel zu komplexen Themenstellungen (wie beispielsweise Schuldatenverarbeitung, Videoüberwachung oder Krankenhausinformationssysteme) als Orientierungshilfen veröffentlicht.

Die Trennung von IT-Sicherheit und operativem Datenschutz verlangt von vielen Expertinnen und Experten auch im Bereich des Datenschutzes ein Umdenken, weil sie über viele Jahre hinweg personenbezogene Daten nur als eine technisch besonders schützenswerte Form von Daten begriffen haben. Es wurde mit dem BSI vereinbart, wechselseitig in den IT-Grundschutz-Katalogen und in den SDM-Dokumenten stärker aufeinander zu verweisen.

Die Schulungs- und Beratungstätigkeiten im Jahr 2016 zum SDM haben gerade im Privatbereich stark zugenommen. Im Rahmen der Beteiligung des ULD am Projekt „Forum Privatheit“ (Tz. 8.1) wurde ein Ablaufprozess für eine Datenschutz-Folgenabschätzung entwickelt, der in seinem materiellen Kernbereich stark auf die Methodik und die Maßnahmen nach dem SDM abstellt.

https://www.datenschutzzentrum.de/sdm/

6.4 Datenschutz-Folgenabschätzung – ein neues Instrument aus der Grundverordnung

In Artikel 35 DSGVO wird von Organisationen eine Abschätzung der Datenschutzfolgen verlangt, um auf dieser Basis eine bessere Beherrschbarkeit der Risiken und einen verantwortungsvollen Umgang mit personenbezogenen Daten zu erreichen. Diese Abschätzung ersetzt die Vorabkontrolle aus § 4d Abs. 5, 6 BDSG bzw. § 9 LDSG-SH.

Eine Datenschutz-Folgenabschätzung (DSFA) (englische Bezeichnung: „Data Protection Impact Assessment“ (DPIA)) ist laut Artikel 35 DSGVO bei Verfahren mit einem vermutlich hohen Risiko für die Rechte und Freiheiten natürlicher Personen erforderlich. Bei der Prüfung solcher Risiken müssen die potenziellen Schäden – diese können nach Erwägungsgrund 75 physischer, materieller oder immaterieller Art sein – und die Eintrittswahrscheinlichkeit berücksichtigt werden.

Artikel 35 DSGVO nennt einige Faktoren, bei denen von einem hohen Risiko ausgegangen werden muss und demnach eine DSFA durchzuführen ist: Einsatz neuer Technologien, automatisierte Einzelentscheidungen einschließlich Profiling, umfangreiche Verarbeitung besonderer Arten personenbezogener Daten oder systematische umfangreiche Überwachung des öffentlichen Raums. Zusätzlich werden die Aufsichtsbehörden eine Liste von Verarbeitungstätigkeiten, für die in jedem Fall eine DSFA durchzuführen ist, erstellen.

Die Bestandteile einer DSFA sind ebenfalls im Artikel 35 DSGVO festgelegt: Gefordert ist u. a. eine Beschreibung des Verfahrens, der Zwecke, der berechtigten Interessen sowie eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung sowie der Risiken für Betroffene. Ebenso gefordert ist eine Beschreibung der geplanten Schutzmaßnahmen mit Nachweis über deren Wirksamkeit. Die DSFA ist durch die Verantwortlichen durchzuführen; Datenschutzbeauftragte sind beratend tätig.

Das ULD hat im Rahmen des Projekts „Forum Privatheit“ (Tz. 8.1) zusammen mit weiteren Projektpartnern ein generisches Prozessmodell zur vollständigen Durchführung einer DSFA erarbeitet. Dieses Prozessmodell funktioniert

nicht nur für eine DSFA von Verarbeitungsvorgängen nach Artikel 35 DSGVO, sondern ermöglicht auch den Einsatz für wissenschaftliche Untersuchungen von abstrakteren Gegebenheiten, z. B. zur vergleichenden Analyse von staatlichen Überwachungslösungen.

Der Ablauf der DSFA umfasst fünf Phasen: (1) Vorbereitungsphase, (2) Bewertungsphase, (3) Maßnahmenphase, (4) Berichtsphase sowie (5) die Einbindung des Verfahrens in das Datenschutzmanagementsystem einer Organisation. Ein White Paper zur Darstellung des Ablaufmodells findet sich auf der Webseite:

https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums.php

Bei der Erarbeitung des Prozessmodells haben sich zwei wichtige Aspekte herausgestellt:

- Bei einer systematischen Durchführung einer DSFA empfiehlt es sich, für die Prüfung der rechtlich angemessenen Funktionalitäten und Schutzmaßnahmen in den Phasen 2 und 3 auf die Methodik und die Maßnahmen des Standard-Datenschutzmodells (Tz. 6.3) zurückzugreifen. Bei der Abschätzung des Risikos bietet es sich an, für die Gewährleistungsziele, die im Artikel 5 der DSGVO als Grundsätze enthalten und im SDM ausgeführt sind, zu untersuchen, ob sie vom geplanten Verfahren im erforderlichen Maße umgesetzt werden.
- Artikel 35 DSGVO verlangt mehr als nur eine Abschätzung, welche Risiken durch die beabsichtigte Nutzung des Verfahrens entstehen. Er fordert auch, Schutzmaßnahmen festzulegen und ihre Wirksamkeit nachzuweisen.

Das ULD rät dazu, vor der Einführung eines Verfahrens im Rahmen einer schlanken „Vorab-DSFA“ zu prüfen, ob vermutlich hohe Risiken für Betroffene bestehen und somit die Notwendigkeit einer DSFA gemäß Artikel 35 DGSVO gegeben ist. Zeigt sich, dass nicht mit einem hohen Risiko zu rechnen ist, kann dies die Grundlage für die Rechtfertigung der Entscheidung bilden, dass keine vollständige DSFA durchzuführen ist. Dies ist zu dokumentieren. Bestehen hohe Risiken, so ist eine vollständige DSFA durchzuführen.

Was ist zu tun?

Jede verantwortliche Stelle sollte jetzt ihre Verfahren daraufhin überprüfen, ob eine Datenschutz-Folgenabschätzung durchzuführen ist, und die notwendigen Maßnahmen ergreifen, um die Pflichten nach der Datenschutz-Grundverordnung rechtzeitig umzusetzen.

6.5 Ausgewählte Ergebnisse aus Vorabkontrollen und Prüfungen

6.5.1 Verfahrensdokumentation bei zentralen Verfahren am Beispiel von „KoPers kommunal“

Die Datenschutzverordnung (DSVO) regelt in Verbindung mit dem Landesdatenschutzgesetz Schleswig-Holstein (LDSG) die Anforderung an die Dokumentation von automatisierten Verfahren. Für viele verantwortliche Stellen ist es nicht leicht, diese Anforderungen an Verfahren in ihrem Verantwortungsbereich in Bezug auf Struktur, Transparenz und Vollständigkeit zu erfüllen.

Die Vorlagen und Handreichungen des ULD zum Themenbereich Dokumentation können in diesem Zusammenhang eine Hilfestellung leisten:

https://www.datenschutzzentrum.de/dsvo/

Bei zentralen Verfahren gibt es jedoch nicht nur eine verantwortliche Stelle, die die Dokumentationspflichten übernimmt, sondern die Aufgabe der Dokumentation verteilt sich auf verschiedene Verantwortungsbereiche. Das sind die zentrale Stelle selbst, die beteiligten Stellen sowie gegebenenfalls externe Dienstleister.

Ein solches zentrales Verfahren ist „KoPers kommunal“, ein Personalmanagementsystem im kommunalen Bereich, das seit mehreren Jahren weiterentwickelt wird. In gemeinsamen Sitzungen mit der Versorgungsausgleichskasse der Kommunalverbände in Schleswig-Holstein (VAK), Dataport und den behördlichen Datenschutzbeauftragten einiger beteiligter Stellen konnte die Grundlage für eine Handreichung des ULD erarbeitet werden, die die Dokumentationspflichten aller am Verfahren beteiligten Stellen beschreibt. Die Handreichung basiert auf den oben beschriebenen Dokumentationsvorlagen und kann auf der Webseite des ULD heruntergeladen werden:

https://www.datenschutzzentrum.de/uploads/dsvo/verfahrensakte/Dokumentation_zentrale_beteiligte_Stelle.pdf

Was ist zu tun?

Bei jedem zentralen Verfahren muss anhand der gesetzlichen Grundlagen festgelegt werden, welche Dokumentationspflichten für die zentrale Stelle, für die beteiligten Stellen und gegebenenfalls für externe Dienstleister bestehen.

6.5.2 Vorabkontrolle beim BAföG-Verfahren

Das Ministerium für Soziales, Gesundheit, Wissenschaft und Gleichstellung (MSGWG) hat sich 2015 entschlossen, das Verfahren „BafSys“ für die Bearbeitung von BAföG-Anträgen einzuführen. Das ULD wurde im Rahmen einer Vorabkontrolle eingebunden.

Während die BAföG-Ämter in den Kreisen, kreisfreien Städten und Studentenwerken das Verfahren anwenden und somit für die Inhalte des Verfahrens sowie für die Umsetzung der Datenschutzanforderungen vor Ort verantwortlich sind, agiert das MSGWG als zentrale Stelle: Es beauftragt und kontrolliert den Dienstleister Dataport in den zentralen operativen Aspekten des Verfahrens.

Die Rechtsgrundlagen der Datenverarbeitung finden sich vornehmlich im Bundesausbildungsförderungsgesetz (BAföG). Die Rolle des MSGWG als zentrale Stelle ist seit dem 01.05.2016 per Verordnung geregelt (Landesverordnung VOzS BaföG). Es liegen Verträge zwischen dem MSGWG und den Kommunen sowie dem MSGWG und Dataport vor. Die Rechtsgrundlagen bezüglich des Übermittelns von BAföG-Daten an andere im Grundsatz gesetzlich berechtigten Bedarfsträger (Bundesverwaltungsamt (BVA), Bundeszentralamt für Steuern (BZSt), KfW-Bank für Vergabe von Studienkrediten) sind jedoch vielfach nicht hinreichend klar dokumentiert.

Die technisch-organisatorischen Maßnahmen wurden aufseiten des ULD unter Zuhilfenahme des Standard-Datenschutzmodells (Tz. 6.3) geprüft. Als Ausgangspunkt für die Gestaltung der Funktionen und Schutzmaßnahmen wurde zunächst der Schutzbedarf des Verfahrens herangezogen und anschließend die zu treffenden Maßnahmen anhand von Gewährleistungszielen (vgl. § 5 LDSG) bestimmt. Geprüft wurden die vom MSGWG vorgelegten Dokumente der zentralen Verfahrensbestandteile von BafSys.

BAföG-Daten sind Sozialdaten und haben damit einen hohen Schutzbedarf, dem alle IT-Komponenten des Verfahrens genügen müssen. Das bedeutet, dass die Funktionen und Maßnahmen des Datenschutzes wirksam umgesetzt und anhand von Protokolldaten und einer vollständigen und aktuellen Dokumentation kontrollierbar sein müssen.

Der zentrale Verfahrensbestandteil von BafSys wird im Sicherheitsbereich „hoch“ des Rechenzentrums von Dataport betrieben. Die Clients für die Fachkräfte in den BAföG-Ämtern sind über das Landesnetz angebunden, die Kommunikation zwischen den Citrix-Clients und den zentralen Servern bei Dataport geschieht laut Auskunft von Dataport verschlüsselt.

Die Trennung der Verfahren pro BAföG-Amt ist als Mandantentrennung innerhalb einer gemeinsamen Datenbank ausgeführt. Diese Trennung ist schwach; Daten können versehentlich (z. B. bei Programmierfehlern) oder vorsätzlich zusammengeführt werden. Auch Fehler bei der

Nutzerverwaltung können relativ leicht dazu führen, dass Zugriffe auf falsche Datenbestände eingerichtet werden. Das MSGWG wurde auf die schwache Trennungsqualität hingewiesen. Die vorliegende Trennung ist zumindest in der Hinsicht hinreichend, dass die Ämter im Normalbetrieb unabhängig voneinander agieren können.

Eine schwache Durchsetzung der Trennungsanforderung bedarf zumindest der Kompensation durch eine besonders gesicherte Prüfbarkeit der Aktivitäten der Systeme, der Sachbearbeitung sowie der Administration. Die Prüfbarkeit des Verfahrensbetriebs muss bereits bei der Spezifikation berücksichtigt werden. Die Datengrundlage bilden Protokolldaten. Hier ist bei BafSys Vieles bislang nicht ausgereift: Weder die Protokollierung auf der Ebene der Sachbearbeitung noch die der Administration der Fachapplikation noch die Tätigkeiten der Systeme auf der Infrastrukturebene und der Schnittstellen sowie deren Administration sind hinreichend konzipiert bzw. aufeinander abgestimmt. Beim Auftragsdatenverarbeiter Dataport fallen zahlreiche Protokolldaten an – nur ist der Verfahrensbezug dieser Protokolle durch das MSGWG nicht sichergestellt. Dies ist jedoch kein BafSys-spezifisches Problem, sondern ein generelles Problem der Arbeitsteilung beim Verfahrensbetrieb in einem Rechenzentrum.

Die Nutzerverwaltung erfolgt im Auftrag durch Dataport und wird auch bei Dataport protokolliert. Die Aktivitäten des Auftragsdatenverarbeiters durch den Verantwortlichen können mit der vorliegenden Protokollierungslösung nicht zweifelsfrei überwacht werden, weil der zu überwachende Auftragnehmer die Instrumente zu seiner Überwachung in der eigenen Hoheit betreibt. Zudem sind bislang keine Prozesse vorgesehen, wenn sich aus Prüfungen Klärungsbedarf ergibt.

Die Dokumentation ließ nicht erkennen, ob und wie Übermittlungen aus dem BafSys-Datenbestand freigegeben werden. In diesem Zusammenhang spielt der Aspekt der Pseudonymisierung und Anonymisierung von Daten eine besondere Rolle, wenn diese zu Zwecken statistischer Auswertungen wie vorgesehen an das Statistische Bundesamt zu übermitteln sind. Diese sind sorgsam zu spezifizierende Prozesse, die bisher jedoch dem ULD gegenüber nicht dargestellt wurden. Aus diesem Grund konnte deren Qualität noch nicht geprüft und daraufhin rechtlich beurteilt werden, ob diese dem hohen Schutzbedarf entsprechen.

Was ist zu tun?

Es muss mit größerem Nachdruck als bislang dafür gesorgt werden, dass die Aktivitäten auf der Ebene der Sachbearbeitung sowie den verschiedenen Ebenen der IT-Systeme und der IT-Administrationen zweifelsfrei anhand der Dokumentation und der Protokolldaten überprüfbar sind.

6.5.3 eBeihilfe – automatisierte Bearbeitung von Beihilfeanträgen

Im Rahmen der Gewährung von Beihilfen für die Beschäftigten des Landes werden derzeit beim Dienstleistungszentrum Personal (DLZP) Beihilfeunterlagen, Anträge und Anlagen (z. B. Rechnungskopien) bearbeitet. In der Vergangenheit wurden diese nach der Bearbeitung und Bescheiderstellung eingescannt und elektronisch archiviert. Die Papieroriginale wurden vernichtet (35. TB, Tz. 4.1.7).

Zur Schaffung von Synergien wurde vor 2011 das Projekt „eBeihilfe“ gestartet, das die Bearbeitung von Beihilfeanträgen automatisieren soll. Das ULD war im Rahmen einer Vorabkontrolle beteiligt. In einer ersten Stufe („Stufe 1a“) wurde die Digitalisierung der eingereichten Unterlagen der Bearbeitung vorgelagert, sodass diese elektronisch der Sachbearbeitung vorgelegt werden. Die Berechnung und Bescheiderstellung erfolgt weiterhin mit der Fachanwendung PERMIS-B. Eine Herausforderung dabei ist neben der Bearbeitung von Fehlern beim Scannen (Unleserlichkeiten) die Klassifizierung der Unterlagen: Anträge, Rechnungen, Rezepte und weitere Belege werden unterschieden, um diese strukturiert bearbeiten zu können. U. a. werden Rezepte automatisiert ausgewertet, damit das Land Arzneimittelrabatte wahrnehmen kann. Die eingereichten Unterlagen und ebenso ihre elektronischen Pendants unterliegen verschiedenen Aufbewahrungsfristen, die sich aus § 91 Abs. 2 Lan-

desbeamtengesetz ergeben: So sind Unterlagen, aus denen sich Rückschlüsse auf die Krankheit ergeben (üblicherweise Rechnungen mit Diagnosen), drei Monate, Rezepte zwölf Monate und übrige Unterlagen fünf Jahre aufzubewahren. Bei Fehlzuordnungen kann manuell die Klassifikation verändert werden.

Papierunterlagen werden drei Monate nach dem Einscannen vernichtet. Für die Löschung der elektronischen Daten liegen mittlerweile Löschkonzepte vor. Dies betrifft zum einen die Beihilfedaten, die in der datenbankbasierten Anwendung PERMIS-B gespeichert sind. Zum anderen sind die elektronischen Dokumente zu löschen. Das Löschen erfolgt automatisiert in Abhängigkeit der vorgegebenen Fristen. Dies wird durch das Verfahren PERMIS-B gesteuert, das das elektronische Archiv ansteuert und die Löschung auslöst. Zu beachten ist dabei, dass im Streitfall (beispielsweise bei Widerspruchs- oder Gerichtsverfahren) die automatische Löschung fall- und dokumentenbasiert aufgeschoben werden muss. Das DLZP entschied sich gegen eine elektronische Signatur der Scandateien, die im Hinblick auf die unterschiedlichen Aufbewahrungsfristen jeweils pro Dokument bzw. Dokumentenklasse erfolgen muss. Beweggrund war neben dem manuellen Prüf- und Signieraufwand auch die Schwierigkeit, im Augenblick des Scans eine zweifelsfreie Klassifikation und damit eine Unterteilung der eingereichten Dokumente vorzunehmen. Einen Entlastungsbeweis über einen streitigen Umfang der eingereichten Dokumente („Wurde Anlage 7 tatsächlich eingereicht“?) kann das DLZP mit einer Signatur nicht führen, denn diese gewährleistet lediglich die Integrität gespeicherter Dokumente und schützt nicht vor Verlust oder Löschung einzelner Dateien.

Was ist zu tun?

Auch in weiteren Projektphasen – nach der Vorabkontrolle – ist eine Beteiligung des ULD sinnvoll, denn Beihilfedaten sind sensibel und gesetzlich besonders geschützt.

6.5.4 Personalbefragungen zum betrieblichen Gesundheitsmanagement

Eingebunden war das ULD in verschiedene Projekte der Staatskanzlei und anderer Behörden, die anhand von Befragungen der Beschäftigten Erkenntnisse für das betriebliche Gesundheitsmanagement gewinnen wollten. Typische Fragestellungen umfassen die Belastungssituation, Zufriedenheit am Arbeitsplatz und gegebenenfalls Hinweise auf Auslöser von Krankheiten, aber auch soziografische Daten wie Alter, Tätigkeitsumfang (Vollzeit/Teilzeit) und Beschäftigtenstatus (angestellt/beamtet). Aufgrund der Sensibilität der Fragen wurde eine anonyme Befragung durch einen darauf spezialisierten Auftragnehmer geplant.

Hierbei sollten sowohl ressortübergreifende Erkenntnisse als auch Erkenntnisse auf Ressort- und Abteilungsebene gewonnen werden. Die Ressorts hatten daher die Möglichkeit, spezifische Fragestellungen innerhalb des Ressorts zu entwickeln und Auswertungen auf Ressort- und Abteilungsebene zu beauftragen. Dies hat zur Folge, dass Antworten zumindest den Abteilungen zugeordnet werden können und somit die Anonymitätsgruppe (d. h. die Gruppe, innerhalb der ein Antwortender anonym ist) höchstens so groß wie die zugehörige Abteilung ist.

Die Herausforderung bestand darin, bei der Durchführung und Auswertung der Befragung die Anonymität der Beschäftigten zu wahren. Würde die Auswertung durch den Auftraggeber direkt erfolgen, könnte dieser mit dem Zusatzwissen der soziografischen Daten die Antworten einzelnen Befragten zuordnen. Daher wurden Dienstleister beauftragt, die einerseits die Befragung und die Auswertung vornahmen, andererseits gerade nicht über das Zusatzwissen verfügten, um Antworten einzelnen Befragten zuordnen zu können. Vertraglich wurde festgelegt, dass die vollständigen Antworten beim Auftragnehmer verbleiben und dass beauftragte Einzelauswertungen so vorgenommen werden, dass bei der untersuchten Gruppe eine Mindestzahl von Mitgliedern (z. B. zehn Personen) das relevante Merkmal umfassen muss. Ist diese Bedingung nicht erfüllt, so darf keine Einzelauswertung erfolgen; stattdessen wird aggregiert ausgewertet. Hat beispielsweise eine Behörde eine Abteilung mit 18 Personen, bestehend aus elf Frauen und sieben Männern,

so kann keine geschlechtsspezifische Auswertung durchgeführt werden. Eine Zusammenfassung der Auswertung mit einer zweiten Abteilung, bestehend aus vier Frauen und vier Männern, ist hingegen möglich, da stets mehr als zehn Personen dasselbe Geschlecht haben.

Eine weitere Fragestellung betraf die praktische Frage, ob eine Online-Befragung möglich ist oder ob eine papierbasierte Befragung erfolgen muss: Bei einer Online-Befragung besteht zumindest theoretisch die Möglichkeit, über die Rückverfolgung von IP-Adressen den Antwortenden zu ermitteln oder einzugrenzen. Dies wurde jedoch vertraglich und konfigurativ ausgeschlossen. Problematisiert wurde auch die Möglichkeit von (unerwünschten) Mehrfachbeantwortungen. Zwar ließe sich technisch relativ einfach sicherstellen, dass jede bzw. jeder Befragte einen Online-Fragebogen nur einmal ausfüllen kann, doch müssten dazu individuelle Kennzeichen (etwa Befragungsnummern) vergeben und den Befragten individuell, aber unter Wahrung der Anonymität zugestellt werden. Man entschied sich, an die Kooperationsbereitschaft zu appellieren und auf eine Authentisierung zu verzichten.

Was ist zu tun?

Personalbefragungen können sensible Informationen beinhalten, sodass Datenschutzmaßnahmen wie verlässliche Anonymisierung und geeignete Verträge mit Dienstleistern besonders wichtig sind.

07

KERNPUNKTE

Sensible Ortsinformationen
Wearables
Medienkompetenz

7 Neue Medien

7.1 EuGH-Verfahren zu Facebook-Seiten

Das seit 2011 laufende Verfahren um die datenschutzrechtliche Verantwortlichkeit von Betreibern von Facebook-Seiten wurde im Februar 2016 vor dem Bundesverwaltungsgericht in Leipzig verhandelt. Entschieden wurde jedoch nichts: Stattdessen legte das Bundesverwaltungsgericht dem Gerichtshof der Europäischen Union (EuGH) sechs Fragen vor, in denen es um die korrekte Interpretation des Datenschutzrechts geht. Diese Fragen betreffen neben der europaweiten Kooperation der Aufsichtsbehörden vor allem die Verantwortlichkeit der Seitenbetreiber.

In dem zugrunde liegenden Sachverhalt haben sich die Betreiber der Facebook-Seiten bewusst für die Nutzung von Facebook entschieden und ihr Angebot dort aufgebaut. Das ULD hatte zuletzt deutlich darauf hingewiesen, dass die fehlende Kontrolle über die Facebook-Seiten kein Argument gegen eine Verantwortlichkeit der Seitenbetreiber sein kann. Auch kann es keine Rolle spielen, dass zwischen Seitenbetreiber und Facebook kein mustergültiger Auftragsdatenverarbeitungsvertrag besteht. Mit diesen Argumenten hatten die Vorinstanzen den Bescheid des ULD noch für rechtswidrig erklärt.

Die Einbindung Dritter in die eigene Datenverarbeitung ist im deutschen Recht genauso wie in der EU-Datenschutz-Richtlinie von 1995 sowie in der ab Mai 2018 geltenden Datenschutz-Grundverordnung weitgehend identisch geregelt: Verantwortlich ist stets der, der über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Die Seitenbetreiber verfolgen mit den von ihnen betriebenen Facebook-Seiten eigene Marketing- und Kundenkommunikationsinteressen und wählen dafür das Instrument der Facebook-Seiten, statt beispielsweise konkurrierende Webseiten-Hosting-Dienste zu bemühen. Facebook verarbeitet folglich die Daten der Seitenbesucher im Interesse des Seitenbetreibers. Nach dem Wortlaut des europäischen Rechts genügt dies, um eine Verantwortlichkeit des Seitenbetreibers zu begründen.

Verantwortlichkeit für Datenschutz

Bezüglich der Verantwortlichkeit von Webseitenbetreibern für die von ihnen gewählten Webseitenhoster (z. B. Facebook als Anbieter der Facebook-Seiten) gibt es Auslegungsprobleme des deutschen Rechts, das teilweise andere Schlussfolgerungen nahelegt, als es die europarechtlichen Vorgaben tun. Dem EuGH liegen ausgehend von dem seit 2011 laufenden Gerichtsverfahren des ULD nun entsprechende Fragen zur Klärung vor. Eine Entscheidung des EuGH wird für Ende 2017 erwartet.

Das aktuelle deutsche Datenschutzrecht hingegen enthält im Wortlaut des § 3 Abs. 7 BDSG eine leicht abweichende Formulierung, die nahelegt, dass zusätzlich zu der Verarbeitung, die Facebook für die Seitenbetreiber durchführt, auch konkrete formelle und tatsächliche Voraussetzungen erfüllt werden müssen. Die Voraussetzungen sind nach Überzeugung des ULD im Europarecht allerdings lediglich Folge der Verarbeitung, nicht jedoch Bedingung für eine Verantwortlichkeit. Die fehlende Kontrolle und die fehlende vertragliche Fixierung der Weisungsrechte eines Verantwortlichen entlassen ihn auch in anderen Fällen nicht aus der datenschutzrechtlichen Verantwortlichkeit, sondern stellen im Gegenteil vielmehr für sich genommen bereits Verstöße gegen datenschutzrechtliche Vorgaben dar.

Ebendiese Abweichungen zwischen europäischen Vorgaben und deutschem Recht sind nun Gegenstand der Vorlagefragen an den EuGH. Die mündliche Verhandlung soll am 27. Juni 2017 stattfinden; mit einer Entscheidung des Gerichtshofs ist noch im Jahr 2017 zu rechnen.

7.2 Rundfunkbeitragsstaatsvertrag – Meldedatenabgleich und (zunächst) keine Adresskäufe

Im Jahr 2016 wurde der Rundfunkbeitragsstaatsvertrag der Länder geändert. Das ULD nahm zu den beabsichtigten Neuregelungen Stellung (Landtagsumdruck 18/6050). Zur Sicherstellung der Aktualität des Datenbestands soll demnach zum 1. Januar 2018 ein neuer Meldedatenabgleich durchgeführt werden, wobei zu jeder volljährigen Person der Familienname, Vornamen, frühere Namen, Doktorgrad, Familienstand, Tag der Geburt, gegenwärtige und letzte Anschrift von Haupt- und Nebenwohnungen einschließlich aller vorhandenen Angaben zur Lage der Wohnung und der Tag des Einzugs in die Wohnung an die Landesrundfunkanstalten übermittelt werden sollen. Die Datenübermittlung soll bis zum 31. Dezember 2018 abgeschlossen sein. Dies wird damit begründet, dass vor dem Hintergrund einer größtmöglichen Beitragsgerechtigkeit und der Vermeidung von Vollzugsdefiziten der Datenbestand in seiner Qualität erhalten werden solle.

Ist dieser geplante Meldedatenabgleich wirklich erforderlich? Bereits im Zuge der Umstellung des Rundfunkbeitrags im Jahr 2013 wurde ein vollständiger Meldedatenabgleich vorgenommen. Gleichwohl gehen die Rundfunkanstalten von einem jährlichen Verlust von rund 200.000 beitragspflichtigen Wohnungen aus, was sich nach deren Hochrechnung im Zeitraum bis 2020 zu einem Ertragspotenzial der dann nicht mehr im Bestand befindlichen Wohnungen zu einer Größenordnung von 750 Mio. Euro aufaddiere. Die genannten Zahlen sind allerdings nicht verifizierbar. Nach Auffassung des ULD ist zu berücksichtigen, dass zur Ermittlung der Beitragsschuldner mehrere Handlungsmöglichkeiten zur Verfügung stehen. Hierzu zählen die bußgeldbewehrte Anzeigepflicht der Inhaber einer Wohnung, einer Betriebsstätte oder eines beitragspflichtigen Kraftfahrzeugs. Weiterhin übermitteln die Meldebehörden dem NDR zum Zweck der Einziehung der Rundfunkbeiträge im Falle der Anmeldung, Abmeldung oder des Todes zu volljährigen Einwohnern einen Datensatz, der die folgenden Daten umfasst: Vor- und Familiennamen, frühere Namen, Doktorgrad, Tag der Geburt, gegenwärtige und letzte frühere Anschriften (Haupt- und Nebenwohnung), Tag des Ein- und Auszugs, bei Ehe oder Lebenspartnerschaft den Familienstand und gegebenenfalls den Sterbetag. Für einen zusätzlichen Meldedatenabgleich im Jahr 2018 besteht daher unserer Meinung nach keine Notwendigkeit.

Im geänderten Rundfunkstaatsvertrag wird auch bestimmt, dass die Landesrundfunkanstalten bis zum 31. Dezember 2020 keine Adressdaten privater Personen ankaufen dürfen und bis dahin keine Einholung von Auskünften bei Vermietern erfolgen darf. Nach diesem Datum aber schon. Doch da die Meldebehörden ohnehin im Falle der Anmeldung, Abmeldung oder des Todes eine Datenübermittlung vornehmen, ist nicht erkennbar, warum es überhaupt eine Option für Landesrundfunkanstalten geben soll, Adressdaten anzukaufen. Dabei ist auch zu berücksichtigen, dass die Datenbestände privater Adresshändler nicht per se aktuell sind. Im Rahmen von Beschwerden bei den Datenschutzaufsichtsbehörden wäre es den Bürgerinnen und Bürgern nicht vermittelbar, warum der Zentrale Beitragsservice im Auftrag der Rundfunkanstalten die Befugnis haben soll, Adressdaten auf dem freien Markt anzukaufen.

Was ist zu tun?

Bei Beratungen der Länder zu Änderungen im Rundfunkbeitragsstaatsvertrag sollte der Landtag sich für eine vollständige Streichung der Option einsetzen, dass der NDR Adressdaten bei privaten Stellen ankaufen darf. Weiterhin sollten zusätzliche Meldedatenabgleiche nicht mehr erlaubt werden, zumal im Melderecht in Schleswig-Holstein bereits eine Bestimmung zur Datenübermittlung an den NDR besteht.

7.3 WhatsApp im Einsatz bei datenverarbeitenden Stellen

Über das Jahr 2016 hinweg erreichten das ULD sowohl Beschwerden von Betroffenen als auch Beratungsanfragen zum Einsatz von WhatsApp durch Unternehmen. Die Nutzung von Messenger-Diensten hat nicht nur klassische SMS und Sprachnachrichten in der Alltagskommunikation verdrängt, sondern wird auch im Unternehmensumfeld nachgefragt. WhatsApp ist als einer der weltweit verbreitetsten Messenger-Dienste dabei oft die naheliegende Wahl.

Das ULD hat wie andere Aufsichtsbehörden bisher die Nutzung von WhatsApp im Unternehmenseinsatz jedoch aus unterschiedlichen Gründen untersagt. Dabei waren anfangs die fehlende Inhaltsverschlüsselung und der generelle Zugriff auf Kommunikationsinhalte durch US-Behörden die entscheidenden Kriterien. Einen solchen generellen Zugriff hatte der EuGH im Schrems-Urteil aus dem Jahr 2015 (Tz. 11.1) als eine Verletzung des Wesensgehalts von Grundrechten gewertet. Zudem hatte WhatsApp in seinen Nutzungsbedingungen bisher die Nutzung zu kommerziellen Zwecken ausgeschlossen, sodass der Dienst nicht den datenschutzrechtlichen Anforderungen an die Verfügbarkeit der Datenverarbeitung genügte.

Nach einer längeren Testphase setzt WhatsApp hinsichtlich der Inhalte der Nachrichten seit April 2016 eine Ende-zu-Ende-Verschlüsselung ein und hat sich nach einer Änderung der Nutzungsbedingungen im August 2016 zudem für den kommerziellen Einsatz geöffnet. Die früheren Kritikpunkte sind damit in gewissem Umfang bearbeitet worden, neue sind jedoch hinzugekommen.

So wurden im Januar 2017 Bedenken hinsichtlich der Verfahren der Schlüsselerzeugung und -verteilung laut, die Voraussetzung für die seit 2016 implementierte Ende-zu-Ende-Verschlüsselung sind. Die bei WhatsApp durch den Nutzer kaum kontrollierbare Verteilung der Schlüssel lasse es laut den Berichten denkbar erscheinen, dass WhatsApp zu einer für den Nutzer unbemerkten Weiterleitung der Nachrichten an Dritte verpflichtet werden könne.

Zudem wurde mit der Änderung der Nutzungsbedingungen nicht nur der kommerzielle Einsatz ermöglicht, sondern gleichzeitig auch eine vielfach kritisierte und bereits europaweit aufsichtsrechtlich untersuchte Datenweitergabe an den Facebook-Mutterkonzern bekannt gegeben. Diesbezüglich betonen jüngere EuGH-Urteile zunehmend die wachsende Bedeutung des Schutzes von sogenannten Metadaten für die Privatsphäre von Kommunikationsteilnehmern. Daten darüber, wer wann mit wem und wie lange kommuniziert, erlauben schwerwiegende Eingriffe in die Grundrechte der Kommunikationsteilnehmer – eine solche Auswertung wird durch Inhaltsverschlüsselung nicht verhindert. Im Gegenteil: WhatsApp liest die Informationen aus dem gesamten Smartphone-Adressbuch des Teilnehmers aus. Die Nutzungsbedingungen verdeutlichen dies: *„Du stellst uns regelmäßig die Telefonnummern von WhatsApp-Nutzern und deinen sonstigen Kontakten in deinem Mobiltelefon-Adressbuch zur Verfügung. Du bestätigst, dass du autorisiert bist, uns solche Telefonnummern zur Verfügung zu stellen, damit wir unsere Dienste anbieten können.“* Eine wirksame Autorisierung aller Kontakte wird in den seltensten Fällen vorliegen. Mit Blick auf die insoweit noch immer unsichere Rechtslage hinsichtlich des WhatsApp-Messengers bleibt das ULD hinsichtlich des Einsatzes zur Kommunikation mit Kundinnen und Kunden sowie unter Mitarbeiterinnen und Mitarbeitern weiterhin kritisch.

Derzeit wird auf europäischer Ebene zudem eine neue Verordnung über Privatsphäre und elektronische Kommunikation diskutiert, die voraussichtlich zusammen mit der Datenschutz-Grundverordnung ab Mai 2018 Geltungskraft erlangen wird und erstmals ausdrücklich auch Messenger wie WhatsApp erfasst. Die darin bisher im Entwurf geregelten Vorgaben hinsichtlich der Vertraulichkeit der Kommunikation sowie der Verarbeitung von Metadaten werden auch eine Neubewertung bei WhatsApp nötig machen. Für Unternehmen und Organisationen bleibt es daher derzeit weiter ratsam, sich hinsichtlich neuer Kommunikationsmittel nur rechtskonformer Dienste zu bedienen.

Was ist zu tun?

Technische und rechtliche Veränderungen bei WhatsApp haben zwar dazu geführt, dass frühere Hürden für den Unternehmenseinsatz reduziert wurden, neue Kritikpunkte sind jedoch hinzugekommen. Auch die voraussichtlich ab Mai 2018 geltende EU-Verordnung über Privatsphäre und elektronische Kommunikation lässt vermuten, dass ein rechtskonformer Einsatz von WhatsApp weiterhin nicht möglich ist. Dies müssen Unternehmen und öffentliche Stellen berücksichtigen.

7.4 „Pokémon Go“ und was Ortsinformationen verraten

Der Sommer 2016 war geprägt von „Pokémon Go“, einem Smartphone-Spiel von der Firma Niantic aus den USA. Der Spieler bewegt sich hierbei durch die normale Welt, fängt dabei virtuelle Fabelwesen (sogenannte Pokémons) ein und besucht Sehenswürdigkeiten, die im Spiel zu „Pokestops“ und „Arenen“ werden, um sich dort aufzurüsten und kleinere Kämpfe zu absolvieren. Uns erreichten zahlreiche Fragen von Bürgern und der Presse, wie es um den Datenschutz bei dem Spiel bestellt ist.

Insbesondere wird dauerhaft die Ortsinformation des Spielers ausgewertet und an den Anbieter übermittelt. Die Datenschutzbestimmungen lassen dabei dem Betreiber weitgehende Nutzungsmöglichkeiten. Auch eine nachträgliche Löschung der Daten ist allenfalls eingeschränkt möglich. Von der Nutzung des Spiels in der Dienstzeit muss somit (nicht nur aus Datenschutzgründen) abgeraten werden: Selbst wenn man gerade nicht aktiv Pokémons fängt, überträgt das Spiel Ortsinformationen. Auch Privatnutzer sollten sich die Gefahr der ständigen Überwachung ihres Aufenthaltsorts bewusst machen. Außerdem sollten sie überdenken, ob sie das Spiel mit ihrem auch für andere Anwendungen benutzten (Google-)Konto verwenden oder lieber ein neues Konto nur für diesen Zweck anlegen.

Ortsinformationen

Viele Smartphone-Anwendungen geben Ortsinformationen an die Anbieter weiter. Achtung: Orts- und Bewegungsdaten können viel über den Nutzer verraten: typische Aufenthaltsorte zu Hause, bei der Arbeit, bei Freunden und über Hobbys, Verkehrsmittel, Beziehungen usw. Dies betrifft nicht nur die eigenen personenbezogenen Daten des Nutzers, sondern verrät auch etwas über dessen Kontakte. Das können sogar sehr sensible Daten sein, z. B. wenn ein Arzt Hausbesuche macht, eine Apotheke Medikamente ausliefert, ein Journalist seine Informanten trifft oder Polizisten zu Einsatzorten gerufen werden. Diese Daten dürfen nicht in falsche Hände geraten – und schon gar nicht an außereuropäische Anbieter gelangen, die sich weitreichende Auswertungen vorbehalten.

Was ist zu tun?

Ortsinformationen sind sensibel, denn sie geben Einblick in viele Lebensbereiche einer Person und können auch weitere Personen betreffen. Das Bewusstsein darüber ist nicht nur im Privatleben angeraten, sondern auch im Arbeitsleben nötig. Es fehlt nicht nur an Transparenz, sondern Hersteller und Entwickler sollten insgesamt ihre Anwendungen so gestalten, dass nur die für den jeweiligen Zweck erforderlichen Daten übertragen und sie nicht zu anderen Zwecken ausgewertet werden.

7.5 Länderübergreifende Untersuchung von Wearables

Fitnessarmbänder und Smart Watches (sogenannte Wearables) erfassen inzwischen bei vielen Menschen umfassend ihre Aktivitäten und den Gesundheitszustand. Unter der Federführung der Kollegen des Bayerischen Landesamts für Datenschutzaufsicht und zusammen mit weiteren Datenschutzaufsichtsbehörden hat sich das ULD an einer bundesweiten Prüfung dieser Geräte beteiligt. Insgesamt wurden 16 Wearables von Herstellern, die ca. 70 % des Marktanteils in Deutschland abdecken, untersucht. Neben den Geräten wurden auch die zugehörigen Apps einer technischen und rechtlichen Analyse unterzogen.

Das ernüchternde Ergebnis: Kein Gerät erfüllt im Ergebnis vollständig die datenschutzrechtlichen Anforderungen. So hapert es schon an der Transparenz und Nachvollziehbarkeit der Datenverarbeitung. Viele Geräte übertragen die Daten der Nutzer über das Internet an unterschiedliche Stellen. Die oftmals nur pauschalen Datenschutzerklärungen liefern für die Betroffenen keine ausreichenden Informationen über Datenübermittlungen, Weitergaben an Dritte oder auch Verarbeitungszwecke. Dies ist umso gravierender, da es sich teilweise um besonders sensible Gesundheitsdaten handelt, die Aussagen über den Fitnesszustand des Nutzers ermöglichen und teilweise sogar Herzschläge erfassen. Viele Hersteller schweigen sich über Löschungsmöglichkeiten der Daten aus, was zumindest für die Fälle wichtig wäre, in denen ein Gerät verloren geht oder der Nutzer aus anderen Gründen die Datenerfassung beendet möchte.

Die Ergebnisse der gemeinsamen Prüfung können hier nachgelesen werden:

https://www.datenschutz-mv.de/datenschutz/themen/beschlue/91_DSK/Entschl-Wearables.pdf

Was ist zu tun?

Die Verbreitung von Wearables, insbesondere in Form von Smart Watches, nimmt zu. Es ist wichtig, dass die Hersteller der Geräte und Betreiber der Anwendungen die rechtlichen und technischen Anforderungen des Datenschutzes nachvollziehbar umsetzen und die Nutzerinnen und Nutzer über bestehende Risiken informieren.

7.6 Medienkompetenz für Schülerinnen und Schüler

Medienkompetenz gehört mittlerweile zu den notwendigen Kernkompetenzen in unserer Gesellschaft. Ein wesentlicher Bestandteil von Medienkompetenz ist Datenschutz: Wie kann man sich in der Informationsgesellschaft vor Risiken schützen? Und wie vermeidet man, dass man selbst zu einem Risiko für andere wird? Dies kann man nicht früh genug lernen.

Das ULD ist deswegen nicht nur Partner im Netzwerk Medienkompetenz Schleswig-Holstein und Mitglied der Lenkungsgruppe des Netzwerks Medienkompetenz Schleswig-Holstein, sondern unterstützt das Lernen von Medienkompetenz mit eigenen Schwerpunktaktivitäten für Kinder und Jugendliche sowie für Eltern und Lehrkräfte:

- Datenschutz-/Medienkompetenzkurse für Schüler „Entscheide DU, sonst tun es andere für Dich!“ ab 7. Klassenstufe
- Datenschutz-/Medienkompetenzkurse für Eltern „Entscheiden SIE, sonst tun es andere für Ihre Kinder!“
- Medienkompetenztage an Schulen für Schüler (7. und 8. Klassenstufe), Eltern und Lehrkräfte in Kooperation mit der Verbraucherzentrale Schleswig-Holstein, der Polizei (Bereich Prävention) und dem Institut für Qualitätsentwicklung an Schulen Schleswig-Holstein
- Regelmäßige Teilnahme an der jährlichen Eintagesveranstaltung „Medienkompetenztag Schleswig-Holstein“ mit Vorträgen, Workshops und Beratungsstand des ULD (Teilnehmer: Lehrkräfte), veranstaltet vom

Netzwerk Medienkompetenz Schleswig-Holstein und organisiert u. a. vom Institut für Qualitätsentwicklung an Schulen Schleswig-Holstein, dem Ministerium für Soziales, Gesundheit, Wissenschaft und Gleichstellung und der Medienanstalt Hamburg/Schleswig-Holstein

- Mitarbeit an dem Projekt „ElternMedien Lotsen – Medienpädagogische Elternabende gestalten“ in Zusammenarbeit mit dem Ministerium für Soziales, Gesundheit, Wissenschaft und Gleichstellung des Landes Schleswig-Holstein und dem Offenen Kanal Schleswig-Holstein
- Broschüre „Entscheide DU, sonst tun es andere für Dich!“ für Schülerinnen und Schüler, Eltern und Lehrkräfte
- Vorträge, Workshops und Veranstaltungen für Kinder, Jugendliche, Schülerinnen und Schüler, Pädagoginnen und Pädagogen, Lehrkräfte und Eltern u. a. in Kooperation mit anderen Partnern wie beispielsweise dem Landesbeauftragten für politische Bildung Schleswig-Holstein (z. B. die Veranstaltung „Nimmt Facebook uns die Wahl? Politische Meinungsbildung in sozialen Medien“) oder dem Offenen Kanal Schleswig-Holstein (z. B. am Safer Internet Day)

Was ist zu tun?

Medienkompetenz gehört verstärkt ins Bewusstsein unserer Gesellschaft. Bei Fragen mit Bezug zum Umgang mit Daten und zu Datenschutzrisiken hilft das ULD.

08

KERNPUNKTE

Selbstdatenschutz
Cloud Computing
Cybersicherheit
Big Data

8 Modellprojekte und Studien

Neben seinen Aufgaben zur Überwachung der Einhaltung der Datenschutzgesetze beteiligt sich das ULD aktiv an drittmittelgeförderten Projekten und Studien zu Datenschutzthemen. Jede Verarbeitung personenbezogener Daten bringt Risiken für die Betroffenen mit sich und muss datenschutzgerecht gestaltet werden. Die Datenschutz-Grundverordnung (DSGVO) verlangt in Artikel 25 nunmehr ausdrücklich Datenschutz durch Technikgestaltung und durch Voreinstellungen (englisch: „data protection by design and by default“). Danach sollen Aspekte des Datenschutzes bereits in einer frühen Entwicklungsphase Berücksichtigung finden.

Unserer Auffassung nach sind datenschutzfördernde Lösungen wichtig, damit die verantwortlichen Stellen ihrer Verantwortung tatsächlich nachkommen können und nicht die Betroffenen einem unbeherrschbaren Risiko aussetzen. Produkte und Dienstleistungen können oft deutlich datensparsamer und datenschutzfördernder ausgestaltet werden. Dies betrifft auch und insbesondere Bereiche, die konzeptionell problematisch für den Datenschutz sind und daher rechtskonform eingegrenzt werden müssen, beispielsweise Big-Data-Verarbeitung.

Zudem können datenschutzfördernde Lösungen Nutzerinnen und Nutzern Wege aufzeigen, um in Zeiten der zunehmenden Digitalisierung aller Aspekte des Lebens ihre Privatsphäre zu schützen. Unmittelbar tragen Projekte zum Selbstdatenschutz zu diesem Ziel bei.

Die Projekte werden am ULD durch das Innovationszentrum Datenschutz & Datensicherheit (ULD-i) koordiniert, das interessierten schleswig-holsteinischen Unternehmen und Hochschulen gern als Ansprechpartner für die Integration von Datenschutz und Datensicherheit in ihre Projekte und Produkte zur Verfügung steht.

ULD-i >>
Datenschutz innovativ

Im Berichtszeitraum hat sich das ULD wieder an einer Vielzahl von Projekten beteiligt. Das Themenspektrum umfasst Privatheit und selbstbestimmtes Leben (Tz. 8.1), Identitätenmanagement und Selbstdatenschutz (Tz. 8.2), Cloud Computing (Tz. 8.3), Cybersicherheit (Tz. 8.4), Big Data (Tz. 8.5) und das Internet der Dinge (Tz. 8.6).

8.1 Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt

Im „Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt“ – kurz Privacy-Forum – (35. TB, Tz. 8.1) geht es weiterhin um die Erforschung von Fragen rund um Privatheit und Datenschutz in einem Team, das Disziplinen wie Technik, Recht, Soziologie, Psychologie, Politologie, Wirtschaftswissenschaften und Ethik vereint. Das ULD vertritt in diesen Diskussionen die Perspektive einer Datenschutzaufsichtsbehörde, die besonders an praxistauglichen Lösungen interessiert ist.

In dem Forum Privatheit wurden mehrere White Paper erstellt, in denen das Forum kritische Positionen bezogen hat: zu Selbstdatenschutz, zum versteckten Internet (u. a. Internet der Dinge, Tz. 8.6), zu Privatheit und Datenflut in der neuen Arbeitswelt, zur Privatheit in öffentlichen WLANs und zur Datenschutz-Folgenabschätzung. Insbesondere das White Paper zur Datenschutz-Folgenabschätzung, die ab Mai 2018 verpflichtend für alle Datenverarbeitungen mit einem voraussichtlich hohen Risiko durchgeführt sein muss, ist auf große Resonanz gestoßen und hat die Diskussion in vielen Communities befruchtet.

In zusätzlichen Positionspapieren hat das Forum Privatheit zu wichtigen Themen, beispielsweise zur Datenschutz-Grundverordnung, Stellung genommen.

Allerdings hat die besonders umfangreiche Interdisziplinarität der Beschäftigung mit dem Thema „Privatheit“ gezeigt, dass sehr viel mehr Diskussionsbedarf besteht, als in der Zeit der Projektdauer erledigt werden konnte. Dies wird nunmehr vom Bundesministerium für Bildung und Forschung (BMBF) dadurch gewürdigt, dass das Projekt verlängert wird und weitere Arbeitsaufträge angegangen werden können,

um die aktuellen Debatten weiterhin inhaltlich und perspektivenübergreifend begleiten zu können. Dies wird im neuen Forum Privatheit geschehen, das zunächst bis Ende 2018 weiterhin durch das BMBF gefördert wird.

https://www.forum-privatheit.de/

Was ist zu tun?

Der interdisziplinäre Diskurs zu Privacy- und Datenschutz-Themen muss lösungsorientiert geführt werden, um Wege für die Praxis zu finden.

8.2 Identitätenmanagement und Selbstdatenschutz

Identitätenmanagement für den Selbstdatenschutz begleitet das ULD als Thema bereits seit vielen Jahren u. a. in den Projekten ABC4Trust, PrimeLife, PRIME und FIDIS (35. TB, Tz. 8.2). Im Offline-Alltag war und ist es für Menschen selbstverständlich, Informationen nur kontextbezogen preiszugeben. Der Arzt erfährt mehr oder andere Informationen als der Partner, der Rest der Familie oder eine Sportbekanntschaft. Ein pseudonymes Agieren im Netz ist daher keineswegs eine Anomalie gegenüber der Offline-Welt, sondern die konsequente Fortsetzung überbrachter sozialer Gepflogenheiten.

Identitätenmanagement

Unter Identitätenmanagement versteht man das Verwalten seiner verschiedenen Identitäten primär in der digitalen Welt. Die zugehörigen Datensätze enthalten teilweise Vornamen und Nachnamen, teilweise kommen sie mit Pseudonymen aus, die häufiger oder auch nur einmal verwendet werden. Ein fortschrittliches, datenschutzorientiertes Identitätenmanagement ermöglicht das komfortable Wechseln zwischen den digitalen Identitäten, das Generieren geeigneter neuer Identitäten und Transparenz darüber, welche Informationen man wem gegenüber preisgegeben hat.

Das Thema „Identitätenmanagement“ hat für den Datenschutz anhaltende Bedeutung. Auch unter Geltung der DSGVO gilt der Grundsatz der Datenminimierung, daher sind – soweit möglich – so wenige Daten wie möglich zu verarbeiten und diese so schnell wie möglich zu löschen, zu anonymisieren oder zu pseudonymisieren. Hauptverantwortlich für eine rechtskonforme Datenverarbeitung bleiben die Verantwortlichen. Unternehmen sind daher in der Verantwortung, neue datenschutzfördernde Lösungen zu prüfen und nach Möglichkeit einzusetzen.

Der grenzüberschreitende Einsatz von online nutzbaren Ausweisen war Thema im Projekt FutureID (Tz. 8.2.1), bei dem eIDs unter Nutzerkontrolle zum Einsatz kamen. Allerdings darf die Wahrnehmung von Datenschutzbelangen nicht auf die Betroffenen abgewälzt werden. Dennoch können Maßnahmen und Tools zum Selbstdatenschutz hilfreich sein, insbesondere im globalen Kontext. Hierzu hat das Bundesministerium für Bildung und Forschung ein eigenes Forschungsprogramm im Bereich IT-Sicherheit mit dem Namen „Selbstbestimmt und sicher in der digitalen Welt“ aufgelegt. Technische Selbstdatenschutzmöglichkeiten werden in den Projekten AN.ON-Next (Tz. 8.2.2) und AppPETs (Tz. 8.2.3) mit dem Ziel einer weniger beobachtbaren Kommunikation und verbesserter Anwendungen sowie im Projekt VVV (Tz. 8.2.4) für eine laientaugliche und sichere Ende-zu-Ende-Verschlüsselung von E-Mails entwickelt. Mit solchen Maßnahmen können Betroffene einer Verkettung ihrer Informationen entgegenwirken und so ihr Informations- und Identitätenmanagement verbessern.

8.2.1 Projekt FutureID – europaweite Nutzung von Identitätsnachweisen

Europaweit gibt es eine Vielzahl elektronischer Identitätsnachweise, kurz eIDs. Neben elektronischen Ausweisdokumenten werden auch Bank- und Kreditkarten, Sozialversicherungsausweise, Softwarezertifikate und weitere Identitätsnachweise, z. B. von Hochschulen, genutzt. Um online einen freien Austausch von Waren und Dienstleistungen und E-Government-Dienste zu ermöglichen, müssen sich die Nutzenden grenzüberschreitend authentisieren können. Schon aus Kostengründen ist es unmöglich, dass alle möglichen Empfänger – also Händler, Dienstleister und Behörden – die Infrastruktur für das Auslesen sämtlicher in der Union anerkannter eID-Lösungen vorhalten. In diesem inhomogenen Feld eine datenschutzgerechte Lösung für eine grenzüberschreitende Authentifizierung und – wo erforderlich – Identifizierung zu entwickeln, war Inhalt des FutureID-Projekts, in dem das ULD zusammen mit 18 weiteren Partnern aus ganz Europa gearbeitet hat (35. TB, Tz. 8.2.2). Das Projekt ist durch die Europäische Kommission gefördert worden.

Die naive Lösung bestünde in der Einrichtung einer zentralen Stelle, die als Mittler Ausweisdaten ausliest und an den Empfänger im Drittland übermittelt. Diese Stelle würde dabei sämtliche Daten der betroffenen Person einschließlich der Informationen erfahren, gegenüber welchen Diensten sich die Betroffenen im Ausland authentifiziert haben. Sie könnte auch umfangreiche Interessenprofile erstellen – ein Datenschutz-Albtraum.

Die im FutureID-Projekt entwickelte Alternative setzt auf eine Vielzahl von frei wählbaren Vermittlern (Brokern). So wird es möglich, nur solche Attribute offenzulegen, die für eine Transaktion auch erforderlich sind. Dies ermöglicht beispielsweise eine anonyme Verifikation von Alter oder Wohnort. Während der neue deutsche Personalweis diese Art der Datenminimierung bereits von Haus aus unterstützt, handelt es sich um einen wertvollen Mehrwert für Nutzerinnen und Nutzer anderer eID-Arten, indem u. a. die im EU-Ausland verbreiteten Ausweis-, Sozialversicherungs- und Bürgernummern gefiltert werden können. Schließlich unterstützt die FutureID-Architektur in weitem Maße die Nichtverkettung und die Ausstellung datenschutzfördernder attributbasierter Credentials (35. TB, Tz. 8.2.1) durch die Broker zur weiteren Verwendung durch die Nutzenden.

Identity Brokerage (Identitätsvermittlung)

Die Verwendung sogenannter Identitätsvermittler (Identity Broker) ermöglicht es Nutzenden, ihre vorhandenen eIDs auch für Dienste zu nutzen, die diese eIDs nicht selbst ausgestellt haben. So könnte mithilfe passender Identitätsvermittler beispielsweise ein elektronischer Personalausweis dazu dienen, einem Arzt in Italien direkten Zugriff auf eine in Frankreich vorgehaltene Patientenakte zu ermöglichen. Zudem ließen sich datenschutzfreundliche attributbasierte Nachweise, z. B. über das Alter einer Person, direkt aus einem geeigneten eID-Ausweis ableiten und über passende Identitätsvermittler auch dann einsetzen, wenn der Diensteanbieter die direkte Verwendung des eID-Ausweises nicht unterstützt. Die Hauptaufgabe der Identitätsvermittler ist dabei die technische Konvertierung der Identitäts- bzw. Attributnachweise zwischen zwei oder mehr Beteiligten unter Einhaltung der rechtlichen Rahmenbedingungen.

http://www.futureid.eu/

Was ist zu tun?

Öffentliche und nichtöffentliche Stellen sollen bei der Auswahl von Authentifizierungsdienstleistern darauf achten, dass diese die Nichtverkettung von einzelnen Vorgängen bereits konzeptionell unterstützen. Dies kann auch für das Vertrauen von Bürgerinnen und Bürgern in E-Government-Dienste wichtig werden.

8.2.2 Projekt AN.ON-Next – praktikable und rechtssichere Anonymität im Internet

In dem durch das BMBF geförderten Projekt „AN.ON-Next – Anonymität Online der nächsten Generation“ werden in den nächsten Jahren effiziente datenschutzfreundliche Lösungen für das Internet entwickelt. Dazu gehört eine weitgehende Unbeobachtbarkeit des Surfverhaltens von Nutzerinnen und Nutzern gegenüber Webseiten- und Diensteanbietern sowie anderen lokalen Angreifern. Notwendig ist dabei, dass die Dienstqualität nicht spürbar eingeschränkt wird, sodass auch Dienste genutzt werden können, die auf Kommunikation in Echtzeit angewiesen sind.

Die Umsetzung der Anonymisierung soll dabei so weit wie möglich von der Internetinfrastruktur erbracht, also auf den Internetserviceprovider verlagert werden. Dadurch wird eine Form der Anonymisierung ermöglicht, die kein eigenes Zutun auf Nutzerseite erfordert. Im Projekt werden dabei in Zusammenarbeit u. a. mit einem Internetzugangsanbieter sowohl der klassische Übertragungsweg als auch Mobilfunkstandards in den Fokus genommen. Untersucht wird, wie Standards wie z. B. IPv6 und 5G datenschutzfördernder als bisher eingesetzt werden können. Auch wenn die eingesetzten Lösungen weitestgehend ohne vorherige Konfiguration der Nutzenden realisiert werden, soll ihnen stets die Möglichkeit gegeben werden, den tatsächlich erreichten Schutz bei Bedarf nachvollziehen und überprüfen zu können.

https://datenschutzzentrum.de/projekte/anonnext/

8.2.3 Projekt AppPETs – Datenschutz eingebaut in Smartphone-Anwendungen

Das Projekt „AppPETs – Datenschutzfreundliche Smartphone-Anwendungen ohne Kompromisse“ soll Entwicklern die Integration datenschutzfreundlicher Technik in Smartphone-Apps erleichtern, indem Funktionen mit eingebautem Datenschutz für wiederkehrende Standard-Anwendungsfälle bereitgestellt werden. Damit soll der jetzige Zustand verbessert werden, in dem eine Vielzahl von Apps wesentlich mehr Daten erhebt und übermittelt, als es zur jeweiligen Diensterbringung notwendig wäre.

Mobile Apps

Der Begriff „Mobile App“ steht für „Mobile Application“, d. h. eine Anwendung, die üblicherweise auf einem Smartphone oder einem Tablet-Computer installiert und damit mobil verwendet wird. Ein Teil der Apps ist bereits bei der Auslieferung der Geräte vorhanden; zusätzliche Apps können aus den für das Gerät passenden „App Stores“, also direkt per Smartphone oder Tablet zugreifbaren Online-Shops, heruntergeladen werden. Einige Apps kosten Geld, andere sind kostenlos. Vielfach greifen die Apps auf Daten und Funktionen auf dem Gerät zu – nicht immer ist dies für ihre Funktionalität und ihren Zweck erforderlich.

Während Nutzerinnen und Nutzer klassischer Webbrowser zumindest zu einem gewissen Umfang die Datenströme nachvollziehen können, laufen die Prozesse bei der Nutzung von Smartphone-Apps zu einem großen Teil im Verborgenen ab. Entwickler von Smartphone-Apps greifen derzeit bei der Programmierung von Apps häufig aus Bequemlichkeit, Zeitdruck oder mangels funktionierender Alternativen auf Softwarebibliotheken zurück, die datenschutzrechtlich bedenkliche und stark verbesserungsfähige Funktionen enthalten.

Das Projekt AppPETs, das im Jahr 2016 gestartet ist und durch das BMBF gefördert wird, will durch eine Reihe an Lösungen zeigen, dass die Implementierung auch komplexer datenschutzfreundlicher Technik möglich ist. Ziel ist es, die entwickelten Lösungen in einer offenen und freien Softwarebibliothek zur Verfügung zu stellen. Außerdem sollen sich solche Apps, die sich einer Kontrolle ihrer Software unterziehen und die datenschutzfördernden Funktionen einbauen, durch ein Siegel auszeichnen können. Schließlich soll den Nutzenden eine Möglichkeit an die Hand gegeben werden, um selbst zu kontrollieren, ob sich eine App nach der Erstinstallation oder nach einem Update an die durch das Siegel bestätigten Vorgaben hält.

https://datenschutzzentrum.de/projekte/apppets/

8.2.4 Projekt VVV – Verschlüsselung einfacher machen

Deutschland will „Verschlüsselungsland Nummer 1“ werden – das steht jedenfalls in der Digitalen Agenda des Bundes. Ende-zu-Ende-Verschlüsselung ist der gegenwärtig gangbare und umsetzbare Weg für eine sichere Kommunikation von Bürgerinnen und Bürgern untereinander sowie mit öffentlichen und nichtöffentlichen Stellen. Bisher fehlt es an einer Lösung, um die dafür benötigten öffentlichen Schlüssel der Kommunikationspartner in einer einfachen und zugleich hinreichend verifizierten Form zu erlangen, weil es an einer entsprechenden Public-Key-Infrastruktur (PKI) fehlt.

Durch das vom BMBF geförderte Projekt „VVV – Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln“ soll die Verteilung öffentlicher Verschlüsselungsschlüssel erleichtert werden, um Ende-zu-Ende-Verschlüsselung in der E-Mail-Kommunikation allen Nutzergruppen zu ermöglichen. Zusammen mit den Projektpartnern wird eine Erweiterung für das E-Mail-Programm Thunderbird bzw. für den Browser der Nutzer entwickelt.

Ende-zu-Ende-Verschlüsselung ist längst noch kein Standard in der E-Mail-Kommunikation. Obwohl es seit Jahren etablierte Programme zur Verschlüsselung gibt, beschränken sich viele Nutzer auf die Verwendung einer Transportverschlüsselung auf der Strecke zwischen Endrechner und E-Mail-Provider für ihren E-Mail-Verkehr. Eine flächendeckende Ende-zu-Ende-Verschlüsselung, die den Inhalt der E-Mails durchgehend vor unbefugter Kenntnisnahme schützt, konnte sich bisher nicht durchsetzen, obwohl Meldungen über schwerwiegende Sicherheitslücken und erfolgreiche Angriffe auf Server verschiedenster Dienste immer wieder Schlagzeilen machen. Das Problem der Schlüsselverteilung ist auf mehreren Ebenen zu lösen. Dies beinhaltet sowohl die Veröffentlichung als auch eine effiziente Suche nach den benötigten öffentlichen Schlüsseln sowie die Etablierung einer vertrauenswürdigen Bezugsquelle.

Ende-zu-Ende-Verschlüsselung

Ende-zu-Ende-Verschlüsselung bedeutet die Verschlüsselung von übertragenen Daten über den gesamten Übertragungsweg vom Sender bis zum Empfänger, ohne dass zwischendurch die Verschlüsselung aufgebrochen werden kann.

Das Projekt VVV führt die E-Mail-Provider als zentrale Verteilungsinstanz für öffentliche Schlüssel ihrer Kunden ein. Die Überlegung dahinter: Da die Nutzer ihrem E-Mail-Provider in Bezug auf ihre E-Mail-Kommunikation bereits vertrauen, können sie ihm auch die Veröffentlichung ihrer öffentlichen Schlüssel anvertrauen. Der Bezug eines öffentlichen Schlüssels wird ebenfalls einfacher und transparenter, denn die Domain-Endung der E-Mail-Adresse des Empfängers zeigt an, wo der öffentliche Schlüssel zu finden ist. Die im VVV-Projekt entwickelten Plug-ins für E-Mail-Clients vereinfachen die Suche zusätzlich durch Übernahme des Schlüsselbezugs und Bereitstellung an die E-Mail-Anwendung.

Da die öffentlichen Schlüssel nur beim E-Mail-Provider der Nutzerinnen und Nutzer hinterlegt sind, bekommen die Nutzenden zudem die Möglichkeit, ihre öffentlichen Schlüssel jederzeit auszutauschen oder zu löschen. Damit behalten sie die Kontrolle über die Veröffentlichung ihrer im öffentlichen Schlüssel enthaltenen personenbezogenen Daten.

Kernaufgabe des ULD im VVV-Projekt ist die Bewertung der entwickelten Erweiterung hinsichtlich der datenschutzrechtlichen Folgen und möglicher Risiken für die Betroffenen. Das ULD trägt mit seiner Erfahrung aus der Datenschutzpraxis dazu bei, dass das Prinzip „Datenschutz by Design“ kontinuierlich in die Entwicklung der Erweiterung einfließt.

https://datenschutzzentrum.de/projekte/vvv/

Was ist zu tun?

Anreize für datenschutzfreundliche Technik, wie in Artikel 25 und 32 DSGVO gefordert, sind notwendig. Dazu gehört, dass Ende-zu-Ende-Verschlüsselung auf dem digitalen Weg im Kontakt zwischen Bürger und Staat Vorbildfunktion einnehmen und selbstverständlich werden sollte.

8.2.5 Projekt PARADISE – Selbstdatenschutz für die Dopingkontrolle im Sport

Im Jahr der Olympischen Spiele war das Thema „Doping“ in aller Munde, beispielsweise wegen deutlich gewordener Mängel der Dopingkontrollpraxis in einigen Staaten. Weniger bekannt ist indes das hiesige Kontrollprozedere, dem sich rund 7000 deutsche Spitzenathletinnen und -athleten unterwerfen müssen (35. TB, Tz. 2.5).

Für die Planung und Anbahnung von Trainingskontrollen setzt die Stiftung Nationale Anti-Doping-Agentur Deutschland (NADA) auf das Anti-Doping-Verwaltungs- und Planungssystem (ADAMS). Dort müssen die deutschen Athletinnen und Athleten quartalsweise im Voraus angeben, wo sie an jedem kommenden Tag für Kontrollen angetroffen werden können. Diese Angaben umfassen u. a. die exakte Beschreibung der Adresse, wo sie zu Bett gehen werden, oder solche Orte, die von ihnen regelmäßig aufgesucht werden. Damit sind die Athletinnen und Athleten gezwungen, den Akteuren im Dopingkontrollsystem intimste Einblicke in ihr Privatleben zu gewähren, ohne den Inhalt oder das Ausmaß dessen beschränken zu können.

Diesen Missstand nahmen verärgerte Athleten zum Anlass, das Projekt „PARADISE – Privacy-enhancing And Reliable Anti-Doping Integrated Service Environment“ ins Leben zu rufen, um die Kontrolle über ihre Daten zurückzugewinnen. Durch den Einsatz von datenschutzfördernder Technik soll ein effektives und datenschutzgerechtes Anti-Doping-Managementsystem entwickelt werden. Dieses soll u. a. ein Wearable enthalten, mit dem Athletinnen und Athleten anlassbezogen für Dopingkontrollen aufgefunden werden können, ohne dass ständig ihre Aufenthaltsorte nachverfolgt (Tracking) und ihre Bewegungsprofile aufgezeichnet werden. Zu Transparenzzwecken sollen die Sportlerinnen und Sportler im Nachhinein zudem konkret einsehen können, wer wann welche Daten zur Umsetzung eines konkret erteilten Prüfauftrags eingesehen hat.

Das ULD hat innerhalb dieses vom BMBF geförderten Projekts die datenschutzrechtlichen Anforderungen für ein solches System erarbeitet und ist für deren datenschutzrechtliche Evaluierung im Projektverlauf verantwortlich. Diese datenschutzfreundlichere Lösung sollte national oder besser noch international Berücksichtigung finden. Dadurch lässt sich das bisherige System verbessern.

https://datenschutzzentrum.de/projekte/paradise/

Was ist zu tun?

Dem Recht auf informationelle Selbstbestimmung der Athletinnen und Athleten muss auch im komplexen Anti-Doping-Kampf Rechnung getragen werden.

8.3 Projekt SPLITCloud – mehr Kontrolle beim Cloud Computing

In dem vom BMBF geförderten Projekt „SPLITCloud – Secure Partitioning of application Logic In a Trustworthy Cloud“ wurde bis März 2017 eine Lösung entwickelt, die es ermöglicht, auch innerhalb von Cloud-Umgebungen durch gezielt eingesetzte Verschlüsselung Zugriffe auf die verarbeiteten Daten zu beschränken. Dieses Konzept dient der Beherrschbarkeit des IT-Systems und wurde unter dem Motto „Teile und herrsche“ im vergangenen Tätigkeitsbericht vorgestellt (35. TB, Tz. 8.3.2).

Die Daten befinden sich in der SPLITCloud-Lösung in einer „Trusted Virtual Domain“ (TVD), die einem Mandanten zugewiesen ist. Dadurch sollen sowohl die Systembetreiber im Rechenzentrum wirksam vom Zugriff auf die verarbeiteten Daten ausgeschlossen werden als auch mögliche Dienstleister, die auf Basis einer selbst oder durch Unterauftragnehmer bereitgestellten Cloud-Infrastruktur Software als Dienstleistung anbieten. Ein zentraler, für die TVD bestellter Verwalter muss dabei Änderungen an der Hardware und am Softwaresystem freigeben sowie Zugriffe autorisieren. Diese Rolle kann auch einer Person der verantwortlichen Stelle übertragen werden, womit Kontrolle und Entscheidungskompetenz maßgeblich in der Auftragskette zurück an den – dem Gesetz nach dafür zuständigen und haftbaren – Verantwortlichen verlagert werden. In der Gesamtbetrachtung verliert eine solche Lösung zwar in Teilen an der im Bereich des Cloud Computing besonders geschätzten Flexibilität, kann aber durch die Rückübertragung der Kontrolle und Transparenz über die Verarbeitung ein zentraler Baustein im Kanon der technischen und organisatorischen Maßnahmen sein, um gegebenenfalls auch einen erhöhten Schutzbedarf zu erfüllen.

Cloud Computing

Cloud Computing bedeutet übersetzt: „Datenverarbeitung in der Wolke“. Damit sind Server gemeint, die passend für die jeweiligen Anforderungen Ressourcen wie Speicherplatz, Rechenleistung oder Software über Rechnernetze bereitstellen. Bei der Nutzung solcher Cloud-Dienstleistungen müssen verantwortliche Stellen gewährleisten, dass sie weiterhin ihre Verantwortung über die Datenverarbeitung ausüben und nicht die Kontrolle vollständig aus der Hand geben. Der Verarbeitungsort in einer Cloud ist durch die dynamische und lastoptimierende Verarbeitung in der Regel nicht fest, ist aber wesentlich für die Bestimmung des Rechtsraums und etwaiger Zugriffe durch staatliche Stellen.

https://datenschutzzentrum.de/projekte/splitcloud/

Was ist zu tun?

Sollen personenbezogene Daten in der Cloud verarbeitet werden, muss der Verantwortliche die Kontrolle behalten. Technische Maßnahmen sind dabei effektiver als rein organisatorische Vorkehrungen.

8.4 Cybersicherheit und Datenschutz

Das technische Fundament unserer Wissensgesellschaft ist die Informationstechnik. Leider ist dieses Fundament brüchig – weil beim Design der Technik nicht auf alle notwendigen Anforderungen geachtet wurde, weil es teilweise wichtiger schien, schnell auf den Markt zu kommen, statt sorgfältiger vorzugehen, und weil sogar Sicherheitslücken gezielt eingebaut wurden (Tz. 2.3). Vertrauenswürdige Informationstechnik ist nicht der Normalfall. Kein Wunder, dass Cybersicherheit vermehrt in den Fokus der Öffentlichkeit gerät.

Dies erzeugt Handlungsdruck in der Politik und erhöht die Gefahr von übereilten Maßnahmen, die nicht geeignet sind, um die Sicherheit der

Bürgerinnen und Bürger zu gewährleisten, und zugleich wesentliche Einschnitte in die Grund- und Bürgerrechte bedingen. Insbesondere zeigt sich, dass viele Lösungen mit (vermeintlich) mehr Sicherheit die Privatsphäre erheblich beeinträchtigen können. Aus diesem Grund begleitet das ULD im Bereich der Cybersicherheit einige Projekte, die bewusst die Einbeziehung datenschutzrechtlicher Aspekte forcieren: Im Projekt ITS.APT (Tz. 8.4.1) wird der Faktor Mensch als Risiko für die IT-Sicherheit betrachtet. Das EIDI-Projekt (Tz. 8.4.2) befasst sich mit Möglichkeiten für eine datenschutzgerechte und effektive Information der Betroffenen nach einem Identitätsdiebstahl. Das Projekt CANVAS (Tz. 8.4.3) zielt darauf ab, einen breit vernetzten Expertenkreis zu schaffen, der die Perspektiven von Informationssicherheit, Ethik und Recht zusammenführt.

8.4.1 Projekt ITS.APT – Stärken des Bewusstseins für IT-Sicherheit

Kritische Infrastrukturen wie Krankenhäuser oder Wasserwerke gehören zu den besonders verletzlichen Zielen bei Cyberangriffen. Dabei setzen Angreifer nicht nur auf Hacking, sondern auch auf Phishing-E-Mails oder Trojaner, die von Beschäftigten versehentlich installiert werden. Während es allmählich Fortschritte beim Schutz der technischen IT-Infrastruktur gibt, ist der menschliche Faktor bisher trotz aller Schulungsbemühungen und umfangreicher Berichterstattungen weiterhin ein schwaches Glied in der Schutzkette.

Phishing

Das Kunstwort „Phishing“ bezeichnet einen Angriffstyp im Internet, um über E-Mails oder gefälschte Webseiten an wichtige Daten der Nutzerinnen und Nutzer zu gelangen – ein „Fischen“ nach den Daten. Phishing-Angriffe sind für einen einzelnen Nutzer häufig nur schwer zu erkennen und können großen Schaden anrichten, wenn der Betroffene darauf hineinfällt.

Das vom BMBF geförderte Projekt „ITS.APT – IT-Security Awareness Penetration Testing“ verfolgt das Ziel, das IT-Sicherheitsbewusstsein von Beschäftigten durch Tests und Schulungen zu stärken. Dabei liegt ein Fokus auf der datenschutzgerechten Ausgestaltung dieser Maßnahmen, insbesondere im Bereich des Beschäftigtendatenschutzes bei der Erhebung der Schulungsbedarfe durch Testmaßnahmen. Die Testmaßnahmen finden ausschließlich auf der IT-Infrastruktur des Arbeitgebers statt, sodass persönliche Belange nicht zwingend betroffen sind. Dennoch bedarf es unserer Auffassung nach der Einbeziehung bestehender Kontrollmechanismen wie des Betriebs- oder Personalrats. Es dürfen den Beschäftigten keine Nachteile durch die Testergebnisse zum Sicherheitsbewusstsein entstehen. Insoweit unterliegen die Ergebnisse einer strengen Zweckbindung hinsichtlich der Verbesserung der IT-Sicherheit durch Aufdecken von Schwächen und Spezifizierung des Schulungsbedarfs des Personals. Die zu entwickelnden Lösungen sollen die Datenschutzanforderungen technisch und organisatorisch umsetzen.

https://datenschutzzentrum.de/projekte/its-apt/

Was ist zu tun?

Beschäftigte werden oft unwillentlich zu Werkzeugen der Angreifer. Schulungen zu IT-Sicherheit und Datenschutz sollten optimal auf die Bedürfnisse vor Ort zugeschnitten werden. Personal- und Betriebsräte sollten Maßnahmen wie Tests der Beschäftigten und darauf aufbauende Schulungen vorab und während der Durchführung kontrollieren.

8.4.2 Projekt EIDI – korrekte und hilfreiche Benachrichtigung von Betroffenen nach einem Cybervorfall

Große Mengen von Identitätsdaten, teils mit E-Mail-Adressen, Passwörtern oder Konto- und Kreditkarteninformationen, finden regelmäßig ihren Weg in das Netz und stehen für einen Missbrauch zur Verfügung. Quellen sind Angriffe auf unsichere IT-Anlagen von Datenverarbeitern, illoyale Mitarbeiter oder sonstige Datenpannen. Solche Daten werden von Kriminellen massenhaft gesammelt, verkauft und im Rahmen von Identitätsmissbrauch zum Betrug und zu anderen Delikten verwendet. Identitätsmissbrauch stellt ein Risiko für die Betroffenen dar.

Identitätsdiebstahl

Unter Identitätsdiebstahl versteht man das Agieren unter der Identität einer anderen Person, beispielsweise zum Zwecke des Betrugs oder um den Ruf des rechtmäßigen Inhabers zu schädigen. Dabei handelt es sich um einen Missbrauch von personenbezogenen Daten, beispielsweise Nutzername und Passwort, Geburtsdatum, Anschrift, Bankkonto- oder Kreditkartennummern.

Natürlich gilt es, an der Ursache anzusetzen, um dieses Problems Herr zu werden, doch ob sich das Problem „Identitätsdiebstahl“ jemals vollständig ausrotten lässt, ist fraglich. Bundesdatenschutzgesetz, Landesdatenschutzgesetz und die Datenschutz-Grundverordnung fordern in solchen Fällen eine verständliche Unterrichtung der Betroffenen und der Aufsichtsbehörde, denn ohne Information über Sicherheitsvorfälle kann man sich noch viel schwerer dagegen zur Wehr setzen. Nicht immer wissen die verantwortlichen Stellen aber überhaupt von dem Problem, dass Daten ihrer Kundinnen und Kunden kopiert wurden und sich als Angebot im Netz wiederfinden. Wenn solche Datensammlungen gefunden werden, ist häufig der Ursprung der Daten nicht offensichtlich. Wie soll dann vorgegangen werden, um die Betroffenen zu warnen?

Das Projekt „EIDI – Effektive Information nach digitalem Identitätsdiebstahl“ beschäftigt sich mit den Möglichkeiten und den Bedingungen der Recherche und Analyse solcher Daten. Das ULD arbeitet seit Anfang 2017 zusammen mit staatlichen Stellen, Forschungspartnern und Vertretern von verantwortlichen Stellen im EIDI-Projekt mit, das vom BMBF gefördert wird. Ziel ist die verständliche Information der Betroffenen über den Vorfall nebst konkreten Hinweisen für die Abwehr weiterer Risiken, die mit dem Missbrauch der kompromittierten digitalen Identität einhergehen. Für eine zielgerichtete Warnung ist u. a. die Ermittlung der Qualität der Datensammlung erforderlich. So bestimmen u. a. Alter, Genauigkeit und Granularität der Daten maßgeblich das Risiko für einen erfolgreichen Missbrauch.

Ist eine verantwortliche Stelle bekannt, deren Daten abhandengekommen sind, ist diese bei Vorliegen eines hohen Risikos für die Betroffenen verpflichtet, die Benachrichtigung der Aufsichtsbehörde und der Betroffenen unverzüglich zu veranlassen. Lässt sich auf die Quelle der Daten nicht zurückschließen, ist rechtlich zu klären, wer eine derartige Unterrichtung durchführen darf oder muss. Soweit auf Basis der Datensammlung selbst keine Kontaktaufnahme mit den Betroffenen erfolgen kann, besteht möglicherweise Bedarf der Verkettung mit bestehenden Datenbanken, um eine Unterrichtung zu ermöglichen – jedoch sind bislang die Rechtsgrundlagen der Datensammlung und -verkettung für derartige Zwecke ungeklärt. Das Projekt untersucht, inwieweit ergänzende gesetzgeberische Aktivität auf europäischer oder nationaler Ebene erforderlich ist.

Als weitere Komponente befasst sich das Projekt mit den Anforderungen an eine verständliche und umfassende Benachrichtigung der Betroffenen. Bei der Gestaltung dieser Benachrichtigungen muss darauf geachtet werden, dass sie ernst genommen wird, die nötigen Informationen vermittelt und auch Laien animiert werden, die erforderlichen Maßnahmen zur Minimierung des Risikos zu ergreifen, damit keine schlimmen Folgen entstehen.

https://datenschutzzentrum.de/projekte/eidi/

Was ist zu tun?

Datensammlungen im Netz sind ein Thema der Cybersicherheit und des Datenschutzes. Maßnahmen für den Schutz der Betroffenen müssen rechtskonform ausgestaltet werden.

8.4.3 Projekt CANVAS – Cybersicherheit zwischen Technik, Ethik und Recht

Das von der Europäischen Kommission geförderte Projekt „CANVAS – Constructing an Alliance for Value-driven Cybersecurity“ führt Experten in einem Netzwerk für Cybersicherheit zusammen, in dem Technikentwickler mit Rechtsexperten, Ethikern und Sozialwissenschaftlern in den Dialog gebracht werden. Die Ergebnisse werden den Entscheidern in Europa und den Mitgliedstaaten zur Verfügung gestellt.

Die wachsende Komplexität der digitalen Welt gehört zu den Ursachen für Cybersicherheitsrisiken, die sich global auswirken. Um dem zu begegnen, reichen eindimensionale Lösungen nicht aus. Vielmehr müssen Grundrechte und zentrale Werte wie Gleichbehandlung, Fairness und Privatsphäre berücksichtigt werden, um vertrauenswürdige Infrastrukturen und Systeme zu erhalten. Andernfalls könnten die Bürgerinnen und Bürger das Vertrauen in die digitale Infrastruktur verlieren. Um sich dieser Herausforderung zu stellen, hat die Europäische Kommission das CANVAS-Projekt damit beauftragt herauszufinden, wie Cybersicherheit mit diesen fundamentalen Grundrechten und europäischen Werten in Einklang gebracht werden kann. Innerhalb der nächsten drei Jahre wird das CANVAS-Projekt Interessenvertreter aus drei zentralen Bereichen der europäischen digitalen Agenda – Gesundheit, Business/Finanzen sowie Polizei/nationale Sicherheit – zusammenbringen. Diese interdisziplinären Expertinnen und Experten werden gemeinsam die Herausforderungen und potenzielle Lösungen diskutieren. Hierbei wird ein besonderer Fokus auf ethischen Fragen aus Wissenschaft und Industrie liegen, die in diversen Workshops intensiv behandelt werden.

Das ULD hat in diesem Projekt die Aufgabe, die datenschutzrechtlichen Aspekte von Cybersecurity aufzuzeigen und die Standpunkte staatlicher Akteure, wie etwa der Aufsichtsbehörden, darzulegen. Damit bringen wir eine breite Wissensbasis über die Datenschutzprobleme sowie über Lösungsansätze aus Datenschutzsicht im Kontext von Cybersecurity in die Diskussion.

https://datenschutzzentrum.de/projekte/canvas/

Was ist zu tun?

Cybersecurity berührt nicht nur den technischen und polizeilichen Bereich, sondern wirkt sich in den Domänen Ethik, Recht und Geisteswissenschaften aus. Hier ist nach gemeinsamen Lösungen zu suchen, die mit den europäischen Grundwerten im Einklang stehen.

8.5 Big Data, soziale Netzwerke und Datenschutz

Unaufhaltsam kommen technische Entwicklungen wie Big Data und das semantische Web auf uns zu. Die Verarbeitung und Verkettung großer Datenmengen birgt für Betroffene besondere Risiken. An die Verantwortlichen für den Betrieb solcher Prozesse werden daher vom Bundesdatenschutzgesetz (BDSG), den Landesdatenschutzgesetzen (LDSG) und künftig von der DSGVO zu Recht hohe Anforderungen gestellt. Gleichzeitig ist der politische Wille unverkennbar, die in Wirtschaft und Forschung beschworenen Mehrwerte von Big-Data-Analy-

sen zu heben. Es gilt daher, Wege aufzuzeigen, in denen die Anforderungen des Datenschutzrechts bei der gewünschten Datenverarbeitung effektiv eingebracht werden. Das ULD beteiligt sich an einem Projekt zur Big-Data-Auswertung für die Gestaltung von Reisewarnungen (Tz. 8.5.1), beim Einwilligungsmanagement im semantischen Netz (Tz. 8.5.2) und im Rahmen der Strafverfolgung (Tz. 8.5.3).

8.5.1 Projekt iTESA – Reisewarnungen auf Grundlage von sozialen Netzwerken

Das Anfang 2015 gestartete Projekt „iTESA – intelligent Traveller Early Situation Awareness“ beschäftigt sich mit der Nutzung von Big Data im Kontext zielgruppengenauer Reisewarnungen. Im Rahmen des Projekts, das vom Bundesministerium für Wirtschaft und Energie gefördert wird, erarbeitet das ULD Anforderungen für die Konzeption, Umsetzung und den Betrieb von Big-Data-Anwendungen. Das Hauptaugenmerk liegt dabei auf „Datenschutz by Design“, also auf der Implementierung von Datenschutzmaßnahmen bereits von Anfang an.

Big Data

„Big Data“ umfasst die Analyse von großen Datenmengen in unterschiedlichen Formaten. Ziel ist das Aufzeigen von Korrelationen innerhalb dieser Daten. Häufig verwendet man für die Analyse bestehende Datensammlungen, die für andere Zwecke angefallen sind. Vielfach beachten Big-Data-Anwendungen das Zweckbindungsprinzip nicht. Weitere Probleme bestehen in einer mangelhaften Datenbasis oder beim Verwechseln von Korrelation und Kausalität.

Ziel des iTESA-Projekts ist die Konzeption und Umsetzung eines automatischen Frühwarnsystems für Reisende, das in Echtzeit entweder im Vorwege einer geplanten Reise oder in deren Verlauf über mögliche Risiken informiert. Diese Risiken sollen durch Analyse zahlreicher Quellen gewonnen werden und können beispielsweise über Epidemien, Naturkatastrophen oder sonstige Gefährdungslagen informieren. Damit soll es den Reisenden ermöglicht werden, Vorkehrungen zur Umgehung der erkannten Risiken zu treffen. Auch sollen sie über den Verlauf der betreffenden Ereignisse auf dem Laufenden gehalten werden. Die Risiken werden auf Grundlage einer semantischen Auswertung der erhobenen Daten erkannt und dem Reisenden bei einer Relevanz für den jeweiligen Reiseort oder die Reiseroute auf dem mobilen Endgerät angezeigt.

Das ULD begleitet die Projektpartner bei der Konzipierung der jeweiligen Komponenten nach den Grundsätzen von „Datenschutz by Design“. Daneben werden im Rahmen der datenschutzrechtlichen Betrachtung der Datenverarbeitungsvorgänge des iTESA-Systems die neuen Regelungen von DSGVO und der ePrivacy-Verordnung Berücksichtigung finden. Kernfragen umfassen hier die Zulässigkeit einer Erhebung öffentlicher Informationen aus dem Netz sowie die zur weiteren Verarbeitung erforderlichen Maßnahmen. Für Big-Data-Projekte unter Geltung der DSGVO werden vor allem Transparenzanforderungen und die Umsetzung der Betroffenenrechte eine Herausforderung darstellen.

https://datenschutzzentrum.de/projekte/itesa/

Was ist zu tun?

Big Data verspricht der Wirtschaft und Politik das Heben von großen Datenschätzen. Im Rechtsstaat dürfen dabei jedoch die Grundrechte Betroffener nicht außer Acht gelassen werden. Dazu gehört, dass durch geeignete Maßnahmen sicherzustellen ist, dass die Datenverarbeitung rechtmäßig ist und die Prinzipien von Datenminimierung und Nichtverkettbarkeit ebenso wie Transparenz und Intervenierbarkeit ausreichende Berücksichtigung finden.

8.5.2 Projekt SPECIAL – Transparenz- und Einwilligungsmanagement für das semantische Netz

Seit Jahresbeginn 2017 forscht das von der Europäischen Kommission geförderte Projekt „SPECIAL – Scalable Policy-awarE linked data arChitecture for prIvacy, trAnsparency and compLiance“ an einer Unterstützung Verantwortlicher bei der datenschutzkonformen Gestaltung von Big-Data-Diensten. Es gibt Stellen, die umfangreiche und für die Analyse geeignete Datenbestände haben, bisher jedoch mit Blick auf datenschutzrechtliche Restriktionen von einer Verwendung absehen. Gesetzliche Erlaubnistatbestände der DSGVO erfordern hier eine Abwägung mit den Interessen der Betroffenen und im Regelfall auch deren ausführliche Information. Bei Einwilligungen ist ein Widerruf, bei gesetzlichen Tatbeständen das Widerspruchsrecht des Betroffenen bereits systemseitig zu berücksichtigen. Dies bedeutet auch, dass es Möglichkeiten geben muss, um mit den Betroffenen zu kommunizieren.

Semantisches Netz

Die Bezeichnung „semantisches Netz“ steht für eine Technik, um Daten zwischen Rechnern leichter auszutauschen und die Kommunikation zwischen Mensch und Computer zu vereinfachen. Inhalte und Begriffe werden dabei in Beziehung gesetzt. So findet eine Suche nach „Stadt, Theodor Storm“ zunächst dessen Gedicht „Die Stadt“. Erst wenn die logische Verbindung zwischen „Husum“ und „Stadt“ hinterlegt ist, kann zielführend nach einem Wohnort gesucht werden. Mit solchen Verkettungen auf Bedeutungsebene wird aus „Big Data“ dann „Smart Data“. Neben der latenten Gefahr für den Datenschutz durch detaillierte Datenauswertungen sowie umfassende Profilbildungen kann diese Technik umgekehrt auch im Sinne des Datenschutzes eingesetzt werden, um z. B. Datenschutzerklärungen mit vorher definierten Präferenzen von Betroffenen abzugleichen und Verantwortliche und Betroffene beim Einwilligungsmanagement zu unterstützen.

Aus Sicht aller Beteiligten ist eine einheitliche Kommunikationsinfrastruktur wünschenswert, sodass Betroffene Einwilligungen übersichtlich unter ihrer eigenen Kontrolle verwalten und Verantwortliche das Rechtemanagement automatisiert ausgestalten können. Sollen gesammelte personenbezogene Informationen im Rahmen von Big Data genutzt und gegebenenfalls auch mit anderen Geschäftspartnern geteilt werden, ist insbesondere ein umfassendes Management für Nutzereinwilligungen erforderlich. Damit in der gesamten Verwertungskette die Berechtigungen und Einschränkungen klar sind, sollen die von den Nutzenden erteilten Rechte und die jeweiligen Verarbeitungszwecke als Metadaten zusammen mit den personenbezogenen Daten übertragen werden. Mit einem solchen System lässt sich ebenfalls Transparenz gegenüber den Betroffenen gewährleisten und ein Widerspruchs- und Widerrufsmanagement umsetzen. Zugleich unterstützt es Verantwortliche beim Compliance-Nachweis gegenüber Betroffenen und Aufsichtsbehörden.

Eine technische Herausforderung stellen die Skalierbarkeit und Performanz eines solchen Systems dar. Zwar ist mit der anvisierten Lösung ein zusätzlicher technischer Aufwand verbunden, doch sind andernfalls Nachweise der Übereinstimmung mit den Anforderungen der DSGVO vermutlich viel schwieriger. Betreiber würden eine gegebenenfalls rechtlich unzulässige Datenverarbeitung riskieren, woraus Sanktionen resultieren können.

Im Wortlaut: Art. 21 Abs. 5 DSGVO

„Im Zusammenhang mit der Nutzung von Diensten der Informationsgesellschaft kann die betroffene Person ungeachtet der Richtlinie 2002/58/EG ihr Widerspruchsrecht mittels automatisierter Verfahren ausüben, bei denen technische Spezifikationen verwendet werden.“

Für die vereinheitlichte Kommunikation mit den Betroffenen wird das SPECIAL-Projekt auf bestehenden Lösungen und Komponenten aufbauen. Es ist beabsichtigt, ein Verfahren zu etablieren, das insbesondere zur automatisierten Ausübung des Widerspruchsrechts bei Diensten der Informationsgesellschaft geeignet ist, wie es in Artikel 21 Abs. 5 DSGVO vorgesehen ist. Im Projekt sollen Vertreter von relevanten Interessengruppen zu Wort kommen, um praxistaugliche Lösungen zu entwickeln.

https://datenschutzzentrum.de/projekte/special/

Was ist zu tun?

Für die Akzeptanz von Big-Data-Anwendungen ist es nötig, dass die Betroffenen informiert und ihre Rechte und Entscheidungen respektiert werden. Es liegt daher im Interesse aller Beteiligten, ein vereinheitlichtes Managementsystem für Betroffenenrechte zu unterstützen.

8.5.3 Projekt VALCRI – Big Data für die Polizei

Das seit Mai 2014 von der Europäischen Kommission geförderte Projekt „VALCRI – Visual Analytics for Sense-Making in Criminal Intelligence Analysis“ arbeitet an der Entwicklung eines Systemprototyps für visualisierte Datenanalyse im Rahmen kriminalpolizeilicher Erkenntnisgewinnung (35. TB, Tz. 8.5.3). Die Arbeit von Kriminalanalysten ist heutzutage üblicherweise davon geprägt, dass sie mithilfe einer rudimentären technischen Ausstattung eine Vielzahl von Verbrechensberichten auswerten, um organisierte Kriminalität sowie Serienstraftaten aufzudecken. Insoweit geht es im Kern um das Verstehen komplexer Sachzusammenhänge und Verbrechensnetzwerke. Das Ziel von VALCRI ist es, einen Softwareprototyp für eine solche komplexe Datenanalyse bereitzustellen, der nicht nur den polizeilichen Anforderungen genügt, sondern auch die datenschutzrechtlichen und ethischen Belange berücksichtigt.

In Zusammenarbeit mit Universitäten, Wirtschaftsunternehmen und potenziellen Anwendern aus dem Bereich der britischen und der belgischen Polizei forscht das ULD daran, wie ein solches System ausgestaltet sein muss, um die Anforderungen aus den unterschiedlichen Bereichen optimal und vor allem grundrechtskonform zusammenzubringen und in die Realität umzusetzen. Hierzu gehören z. B. Komponenten zur Anonymisierung und Pseudonymisierung personenbezogener Informationen, eine effiziente elektronische Zugangs- und Zugriffskontrolle sowie Konzepte zur Umsetzung von Transparenz in Bezug auf hochkomplexe Datenanalyseprozesse.

Das ULD bringt in diesem Forschungsprojekt das Fachwissen um die datenschutzrechtlichen Vorgaben im Polizei- und Justizbereich ein. Hierbei wird die Chance wahrgenommen, schon jetzt bei der Implementierung auf die zukünftigen Erfordernisse nach der ab 2018 geltenden EU-Richtlinie für Justiz und Inneres (JI-Richtlinie) einzugehen. Über die gesetzlichen Minimalanforderungen hinaus jedoch wird auch der Blick darauf gerichtet, wie der sogenannte „Datenschutz by Design“-Ansatz von Anfang an auf der Basis der Gewährleistungsziele des Standard-Datenschutzmodells (Tz. 6.3) in dem Prototyp technisch und organisatorisch verankert werden kann. Ein enger Austausch besteht in dem Zusammenhang auch mit denjenigen Projektpartnern, die sich mit ethischen Fragen beschäftigen, sowie mit dem Ethik-Board des Projekts.

https://datenschutzzentrum.de/projekte/valcri/

Was ist zu tun?

Die Auswertung großer Datenmengen durch die Polizei stellt einen erheblichen Eingriff dar. Daher sind die Grundrechte der Bürgerinnen und Bürger besonders zu beachten. Vor allem ist wichtig, dass die Analysetechnik bereits von Anfang an so gestaltet ist, dass datenschutzrechtliche Grundsätze wie Transparenz und Intervenierbarkeit umgesetzt werden.

8.6 Internet der Dinge

Das Internet der Dinge erfasst mittlerweile immer mehr Gegenstände des alltäglichen Gebrauchs. Dazu gehört beispielsweise das Smart Home, das mit vielen Sensoren ausgestattet ist, um sich den Wünschen der Bewohnerinnen und Bewohner anzupassen, beispielsweise zur Temperatur oder Zugangssicherung. In der Wohnung halten bewusst installierte „Lauscher“ Einzug, um Verbraucherinnen und Verbrauchern einen Bestellwunsch von den Lippen abzulesen. Zunehmend erhalten Alltagsgeräte wie Fernseher Sensoren und Kommunikationsmöglichkeiten mit dem Netz. Außerhalb der eigenen vier Wände findet man Überwachungskameras mit Schnittstellen ins Internet. Smart Cars werden künftig mithilfe ihrer Sensorik und Vernetzung untereinander, mit Ampeln und Straßen und mit ihren Herstellern kommunizieren.

Bei alledem sind die Rechte der betroffenen Personen zu wahren. Hier sind die Kaufinteressierten bereits bei der Auswahl von Geräten gefragt – und mangels ausreichender und verständlicher Information überfordert. Hersteller müssen daher transparenter darstellen, welche Verbindungen nach außen ein Gerät aufnimmt und welche Daten ausgetauscht werden. Nutzerinnen und Nutzer dürfen dem nicht ausgeliefert sein, sondern müssen selbst eingreifen können.

Internet der Dinge

Im Internet der Dinge (englisch: „Internet of Things“ (IoT)) werden zusätzlich zu den heutigen Computern auch alle möglichen anderen Gegenstände vernetzt und tauschen Daten aus. Die Datenverarbeitung geschieht oft so, dass Nutzende dies kaum bemerken und noch weniger steuern können.

Das ULD beschäftigt sich aktuell sowohl mit der Vernetzung und Automatisierung von Fahrzeugen (Tz. 8.6.1) als auch mit Ansätzen für verbesserte Nutzungsschnittstellen im Internet der Dinge für mehr Transparenz und Intervenierbarkeit (Tz. 8.6.2). Im Forum Privatheit (Tz. 8.1) arbeiten wir zu weiteren Themen der datenschutzfördernden Gestaltung der „smarten“ Welt. Die Prüfung der Wearables (Tz. 7.5) zeigt einen Bereich auf, in dem smarte Uhren und Fitnesstracker bereits Einzug in das Leben vieler Verbraucherinnen und Verbraucher gefunden haben.

8.6.1 Projekte iKoPA und SeDaFa – Datenschutz für den vernetzten Verkehr

Vernetzte und automatisierte Fahrzeuge sollen den Verkehr revolutionieren. Die damit verbundene Datenverarbeitung ist aber meist außerordentlich sensibel. Insbesondere in ländlichen Räumen ist das Auto für viele Menschen das zentrale Fortbewegungsmittel. Dementsprechend tief gehend sind auch die Einblicke in die Lebensführung der Betroffenen, die durch Fahrzeugdaten gewonnen werden können.

Smart Cars

Unter „Smart Cars“ versteht man vernetzte Fahrzeuge, die Daten untereinander, mit ihrer Umgebung und mit Herstellern austauschen. Ziele sind zumeist eine Verbesserung der Sicherheit und der Bequemlichkeit bis hin zum vollständig automatisierten Fahren.

Werden Positionsdaten verarbeitet, lassen sich aus diesen Daten z. B. Aussagen über den Alltagsablauf, Arztbesuche, politische und religiöse Orientierungen oder Hobbys machen.

Ganz ohne Datenverarbeitung ist autonomes Fahren nicht möglich. Vernetzte und autonome Fahrzeuge versprechen einen erheblichen Sicherheitsgewinn und einen nachhaltigeren, umweltschonenderen Verkehr. Das ULD beteiligt sich in den vom BMBF geförderten Forschungsprojekten „iKoPA – Integrierte Kommunikationsplattform für automatisierte Elektrofahrzeuge“ und „SeDaFa – Selbstdatenschutz im vernetzten Fahrzeug“ an der Entwicklung datenschutzfreundlicher Lösungen. Herausfordernd ist dabei die Vielzahl der möglichen betroffenen Personen – dies sind nicht nur Fahrer, sondern z. B. auch Mitfahrer, Fahrer anderer Fahrzeuge und Fußgänger. An den Daten in und von den Fahrzeugen besteht ein großes Interesse von Automobilherstellern,

Werkstätten, Versicherungen und Polizei- und Ordnungsbehörden.

Beim Projekt iKoPA liegt der Schwerpunkt auf der automatisierten elektrischen Mobilität. Ziel des Projekts ist die Entwicklung einer offenen Integrationsplattform für Services im vernetzten Verkehr. Für die Elektromobilität spielt beispielsweise die effiziente und verlässliche Bereitstellung von Ladesäulen eine große Rolle. Um diese Verlässlichkeit zu gewährleisten, werden im Projekt datensparsame Konzepte für die Reservierung von Ladesäulen entwickelt.

Das Projekt SeDaFa betrachtet schwerpunktmäßig die Möglichkeiten für Selbstdatenschutz durch die Betroffenen. Dazu ist es notwendig, dass sie umfassend über Datenverarbeitungsvorgänge informiert werden, und zwar auf eine Art und Weise, die es ihnen ermöglicht, tatsächlich ein Verständnis zu entwickeln. Dies ist zwingende Voraussetzung einer selbstbestimmten Kontrolle über die Datenverarbeitung, die den betroffenen Personen ermöglicht werden soll.

Bei der weiteren Entwicklung von vernetzten Fahrzeugen ist zu beachten, dass die informationelle Selbstbestimmung der Betroffenen gewahrt wird. Öffentliche und nichtöffentliche Stellen sind in der Verantwortung, ihre Fahrzeuge auch nach datenschutzrechtlichen Aspekten sorgfältig auszuwählen. Andernfalls bestünde die Gefahr, dass Dritte durch die Analyse der anfallenden Daten Rückschlüsse auf das Verhalten der Beschäftigten oder auf Kundenkontakte ziehen können. Ganz besonders deutlich wird dies in medizinischen Berufen, bei Anwälten oder bei der Polizei, wenn dort eingesetzte Fahrzeuge Datenspuren hinterlassen. Daraus entsteht ein Gestaltungsdruck auf die Hersteller, die Fahrzeugtechnik gegen unerlaubte Zugriffe abzusichern und den Betroffenen Eingriffsmöglichkeiten zu geben. Datenverarbeitungsvorgänge müssen entsprechend ihrem Schutzbedarf gesichert und das Löschen von Daten ermöglicht werden.

Hinsichtlich der Kommunikationsarchitektur ist das Entstehen von zentralen Entitäten mit umfassender Datensammlung zu vermeiden. Wir sehen es als kritisch an, wenn die personenbezogenen Daten vieler betroffener Personen für unterschiedliche Zwecke verarbeitet werden können – unabhängig davon, ob dies bei den Autoherstellern, bei Versicherern, bei den dominierenden Internetfirmen oder beim Staat passiert. Solche zentralen Datensammlungen stellen für Angreifer von außen ein besonders lohnendes Ziel dar und bergen gleichzeitig die Gefahr des Missbrauchs, wenn für unterschiedliche Zwecke erhobene Daten miteinander verkettet werden.

https://datenschutzzentrum.de/projekte/ikopa/
https://datenschutzzentrum.de/projekte/sedafa/

Was ist zu tun?

Bei der smarten Mobilität fallen viele schutzbedürftige Informationen an. Behörden und Unternehmen sind bei der Auswahl solcher Fahrzeuge in der Pflicht, die datenschutzrechtlichen Anforderungen als wichtige Kriterien heranzuziehen. Hersteller sind gehalten, entsprechende Angebote für den europäischen Markt zu gestalten.

8.6.2 Projekt Privacy&Us – Usability für das Internet of Things

Erstmals beteiligt sich das ULD an einem Marie-Skłodowska-Curie-Projekt, bei dem die Ausbildung von Nachwuchswissenschaftlern gefördert wird. Dreizehn Doktoranden arbeiten verteilt auf Europa und Israel im Austausch an Fragen des Datenschutzes zu „Privacy&Us – Privacy & Usability“, um Vorschläge zu erarbeiten, wie sich Datenschutzanforderungen nutzergerecht umsetzen lassen. Schwerpunkt der Forschung im ULD liegt dabei auf dem Internet der Dinge (Internet of Things (IoT)) und den sich daraus ergebenden Fragestellungen für die Nutzungsfreundlichkeit.

Im Zentrum steht zunächst eine Sachstandserhebung durch eine Online-Umfrage: Welche IoT-Produkte sind verbreitet? Nehmen die Nutzenden diese als komplexe Computer wahr

oder als bloße Nachfolger der altbekannten Geräte, beispielsweise wie einen Fernseher, bei dem lediglich das Smartphone und Sprachsteuerung die Fernbedienung ersetzen? Wie vielen ist bekannt, dass solche Geräte Sicherheitsupdates des verwendeten Betriebssystems benötigen, um nicht das heimische Netz, die Privatsphäre oder Geschäftsgeheimnisse zu gefährden? Aufbauend auf diesen Erhebungen wird untersucht, wie solche Produkte aus Sicht des Datenschutzes besser gestaltet werden können. Untersucht wird, welche Warnhinweise ernst genommen werden und wie über Risiken und Optionen so aufgeklärt wird, dass die Verbraucherinnen und Verbraucher informierte Entscheidungen treffen.

Aus Datenschutzsicht müssen Betroffene – das können neben dem Eigentümer auch Familienmitglieder und Gäste sein – nachvollziehen können, was ein Gerät mit ihren personenbezogenen Daten tut. Wird z. B. das gesprochene Wort lokal ausgewertet oder stets an die Server des Herstellers übermittelt? Wenn ja, wohin werden gegebenenfalls vertrauliche Informationen gesendet, und kann dies durch Konfiguration ohne erheblichen Verlust der Funktionalität geändert werden? Zwar noch kaum in der Realität vorzufinden, aber künftig zu berücksichtigen ist das Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Artikel 25 DSGVO).

Schließlich bleibt auch bei gut gestalteten Geräten das Problem der geeigneten Vermittlung der wesentlichen Informationen. Hier fehlen derzeit praktische Handreichungen für Hersteller, wie die erforderliche Transparenz hergestellt werden kann. Letztlich ist dies auch im Interesse der Hersteller, um sich durch ein gezieltes Aufzeigen der Mehrwerte für den Schutz der Privatsphäre am Markt durchsetzen zu können.

https://datenschutzzentrum.de/projekte/privacy-us/

09

KERNPUNKTE

Zertifizierung nach Datenschutz-Grundverordnung
Datenschutz-Gütesiegel
Datenschutz-Audit
IT-Grundschutz

9 Audit und Gütesiegel

9.1 Zertifizierung wird europäisch

9.1.1 Auswirkungen der Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung beinhaltet einige neue Regelungen zu Zertifizierungen. So erhalten die Aufsichtsbehörden durch Artikel 57 neue Aufgaben, beispielsweise das Billigen von Zertifizierungskriterien, Überprüfung von Zertifizierungen oder auch das Abfassen von Akkreditierungsregelungen. Auch können sie nunmehr, nach Artikel 58 der DSGVO, erteilte Zertifizierungen widerrufen.

Grundsätzlich können sowohl die Aufsichtsbehörden selbst als auch akkreditierte Zertifizierungsstellen Zertifizierungen vornehmen. Welche Stelle die Akkreditierung der Zertifizierungsstellen vornimmt, ist den nationalen Gesetzgebern überlassen worden. In Deutschland kann diese Aufgabe den Aufsichtsbehörden oder der Deutschen Akkreditierungsstelle GmbH (DAkkS) zukommen.

Möchte eine Organisation eine Zertifizierung erhalten, so muss durch Zertifizierungsstellen bzw. deren Sachverständige anhand genehmigter Kriterien geprüft werden, ob die Datenschutz-Grundverordnung bei den Verarbeitungsvorgängen von den Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Im Gegensatz zum Datenschutz-Gütesiegel des ULD können somit nicht nur Produkte, sondern auch Verfahren von öffentlichen und nichtöffentlichen Stellen zertifiziert werden.

Die Zertifizierung bringt den entsprechenden Organisationen zahlreiche Vorteile. So können sie eine Zertifizierung nicht nur werbewirksam ihren Kunden oder der Öffentlichkeit gegenüber verwenden; die Zertifizierung kann nach der Datenschutz-Grundverordnung auch als Faktor herangezogen werden, um die Erfüllung der datenschutzrechtlichen Anforderungen gegenüber Aufsichtsbehörden und Kunden nachzuweisen.

Auch das ULD will ab Mai 2018 Zertifizierungen im Sinne der Datenschutz-Grundverordnung durchführen und wird seine Kriterien und Verfahren entsprechend anpassen. Dabei werden wir uns an unserem bestehenden, aus dem Datenschutzrecht abgeleiteten Kriterienkatalog orientieren, um den bisherigen Zertifizierungen eine einfache und kostengünstige Fortentwicklung zu dem neuen System der DSGVO zu ermöglichen. Auch soll nach unserer Planung das bewährte zweistufige Verfahren, bei dem anerkannte Sachverständige die Prüfung vornehmen und das ULD dann nach einer Plausibilitätsprüfung das Siegel erteilt, bestehen bleiben.

Was ist zu tun?

Es sind Akkreditierungskriterien und Zertifizierungskataloge zusammen mit den anderen Aufsichtsbehörden und der Deutschen Akkreditierungsstelle GmbH zu erarbeiten, um den neuen Aufgaben entsprechend der Datenschutz-Grundverordnung nachkommen zu können. Außerdem ist das Datenschutz-Gütesiegel an die neuen Regelungen der Datenschutz-Grundverordnung anzupassen, um ebenfalls deren Voraussetzungen für die Zertifizierung zu erfüllen.

9.1.2 AG Zertifizierung

Sämtliche Aufsichtsbehörden in Deutschland haben durch die Datenschutz-Grundverordnung zahlreiche neue Aufgaben auch im Bereich der Zertifizierung erhalten. Auch wenn keine eigene Zertifizierung erteilt werden soll, sind sie in den Akkreditierungsprozess von Zertifizierungsstellen und auch in die Überwachung von Zertifizierungsstellen und gültigen Zertifizierungen eingebunden. Um hierbei ein einheitliches Vorgehen zu erreichen, wurde im Sommer 2016 die AG Zertifizierung gegründet. Ihr gehören Vertreter eines Großteils der Datenschutzaufsichtsbehörden der Länder und der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit an. Geleitet wird sie vom ULD.

Bei bisherigen Treffen bestand Einigkeit darüber, dass es notwendig ist, gemeinsame Kriterien zu entwickeln und in vergleichbarer Form aufzutreten. Insbesondere wurde vereinbart, bei der Erstellung der Akkreditierungskriterien eng mit der Deutschen Akkreditierungsstelle GmbH zusammenzuarbeiten.

2016 fanden zwei Treffen statt, um die wichtigen Punkte mit übergreifendem Abstimmungsbedarf herauszuarbeiten und mit der Erarbeitung der Kriterien für eine Akkreditierung von Zertifizierungsstellen zu beginnen. 2017 werden weitere Treffen stattfinden, wobei auch die Zusammenarbeit mit der Deutschen Akkreditierungsstelle GmbH intensiviert wird.

9.2 Datenschutz-Gütesiegel

9.2.1 Abgeschlossene Gütesiegelverfahren

Im Zeitraum 2015/2016 konnte das ULD für zwölf Produkte erstmalig ein Datenschutz-Gütesiegel verleihen. Weiterhin konnten zwanzig Produkte nach Fristablauf der bestehenden Zertifizierung in einem vereinfachten Verfahren rezertifiziert werden.

Im Vergleich zum vorhergehenden Berichtszeitraum 2013/2014 stiegen sowohl die Zahl der Neuvergaben des Datenschutz-Gütesiegels als auch die Rezertifizierungen um jeweils etwa fünfzig Prozent an. Dies zeigt, dass das Datenschutz-Gütesiegel Schleswig-Holstein bei Herstellern und Diensteanbietern weiterhin akzeptiert ist und nachgefragt wird. Wie auch in der Vergangenheit weist das Gütesiegel in einigen Branchen, wie etwa bei der Akten- und Datenträgervernichtung, eine besonders hohe Marktdurchsetzung auf. Darüber hinaus hat sich die Zunahme von Zertifizierungsverfahren, die Produkte im Bereich der Medizin- und Sozialdaten betreffen, im zurückliegenden Berichtszeitraum fortgesetzt.

Neben der verstärkten Nutzung von Cloud-Diensten konnte in den Jahren 2015/2016 auch eine zunehmende Einbindung von mobilen IT-Systemen (Smartphones, Tablets usw.) und Apps bei der Erbringung von Dienstleistungen in unterschiedlichsten Bereichen festgestellt werden. Insbesondere die Orientierungshilfen des Düsseldorfer Kreises bzw. der ihm angegliederten Arbeitskreise gewinnen bei der Definition der notwendigen rechtlichen und technischen Anforderungen zunehmend an Bedeutung.

Im Hinblick auf die sehr unterschiedliche Ausgestaltung der einzelnen Zertifizierungsgegenstände und der hierbei zum Teil hochsensiblen personenbezogenen Daten der Betroffenen ist die punktuelle Einbindung anderer Referate des ULD, aber auch anderer Aufsichtsbehörden in den Zertifizierungsprozess von zunehmender Bedeutung.

Im Einzelnen wurden folgende Produkte **neu zertifiziert**:

- „Chronic Care Application CCA“, Version 1.23: serverbasierte Webanwendung zur Unterstützung der medizinischen Patientenversorgung bei chronischen Erkrankungen,
- „en:key“, Stand Mai 2015: batterielose Kombination aus Raumsensor und Reglerventil, die Nutzungsprofile zur Steuerung der Leistung von Heizungen erstellt und verwendet,
- „Secure Data Space (Online, Dedicated und Virtual Appliance)“, Version 3.0: webbasierter, virtueller Datenraum zum Hochladen, Speichern, Verwalten und Austauschen von Daten,

- „HealthDataSpace“, Version 2: webbasierter, virtueller Datenraum zum Hochladen, Speichern, Verwalten und Austauschen von medizinischen Daten,
- „MedicalPad“, Version 7.0: Patientenerfassungs- und Protokollsoftware zur Erstdokumentation und Protokollierung von Rettungsdiensteinsätzen,
- „AQUA SQG – Externe (sektorenübergreifende) Qualitätssicherung“, Stand Oktober 2015: Verfahren zur Durchführung von Qualitätsuntersuchungen im Zusammenhang mit der Erbringung von medizinischen Leistungen im Rahmen der Gesundheitsversorgung,
- „ViViAN“, Version 4.0: Datenaustausch in einem Ärzte- oder Praxisnetzwerk,
- „IzB stationär“, Version 1.1.6.1: Software zur Behandlungsplanung und Behandlungsdokumentation für verschiedene Bereiche der Rehabilitation,
- „Online Terminmanagement“, Version 2.1: Online-Terminbuchungslösung für Zahnarztpraxen von der DAMPSOFT GmbH,
- „Aktenvernichtungsverfahren Eiderheim“, Stand Mai 2016: Verfahren der Aktenvernichtung (Originalgröße/Papierform) sowohl mit Abholung von Transportbehältern als auch Direktanlieferung durch den Kunden,
- „Verschlüsselungsautomat S/MIME 1.0“, Version 1.0: Add-on für ein E-Mail-System auf Basis von De-Mail, das eine Ende-zu-Ende-Verschlüsselung durch das Verschlüsselungsverfahren S/MIME erlaubt,
- „teamplay“, Stand 06.10.2016: onlinebasierte Plattform zur Vernetzung medizinischer, bildgebender Systeme zur Optimierung der Geräteauslastungen und Strahlendosis.

Im Rahmen eines Rezertifizierungsverfahrens wurden folgende Produkte in einem vereinfachten Verfahren erneut überprüft und zertifiziert:

- „mdex fixed.IP+“ (zuvor mdex fixed.IP), Stand Mai 2015: Ermöglichung der IP-basierten Kommunikation zwischen Mobilgeräten über Mobilfunknetze bzw. Kommunikation von stationären Geräten mit einem Mobilgerät über ein Mobilfunknetz auf IP-Basis,
- „DC+, DCM+, DC4, DCM4“, Stand Juni 2015: Lesegeräte zur Altersverifikation der Firma ICT Europe GmbH,
- „e-pacs Speicherdienst“, Version 3.0: elektronische externe Archivierung von Röntgenbildern und anderen patientenbezogenen medizinischen Daten,
- „WIMES“, Stand Juni 2015: Webportal zur Evaluation der Wirksamkeit von Hilfen zur Erziehung,
- „Business Keeper Monitoring System“ (BKMS), Version 3.1: Dialog zwischen Hinweisgebern und Hinweisbearbeitern, um Missstände, Gefahren und Risiken in einer Organisation melden zu können (Whistleblowing),
- „Zentrale Kassenprüfungssoftware“, Stand September 2015: Analyse der Kassendaten zur Aufdeckung von Manipulationen im Kassierprozess,
- „NaVIS – Nachbau-, Verwaltungs- und Informations-System“, Version 3.1.16: technische Realisierung des Abrechnungs- und Verwaltungsverfahrens von Nachbaugebühren,
- „RWAS R3“, Stand Oktober 2015: Lagerverwaltungssoftware, die Prozesse der Aktenarchivierung in strukturierten Lagern unterstützt,
- „Altersverifikation KBA 18“, Stand Dezember 2015: Altersüberprüfung durch Einlesen des Personalausweises oder des Führerscheins,
- „Elefant Profi (im Security-Mode)“, Version 16.01: Verwaltungsprogramm für psychotherapeutische und ärztliche Praxen,
- „Verfahren der Akten- und Datenträgervernichtung“, Stand März 2016: Verfahren zur Vernichtung von Akten und Datenträgern durch die Ropakt GmbH,
- „TeamDrive (TeamDrive Free, TeamDrive Personal und TeamDrive Professional)“, Version 4: Kollaborationstool für den Zugriff mehrerer Benutzer auf einen verschlüsselten Datenbestand zur gemeinsamen Bearbeitung von Dokumenten,
- „Dataport Firewall Altenholz“, Stand März 2016: Schutz der Ressourcen im Netzwerk von Dataport gegen unberechtigte Zugriffe aus dem Internet durch Einschränken der Verbindungen von und zu dem Internet auf zulässige Dienste,
- „Scola Schulverwaltung“, Version 2015: Schulverwaltungssoftware zur Verwaltung der Daten von Schülern, Lehrern und sonstigen zur Verwaltung und zum Betrieb einer Schule erforderlichen Personen,

- „OPEN/PROSOZ“, Version 2015.3.0.0: Dialogsystem für den Einsatz im Bereich der sozialen Sicherung,
- „Verfahrensregister“, Version 1.0 (2016): Unterstützung des betrieblichen Datenschutzbeauftragten bei der Erstellung und Verwaltung eines Verfahrensregisters,
- „Erbringung von Postzustelldienstleistungen“, Stand Juli 2016: von Postcon National GmbH & Co. KG (ehem. TNT Post) erbrachte Postzustelldienstleistungen,
- „Datenträgervernichtung“ (DV), Stand November 2016: mobile und stationäre Akten- und Datenträgervernichtung im Rahmen einer Auftragsdatenverarbeitung durch die Firma Rhenus Data Office GmbH,
- „Easybooth Modell 37, Easybooth V3 Modell 36, Minicabine3 Modell 38 und UPB Modell 3“ (ehemals FOTOFIX EB digital): digitale Fotokabine mit integrierter biometrischer Bildbearbeitung zur Nutzung in Meldebehörden,
- „RED Medical 2016“, Stand November 2016: Erhebung, Verarbeitung und Nutzung von medizinischen Patientendaten zur Unterstützung von ärztlichen Anamnesen, Diagnosen und Therapien.

Was ist zu tun?

Trotz einer erfreulich hohen Nachfrage nach einer Neuzertifizierung im Zeitraum 2015/2016 ist das Datenschutz-Gütesiegel noch nicht in allen Bereichen der Wirtschaft bekannt. Daher ist es auch zukünftig wichtig, Anbieter, einsetzende Stellen und Betroffene in diesen Bereichen anzusprechen und auf die Vorzüge einer Zertifizierung hinzuweisen. Dies gilt insbesondere auch für Ausschreibungen. Das Zertifizierungsverfahren ist an die Datenschutz-Grundverordnung anzupassen.

9.2.2 Sachverständige

In den Jahren 2015 und 2016 konnten zwölf neue Sachverständige für das Verfahren zur Erlangung des Datenschutz-Gütesiegels Schleswig-Holstein anerkannt werden.

Im Zuge des zweistufig aufgebauten Gütesiegelverfahrens erfolgt die Begutachtung der Zertifizierungsgegenstände durch beim ULD anerkannte Gutachter. Eine Anerkennung als Gutachter kann entweder für den Bereich Recht oder den Bereich Technik beantragt werden, bei Nachweis einer entsprechenden Qualifikation besteht auch die Möglichkeit einer Doppelzulassung. Ebenso ist die Anerkennung einer Prüfstelle möglich. Für eine Anerkennung als Gutachter sind durch den Antragsteller dessen Zuverlässigkeit und Unabhängigkeit sowie die erforderliche Fachkunde nachzuweisen. Letztere muss sich insbesondere auf den Bereich Datenschutz und die Durchführung von Prüfungen oder Begutachtungen beziehen und mehrjährige praktische Erfahrungen beinhalten.

Hinzugekommen als Sachverständige/sachverständige Prüfstellen sind 2015/2016:

- greeneagle certification GmbH, Hamburg (Recht/Technik),
- Dr. Bernhard Freund, LL.M., M.Comp.Sc., Hamburg (Recht/Technik),
- Tina Vieten, Mannheim (Technik),
- Dr. Niels Lepperhoff, Düsseldorf (Technik),
- Sebastian Schulz, Königs Wusterhausen (Recht),
- Dr. Bernd Schmidt, Hamburg (Recht),
- Nina Diercks, M.Litt, Hamburg (Recht),
- David Oberbeck, Hamburg (Recht),
- Michael Schüssler, Aschaffenburg (Technik),
- Dr. Gerolf J. Starke, LL.M., Kaiserslautern (Recht),
- Dr. Andreas Freitag, Hamburg (Recht),
- Dipl.-Wirtschaftsing. Kerstin Kafke, Hamburg (Technik).

Momentan sind beim ULD 70 anerkannte Einzelsachverständige und 14 Prüfstellen registriert.

Wie in den Jahren zuvor fand auch 2015 und 2016 im Anschluss an die jährliche Sommerakademie ein Gutachter-Workshop für die Gutachter des Datenschutz-Gütesiegels Schleswig-Holstein in Kiel statt. Diese Möglichkeit des Erfahrungsaustausches wurde auch dieses Mal von zahlreichen Sachverständigen wahrgenommen, um generelle und aktuelle Fragen rund um das Gütesiegel Schleswig-Holstein sowie das Thema „Zertifizierung“ im Allgemeinen zu erörtern. Themen dieses Workshops waren u. a. die Entwicklung des Standard-Datenschutzmodells (SDM), die Datenschutz-Folgenabschätzung nach der Datenschutz-Grundverordnung sowie die Zukunft und Positionierung des Datenschutz-Gütesiegels Schleswig-Holstein im Hinblick auf die europäischen Regelungen und die sich daraus ergebenden Entwicklungen in anderen (Bundes-)Ländern auf diesem Gebiet. Diskutiert wurde ferner über ein mögliches Anerkennungsverfahren von EuroPriSe-Zertifizierungen (European Privacy Seal; 35. TB, Tz. 9.2.5) und von Gütesiegeln aus Mecklenburg-Vorpommern.

Weitere Informationen für Sachverständige befinden sich im Internet unter:

https://datenschutzzentrum.de/guetesiegel/sachverstaendige/

Was ist zu tun?

Um das Verfahren der Zertifizierung weiterhin effektiv zu gestalten und den Ablauf stetig zu verbessern, ist es auch zukünftig wichtig und notwendig, die Sachverständigen in ihrer Arbeit zu unterstützen.

9.3 Datenschutzaudits

9.3.1 Wie ein typisches Datenschutzaudit in der Verwaltung abläuft

Mit dem Datenschutzaudit erhalten öffentliche Stellen in Schleswig-Holstein die Möglichkeit, ihr Datenschutzkonzept durch das ULD prüfen und beurteilen zu lassen. Grundlage des Audits ist eine schriftliche Vereinbarung der jeweiligen Behörde mit dem ULD.

Die folgenden Schritte gehören typischerweise zu dem Audit:

- Überprüfung der Abgrenzung des Auditgegenstandes,
- Analyse der Dokumentation (Datenschutzkonzept),
- Begutachtung der Wirkungsweise des Datenschutzmanagementsystems und der Erreichung der festgelegten Datenschutzziele,
- Hervorhebung von anerkennenswerten und datenschutzfreundlichen Datenverarbeitungsprozessen,
- stichprobenartige Überprüfung der Umsetzung der im Datenschutzkonzept festgelegten Sicherheitsmaßnahmen,
- Überprüfung der Einhaltung datenschutzrechtlicher und bereichsspezifischer Vorschriften in Bezug auf den Auditgegenstand,
- Erstellung eines Gutachtens,
- Verleihung des Datenschutzauditzeichens.

Was ist zu tun?

Auditverfahren dienen dazu, die Datenverarbeitung in einer Behörde zu überprüfen und datenschutzkonform auszugestalten. Behörden sollten deshalb diese Dienstleistung des ULD in Anspruch nehmen.

9.3.2 Audit für den SafeMail-Dienst der Kassenärztlichen Vereinigung Schleswig-Holstein (KVSH)

Die seit Jahren bestehende intensive Zusammenarbeit der Kassenärztlichen Vereinigung Schleswig-Holstein (KVSH) mit dem ULD wurde auch im Berichtszeitraum erfolgreich fortgeführt. Im November 2015 hat die KVSH ihren E-Mail-Dienst „SafeMail“ im Rahmen eines Audits erneut überprüfen und reauditieren lassen.

Zur Erinnerung: Die KVSH betreibt in einem geschlossenen System einen E-Mail-Dienst für Arztpraxen (34. TB, Tz. 9.1.1). Ursprünglich unter dem Namen „eKVSH“ gestartet, heißt der Dienst mittlerweile „SafeMail“. Innerhalb dieses Systems können zwischen Arztpraxen elektronische Nachrichten und angehängte Dokumente ausgetauscht werden, die durch eine Ende-zu-Ende-Verschlüsselung geschützt sind. Eine solche Verschlüsselung sichert die Vertraulichkeit und Integrität der Nachrichten nicht nur auf dem Transportweg zwischen den beteiligten Mailservern, sondern auch bis hin zum Client, mit dem die Nachricht bearbeitet wird. Somit können auch die Betreiber des Dienstes keinen Einblick in die Inhalte der Nachrichten nehmen.

Im Rahmen einer Reauditierung werden regelmäßig die Veränderungen am Auditgegenstand überprüft. Daneben erfolgte eine stichprobenartige Überprüfung der Umsetzung des Datenschutz- und Informationssicherheitsmanagementsystems.

Auch wenn die Inhalte der Nachrichten (und somit Patientendaten) der KVSH nicht zur Kenntnis gelangen können, so könnte diese als Betreiber des Dienstes das Kommunikationsverhalten der beteiligten Arztpraxen beobachten. Dieses Kommunikationsverhalten wird auch teilnehmerbezogen erfasst, da die KVSH die Teilnehmenden mit einem Geldbetrag unterstützt, der sich nach der Anzahl der versandten und empfangenen Nachrichten bemisst. Nach Erstellung der Abrechnung werden die Aufzeichnungen anonymisiert, indem die Teilnehmernummern, die die beteiligten Kommunikationspartner bezeichnen, gelöscht werden. Die anonymisierten Aufzeichnungen werden benötigt, um Kapazitäten und Wartungen zu planen, beispielsweise zur Bestimmung des optimalen Zeitpunktes für eine Dienstunterbrechung zu Wartungszwecken.

Auch über einzelne Verfahren hinaus arbeitet die KVSH mit dem ULD zusammen. So wurde im April 2017 ein Projekt begonnen, in dem das ULD die KVSH dabei unterstützt, ihr gesamtes Datenschutz- und Informationssicherheitsmanagementsystem an die Erfordernisse des IT-Grundschutzes unter Berücksichtigung der Vorgaben der Datenschutz-Grundverordnung anzupassen.

9.4 Auditberatungen – IT-Grundschutz wird zunehmend nachgefragt

9.4.1 Grundschutz für die IT der Kernkraftfernüberwachung

Das ULD wurde vom Ministerium für Energiewende, Landwirtschaft, Umwelt und ländliche Räume des Landes Schleswig-Holstein (MELUR) im Jahr 2015 beauftragt, die Grundschutzkonformität der IT-Komponenten der Kernkraftwerkfernüberwachung in Schleswig-Holstein (KFÜ-SH) auf der Basis von IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu begutachten.

Die KFÜ-SH ist ein Instrument der atomrechtlichen Aufsicht. Es dient zur Überwachung der radioaktiven Abgaben (Emissionen) aus den Kernkraftwerken (KKW) sowie zur Kontrolle der daraus resultierenden Immissionen in der Umgebung der Anlagen. Außerdem werden ausgewählte Parameter zum Betriebszustand einer Anlage überwacht, die geeignet sind, den Freisetzungspfad radioaktiver Stoffe zu ermitteln.

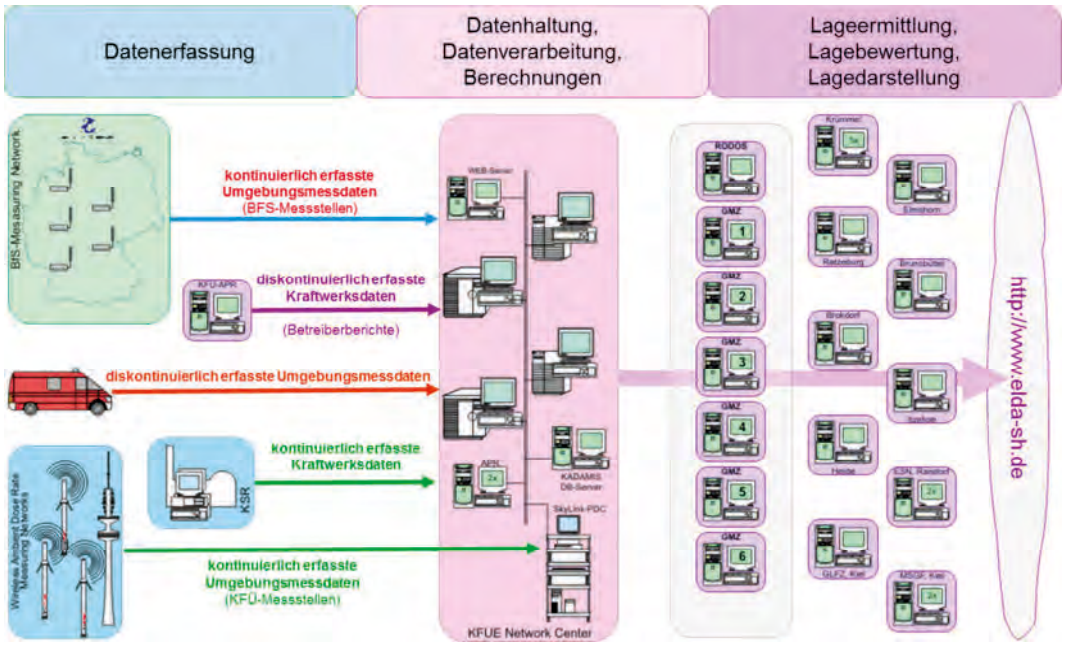


Abbildung: Informationsmanagement KFÜ-SH (Quelle: MELUR V7 Betriebskonzept)

Die Umsetzung des Grundschutzstandards wurde von der Abteilung V7 des MELUR für die gesamte Datenverarbeitung der KFÜ-SH festgelegt. Der Informationsverbund enthält somit alle im Rahmen der KFÜ-SH durchgeführten Geschäftsprozesse. Aufgrund der Komplexität der infrastrukturellen und technischen Gegebenheiten der KFÜ-SH wurde der Informationsverbund in folgende Teilinformationsverbünde untergliedert:

- Kernkraftwerkfernüberwachungszentrale,
- Stabsräume Reaktorsicherheit,
- Energiesysteme Nord ESN,
- Dataport,
- Siemens,
- Kernkraftwerk Krümmel,
- Kernkraftwerk Brunsbüttel,
- Kernkraftwerk Brokdorf,
- Arbeitsplätze Katastrophenschutz,
- Ortsdosisleistungsmessnetz,
- Datenerfassung Kernkraftwerke.

Das MELUR hat für den Betrieb der KFÜ-SH in der Abteilung V7 ein eigenständiges Informationssicherheitsmanagementsystem (ISMS) eingeführt. Dieses umfasst sowohl eine IT-Sicherheitsbeauftragte als auch ein zusätzliches IT-Sicherheitsmanagement-Team (ITSM-Team). Das ITSM-Team besteht aus Mitarbeitern der Firmen Siemens, ESN und Dataport, die in ihrem jeweiligen Zuständigkeitsbereich über die fachtechnische Tätigkeit hinaus auch für die Gewährleistung der Informationssicherheit verantwortlich sind. Die von der IT-Sicherheits-

beauftragten und vom ITSM-Team umzusetzenden Sicherheitsziele wurden in einer „Leitlinie zur Informationssicherheit KFÜ“ festgelegt.

Das ULD hat während der Begutachtung folgende Aufgaben durchgeführt:

- Analyse der Aufbau- und Ablauforganisation für die Festlegung und Abgrenzung des Informationsverbunds (Bestandsaufnahme),
- Abgrenzung des Informationsverbunds und Erstellung von Teilverbünden mit dem Grundschutztool,
- gemeinsame Erstellung eines Stufenprojektplans für die Implementierungsphase,
- Unterstützung bei der Einrichtung eines übergreifenden Sicherheitsmanagements,
- Durchführung von Schulungen zum Grundschutzstandard und zum Grundschutztool,
- Mitwirkung und Überprüfung der Festlegung der Schutzbedarfe nach den Grundschutzanforderungen,
- Zuweisung der Sicherheitsmaßnahmen aus den IT-Grundschutz-Katalogen,
- Überprüfung der Sicherheitsmaßnahmen bezüglich des Umsetzungsstandes (Basissicherheitscheck),
- Steuerung der Umsetzung offener Sicherheitsmaßnahmen,
- Mitwirkung bei der Durchführung der ergänzenden Sicherheits- und Risikoanalyse,
- Mitgestaltung bei der Erstellung erforderlicher Dokumentationsunterlagen,
- Bestätigung der grundschutzkonformen Umsetzung entsprechend dem Stufenprojektplan nach abschließender Implementierung.

Die während des Audits durchgeführten Überprüfungen haben ergeben, dass das MELUR, Abteilung V7, den Grundschutzstandard für das KFÜ-System vollständig umsetzt und die Grundschutzkonformität gewährleistet.

Was ist zu tun?

Das MELUR, Abteilung V7, hat vorbildlich den international anerkannten IT-Grundschutzstandard des Bundesamts für Sicherheit in der Informationstechnik für die Kernkraftwerkfernüberwachungssysteme umgesetzt. Auch die anderen Ministerien in Schleswig-Holstein sollten konsequent für ihre Datenverarbeitung die Grundschutzkonformität anstreben.

9.4.2 Grundschutz in einem Forschungsinstitut

Die IEA (International Association for the Evaluation of Educational Achievement) ist eine unabhängige, gemeinnützige Forschungsorganisation. Sie führt große internationale und nationale Vergleichsstudien zu Schülerleistungen und anderen Aspekten von Bildung durch, um die Auswirkungen von Steuerung und Praktiken innerhalb einzelner und im Vergleich unterschiedlicher Bildungssysteme zu verstehen. Bei der IEA Hamburg sind über einhundert Experten an der Planung und Durchführung der verschiedenen Studienaufgaben beteiligt, die von der Stichprobenziehung bis hin zur Datenanalyse reichen. Die Experten bieten darüber hinaus auch eine breite Palette von Dienstleistungen im Zusammenhang mit internationalen und nationalen Erhebungen an.

Im Jahr 2016 hat die IEA Hamburg das ULD beauftragt, die Ausrichtung und Implementierung ihres Datenschutz- und IT-Sicherheitsmanagements nach datenschutzrechtlichen Vorgaben und dem IT-Grundschutzstandard beratend zu begleiten. Dabei wurden mit der IEA Hamburg folgende Schritte festgelegt:

- Bestandsaufnahme und Abgrenzung des Informationsverbunds,
- Einrichtung der Organisationsstrukturen für ein Datenschutz- und Informationssicherheitsmanagement,

- Schulung und Sensibilisierung der Beschäftigten und der für Datenschutz und IT-Sicherheit zuständigen Personen,
- Ermittlung der Schutzbedarfe in einer Schutzbedarfsfeststellung,
- Einsatz von z. B. Verinice mit Verbunderfassung und Bausteinzuordnung aus den Grundschutz-Katalogen sowie Entwicklung spezieller Datenschutzbausteine,
- Maßnahmenbearbeitung im Rahmen von Inspektionen und Interviews,
- Prüfung des Umsetzungsstandes der Datenschutz- und Grundschutzmaßnahmen,
- Erstellung der erforderlichen Datenschutz- und Grundschutzdokumentationen,
- Durchführung einer Risikoanalyse für Bereiche mit hohem Schutzbedarf,
- optional: gegebenenfalls Abgleich des Informationsverbunds mit dem BSI und Begleitung bzw. Durchführung des Zertifizierungsverfahrens.

Zum gegenwärtigen Zeitpunkt hat die IEA Hamburg die Organisationsstrukturen für das Datenschutz- und IT-Sicherheitsmanagement BSI-konform umgesetzt. Die Institutsleitung unterstützt die betrieblichen Beauftragten für Datenschutz und für Informationssicherheit dabei, die Datenschutz- und IT-Grundschutzanforderungen in die Arbeitsabläufe der IEA Hamburg zu integrieren. Als nächster Schritt werden die festgelegten Schutzmaßnahmen ergänzend zu den bestehenden vollständig in die Umsetzung gebracht. Ziel der IEA Hamburg ist es, bis Ende 2017 alle erarbeiteten Anforderungen zu erfüllen, um den Schutz der verarbeiteten Daten auf hohem Niveau zu gewährleisten und gegenüber ihren Kunden und Kooperationspartnern einen geeigneten Nachweis zu erbringen.

Was ist zu tun?

Der IT-Grundschutzstandard des Bundesamts für Sicherheit in der Informationstechnik gewinnt zunehmend an Bedeutung. Mit Geltung der Datenschutz-Grundverordnung 2018 werden die Anforderungen für Behörden und Unternehmen im Hinblick auf ein angemessenes Datenschutz- und IT-Sicherheitsmanagement erhöht. Behörden und Unternehmen können ihre Datenverarbeitung durch das ULD auf Herz und Nieren prüfen lassen und dabei feststellen, inwieweit sie die Datenschutz- und Sicherheitsanforderungen erfüllen.

10

KERNPUNKTE

Verschlüsselung
Windows 10
Metadaten-Löschungen und Schwärzungen
Smart Home

10 Aus dem IT-Labor

10.1 Webbrowser und Erweiterungen – Spionage durch die Hintertür

Der Browser als Fenster zum Internet verliert durch Apps deutlich an Boden. Auf Smartphones und Tablets bieten dedizierte Apps oft mehr Komfort, sodass immer seltener auf den Generalisten „Browser“ zurückgegriffen werden muss. Trotzdem bleibt er in vielen Bereichen das Werkzeug der Wahl, um mit Online-Diensten zu kommunizieren.

Dabei muss deutlich zwischen herkömmlichen Desktop-Browsern und ihren mobilen Pendants, die häufig nur einen Abglanz der Desktop-Vorbilder darstellen, unterschieden werden. Neben eingeschränkten Konfigurationsmöglichkeiten fehlt den Mobilbrowsern oft vor allem die Möglichkeit, mit Erweiterungen – auch Add-ons genannt – um wichtige Funktionen ergänzt zu werden. Rühmliche Ausnahme ist hier der Browser Firefox, der auf denselben Erweiterungspool zugreifen kann wie sein großer Desktop-Bruder. Datenschutzfunktionen wie die Blockierung von Inhalten, die der Nachverfolgung von Nutzern dienen (sogenannte Tracker), oder zur automatischen Nutzung verschlüsselter Verbindungen lassen sich so auch auf dem Smartphone oder Tablet leicht nachrüsten.

Erweiterungen im Blickpunkt

Ein selten beachteter Aspekt von Browser-Erweiterungen ist jedoch, dass sie in der Regel vollständigen Zugriff auf die Surfhistorie des Nutzers haben. Im Falle des Add-ons „WOT – Web of Trust“ wurde das zu einem Problem. Der Anbieter des Add-ons verspricht, Nutzern eine Rückmeldung über die Vertrauenswürdigkeit der jeweils besuchten Webseite in Form einer Ampel zu geben. Um jene Vertrauenswürdigkeit abschätzen zu können, wird die besuchte Adresse zum WOT-Server gemeldet, der anhand seiner Datenbank mit Rot, Gelb oder Grün antwortet. Im Falle der WOT-Erweiterung wurden jedoch einerseits deutlich mehr Daten übertragen, als zur eigentlichen Diensterbringung nötig gewesen wären, zum anderen wurden die so übertragenen Informationen auch an Dritte weitergegeben.

Der Fall WOT zeigt exemplarisch, welche Risiken Browser-Erweiterungen mit sich bringen. Einerseits wollen und müssen sie Zugriff auf möglichst viele Informationen zur aktuellen Surfsitzung haben. Andererseits ist der Urheber einer Erweiterung dem Nutzer in den seltensten Fällen bekannt, das Vertrauen in die Erweiterung stützt sich auf Nutzerrezensionen und „Sternchen-Bewertungen“ im Download-Portal des Browser-Anbieters. Insbesondere wenn eine Erweiterung wie im Fall von WOT für die versprochene Funktion Daten übertragen muss, ist für den Nutzer kaum nachzuvollziehen, ob und inwieweit die tatsächliche Übertragung verhältnismäßig zur versprochenen Funktion ist. Hinzu kommt der Umstand, dass oft – so auch bei WOT – von „anonymen“ Daten gesprochen wird, obwohl dies nicht der Fall ist. Die WOT-Erweiterung versah die aufgerufenen URLs mit einer nutzerspezifischen ID, in völliger Verkennung der Tatsache, dass in vielen der aufgerufenen Webadressen auch Identifizierungsmerkmale wie Nutzernamen oder Kundennummern auftauchten.

Als die Berichte über WOT durch die Presse gingen, hagelte es in den Download-Portalen der Browser-Hersteller erwartungsgemäß schlechte Bewertungen, die aber aufgrund mehrerer Tausender positiver Bewertungen der Vorjahre den Durchschnittswert nur unwesentlich beeinflussten. Wer als Nutzer nur die Durchschnittsbewertung ansieht, wird in die Irre geführt.

Als Konsequenz aus dem WOT-Vorfall bleibt die unbequeme Erkenntnis, dass jede Browser-Erweiterung den Nutzer potenziell belauschen kann – unabhängig davon, was ihr ursprünglich anvisierter Einsatzzweck ist. Erweiterungen sollten also nur zum Einsatz kommen, wenn sie benötigt werden. Bei der Auswahl von Erweiterungen ist ebenfalls Umsicht nötig. Keinesfalls sollten Erweiterungen unbedacht „einfach so“ installiert werden. Mindestens ein Blick in die Nutzerbewertungen, besser noch eine Websuche nach professionellen Tests und Evaluationen oder gemeldeten Problemen mit der Erweiterung sollten vorangehen.

Tracking-Schutz und Werbeblocker

Ein Hauptanwendungszweck von Browser-Erweiterungen sind Werbeblocker. Solche Erweiterungen klinken sich in den Datenverkehr des Browsers ein, um die empfangene Webseite von Werbebannern und Textanzeigen zu

befreien. Dazu analysieren die Blocker den HTML-Quellcode der Seite und entfernen Referenzen auf dem Werbeserver. Aus Datenschutzsicht sind Werbeblocker deshalb relevant, weil die Einbindung von Anzeigen auf Webseiten fast ausnahmslos mit der Nachverfolgung der Webseitenbesucher einhergeht. Neben den reinen Grafiken, die dem Nutzer dargestellt werden sollen, übermitteln die externen Werbeserver Scripts und Cookies, deren Zweck darin besteht, die Nutzer über einen möglichst langen Zeitraum wiedererkennbar zu machen, um auf Basis dieser Informationen passgenaue Werbung auszuwählen.

Dabei hat der Betreiber der ursprünglich aufgerufenen Webseite keinerlei Einfluss auf das, was der Werbepartner aus seinem Netzwerk an den Besucher ausliefert. Zwar kann er im Vorfeld Anzeigenkategorien wählen oder ausschließen; was jedoch konkret an seine Besucher ausgeliefert wird und welche Informationen bei der Auslieferung der Inhalte von seinen Besuchern abgegriffen werden, ist für den Webseitenbetreiber nicht zu steuern.

Ein weiteres Problem besteht aus Datensicherheitssicht: In der Vergangenheit wurde statt Werbung mitunter Schadcode verteilt, der in das Werbenetzwerk eingeschleust wurde. Überspitzt dargestellt, muss man sich die gegenwärtige Situation wie eine Zeitschrift vorstellen, bei der die Werbekunden ihre Anzeigen direkt an die Druckerei liefern. Der Chefredakteur hat keine Ahnung, ob seine Werbepartner Autos, nackte Haut oder Bombenbauanleitungen in die Zeitschrift drucken oder ob ein Dritter die Werbung gegen Rasierklingen ausgetauscht hat, die automatisiert ins Heft geklebt werden. Online passiert aber genau das: Webseiten werden ausgeliefert, und ein Werbenetzwerk gibt irgendwelche Inhalte dazu.

Von der Verantwortung dafür freisprechen können sich die Webseitenbetreiber allerdings nicht, denn erst durch den von ihnen eingebauten Code auf der Webseite wird der Browser auf Nutzerseite dazu gebracht, die Inhalte der Werbeanbieter zu laden (Tz. 7.1). Dass ein Nutzer durch den Klick auf eine Webseite weitere Zugriffe seines Browsers auf eine Vielzahl von Servern auslöst, entspricht zumeist nicht seiner Erwartung, ist aber in der heutigen Realisierung vieler Angebote üblich.

Solange Webseitenbetreiber ihren Besuchern Inhalte von Dritten präsentieren, bleiben Werbeblocker ein unerlässliches Mittel zum Selbstschutz. Das Blockieren von Werbung mag unter Wertschöpfungsaspekten für die Betreiber von Webseiten misslich sein, unter Datenschutz- und Datensicherheitsaspekten betrachtet ist das Unterbinden von solchen Inhalten geboten, die Dritte unkontrolliert an den eigenen Rechner übertragen.

Werbeblocker werden aber nicht nur aufgrund der Interessenskollision mit den Webseitenbetreibern kritisiert. Ähnlich wie WOT versuchen auch einige Anbieter von Werbeblockern, aus der Browser-Erweiterung Kapital zu schlagen. Beispielsweise leiten einige Anbieter bestimmte Werbung trotz aktivierten Blockers durch. Das Problem unkontrollierter Drittinhalte lösen solche Konzepte nicht. Daher ist es ratsam, eine Erweiterung zu verwenden, die Drittanbieter-Inhalte ohne Rücksicht auf finanzielle Interessen blockiert. Die Erweiterung „uBlock Origin“ z. B. ist sowohl für Firefox als auch Chrome verfügbar. Hier lassen sich neben Werbefiltern auch spezielle Tracking-Filter auswählen.

Was ist zu tun?

Browser-Erweiterungen können den Datenschutz der Nutzerinnen und Nutzer deutlich verbessern. Vorsicht ist aber bei der Auswahl geboten, da nicht jedes Angebot vertrauenswürdig ist.

10.2 Webseitenverschlüsselung – HTTPS wird immer moderner

Das Protokoll HTTP zur Übertragung von Webseiten ist allgemein geläufig. Die meisten kennen auch die abgesicherte Variante HTTPS. Wer bisher allerdings dachte, man müsse nur beim Online-Banking und beim E-Mail-Abruf auf das „s“ hinter dem „http“ achten, hinkt allerdings der Zeit deutlich hinterher.

Lauschangriffe auf Abrufe von Webseiten sind inzwischen an der Tagesordnung. In vielen größeren Netzen ist irgendein Gerät mit Schadsoftware infiziert, die versucht, alles mitzuschneiden, was nur irgendwie geht. Oft sind diese infizierten Geräte zu sogenannten Bot-Netzen verbunden, in denen gesammelte Daten fleißig ausgetauscht und schließlich von den Betreibern dieser Schadnetze missbraucht oder verkauft werden. Schon deshalb geht die Entwicklungsrichtung im Internet erfreulicherweise klar in die Richtung, jegliche Datenübertragung sicher zu verschlüsseln, und zwar nicht nur auf dem Übertragungsweg zwischen zwei Servern, sondern wirklich „Ende zu Ende“.

Forward Secrecy

Mit „Forward Secrecy“ wird der Schlüssel eines Kryptozertifikats nur genutzt, um für jede Verbindung einen einmaligen individuellen Schlüssel zwischen Browser und Server auszuhandeln, der nicht gespeichert wird. Auf diese Weise können auch ausgespähte und aufgezeichnete Verbindungen später nicht mehr entschlüsselt werden, selbst wenn das Kryptozertifikat unbefugt ausgelesen wird, da jede Verbindung einen anderen Schlüssel nutzt.

Die dauerhafte Nutzung verschlüsselter Protokolle für alle Verbindungen kann serverseitig erzwungen werden, beispielsweise durch „Strict Transport Security-Header“ – dies kann man durchaus als Stand der Technik bezeichnen. Nicht nur unter Sicherheitsaspekten ist dies der richtige Schritt. Auch zur Sicherstellung der Auffindbarkeit der eigenen Webseiten sollte man auf HTTPS setzen: Der Suchmaschinenbetreiber Google hatte bereits 2014 angekündigt, die Nutzung von HTTPS als Faktor in die Bewertung aufzunehmen; unverschlüsselte Seiten landen bei den Suchergebnissen daher seit einiger Zeit im Zweifel weiter unten. Auch die Browser-Hersteller ziehen die Daumenschrauben an: Wenn Webseiten Formulardaten wie Passwörter unverschlüsselt übertragen wollen, bekommen die Nutzer eine unschöne Warnmeldung angezeigt. Gleichzeitig sind die Kosten für eine Umstellung auf HTTPS inzwischen so deutlich gesunken (teilweise sogar kostenfrei), dass auch finanziell einer Umstellung nichts mehr entgegensteht. Wichtig ist zudem der Einsatz von „Forward Secrecy“-Methoden.

Auch Sicherheitsmechanismen können technisch unterwandert und die Verschlüsselung aufgebrochen werden: Dabei wird der Datenverkehr durch einen Proxy geleitet und dem Browser ein anderes Zertifikat untergeschoben, als vom Server gesendet wurde. Solche Proxys können durch Dritte zum unbefugten Mitlesen genutzt werden, etwa in autokratischen Staaten. Sie werden aber auch als „Sicherheitsproxys“ durch Organisationen eingesetzt, die damit ihren Datenverkehr im Namen der IT-Sicherheit untersuchen wollen. Auch sogenannte Antivirensoftware bietet teilweise entsprechende Funktionalitäten an – mit haarsträubenden Resultaten. Das Aufbrechen der Verschlüsselungen durch solche Man-in-the-Middle-Angriffe, wie sie in der Fachsprache heißen, hebelt gleich eine ganze Reihe von Sicherheitsfunktionalitäten aus. Nutzerinnen und Nutzer können beispielsweise nicht mehr erkennen, ob sie nach außen mit dem richtigen Server verbunden sind, und geben womöglich sensible Daten Angreifern preis, die dies ausnutzen. Experten fanden zudem diverse Angriffsmöglichkeiten auf Systeme, die ohne das Zwangsaufbrechen der Verschlüsselung nicht möglich gewesen wären. Deshalb werden zunehmend Maßnahmen auf Webservern und auf Clients eingesetzt, die solche Verschlüsselungsunterbrechungen entweder verhindern oder für die Nutzenden zumindest erkennbar machen.

TLS

„Transport Layer Security“ ist ein Verschlüsselungsprotokoll zur Datenübertragung im Internet. TLS ist der Nachfolgestandard von SSL („Secure Socket Layer“).

Erfreulicherweise sehen die Kryptostandards immer mehr Methoden vor, um sich gegen etwaige Angriffe abzusichern. Aktuell wird für HTTPS der SSL-Nachfolger TLS in der neuen Version 1.3 in Server und Clients implementiert. Darin wird einigen möglichen Angriffswegen entgegengewirkt, und Algorithmen, die inzwischen als nicht mehr hinreichend sicher gelten, werden ausgemustert. Wichtig für Administratoren: Auch beim Einsatz moderner Kryptoverfahren kann man Fehler machen, indem man z. B. zu kurze Schlüssel wählt. Für den Einsatz von TLS auf Webservern (und auch Mailservern) sind Schlüssel, die kürzer als 2048 Bit sind, inzwischen als zu kurz anzusehen. Das ULD empfiehlt hier aktuell eine Schlüssellänge von 4096 Bit.

Was ist zu tun?

Webserver müssen auf HTTPS umgestellt werden. Es ist durchgängig zu gewährleisten, dass gebrochene Verschlüsselungsmethoden nicht mehr verwendet werden. Methoden wie „Strict Transport Security“ zum Erzwingen verschlüsselter Verbindungen oder „Forward Secrecy“ zum Schutz vor nachträglicher Entschlüsselung sind Stand der Technik; ihr Einsatz ist dringend angeraten. Auch bei Mailservern muss TLS-Verschlüsselung zumindest optional verfügbar sein (opportunistisches SSL/TLS). IT-Systeme, die keine aktuelle Verschlüsselung unterstützen, müssen umgehend ersetzt werden.

10.3 Windows 10 – Datenabfluss by Design

Mit Windows 10 verabschiedet sich Microsoft vom Konzept des PC-Betriebssystems als eigenständigem Programm auf der Festplatte des Kunden. Stattdessen verwebt der Hersteller einen klassischen Betriebssystemkern mit diversen Online-Komponenten, um eine geräteübergreifende Nutzung zu ermöglichen. Viel ist von „Personalisierung“ von Windows die Rede, wobei eine klassische, lokale Nutzung des Betriebssystems im neuen Microsoft-Kosmos nicht mehr vorkommt. Um die Personalisierung nach Redmonder Lesart voranzutreiben, benötigt so ein Cloud-Betriebssystem-Hybrid natürlich vor allem eines: Daten über den Nutzer. Schon während der Installation lässt sich Microsoft das Abgreifen verschiedenster Nutzerinformationen per Klick bestätigen – durch stets voreingestellte Freigaben und verbrämt als „Expresseinrichtung“. Die Optionen zum Deaktivieren dieser Weitergabe verbirgt der Konzern in winzigen Links. „Datenabfluss by Design“ könnte man böswillig sagen, denn Datensparsamkeit und Transparenz sehen anders aus. Besonders problematisch ist in diesem Kontext die Übermittlung der Telemetriedaten, die der Nutzer nur reduzieren, nicht aber abschalten kann (https://docs.microsoft.com/de-de/windows/configuration/configure-windows-telemetry-in-your-organization).

Für datenschutzbewusste Privatnutzer, die Windows 10 einsetzen wollen, ist es unerlässlich, zumindest die von Microsoft gewährten Einstellungsmöglichkeiten auszuschöpfen, um beispielsweise die Identifikation durch eine dauerhafte Werbe-ID zu unterbinden. Wer im Rahmen der Expresseinrichtung die diversen Datenweitergaben genehmigt hat, kann diese an verschiedenen Stellen der Systemsteuerung nachträglich deaktivieren.

Telemetriedaten

Der Begriff „Telemetriedaten“ ist nicht fest definiert. Microsoft versteht darunter detaillierte Daten zur Hardware, zur Konfiguration des Betriebssystems, zu installierter Software einschließlich deren Nutzungsmuster, Fehlermeldungen (insbesondere von Treibern) bis hin zu Eingaben in Suchfeldern des Browsers (bei der uneingeschränkten Übertragung „Full Telemetry“). In jedem Falle werden Device-IDs von Geräten und Komponenten übertragen.

Aber Microsoft lässt eben nicht bei allen Datenübertragungen eine vollständige Deaktivierung mit Bordmitteln zu. Mittlerweile gibt es mehrere Programme, die solche Datenübertragungen zu unterbinden versuchen. Dass Nutzer dem Windows-System mit Tools zu Leibe rücken müssen, um es nach eigenen Vorstellungen wenigstens einigermaßen zum Schweigen zu bringen, ist zwar nichts Neues. Der Umfang, in dem Microsoft Daten bis hin zum Tippverhalten einsammelt, ist jedoch erstaunlich.

Für Behörden und Unternehmen, die der Übertragung von Daten ihrer Beschäftigten an Microsoft kritisch gegenüberstehen und trotzdem Windows 10 einsetzen möchten, bietet der Hersteller die Enterprise-Version für den sogenannten „Long Term Service Branch“ (LTSB) an. Eigentlich für geschäftskritische Systeme (z. B. Datenbankserver, Geldautomaten oder Krankenhausinformationssysteme) gedacht, zeichnet sich diese Version neben der Abwesenheit der persönlichen (und vor allem datenhungrigen) Assistenzsoftware Cortana vor allem

durch einen relativ fixierten Funktionsumfang aus: Wo das normale Windows 10 regelmäßig ohne Zutun des Nutzers um neue Funktionen und Programme ergänzt wird, ist der Umfang von Windows 10 LTSB für mindestens zwei Jahre stabil. Leider ist die LTSB-Version den Volumenlizenzkunden vorbehalten. Für kleine und mittelständische Unternehmen oder gar Privatanwender existiert kein vorgesehener Bezugsweg für diese Version. Dabei ist ein fixierter Funktionsumfang eigentlich generell erstrebenswert, bergen doch neue Programme und Funktionen stets Risiken, die gegen einen eventuellen Nutzen abgewogen werden müssen.

An Cortana zeigt sich gut das Dilemma der heutigen Gestaltung von Diensten: Statt lokal mit eingeschränkter Datenbasis zu arbeiten, wird die Datenverarbeitung in die Cloud verschoben, wo die Programme auf viel mehr Daten zurückgreifen können – gespeist aus den Systemen bei allen Kunden. Durch die unterschiedlichen Identifier, angefangen von der Geräte-ID über das Microsoft-Konto bis hin zur Werbe-ID, hat Microsoft enorme Verkettungsmöglichkeiten. Rund zwei Jahre nach dem Erscheinen der ersten Version veröffentlichte Microsoft im April 2017 auch eine Liste der Daten, die das Betriebssystem standardmäßig überträgt (https://docs.microsoft.com/de-de/windows/configuration/windows-diagnostic-data). Das Beispiel der mangelhaften Anonymisierung von Nutzerdaten im Falle des WOT-Plug-ins (Tz. 10.1) lässt erahnen, welches Potenzial die Datenberge in Redmond besitzen.

Mit Windows 10 schafft Microsoft eine Basis für künftige Dienstleistungsgeschäfte. Das Betriebssystem mutiert zu einer Plattform, die der Konzern nach Belieben umbauen und auf seine Bedürfnisse (wohlgemerkt die des Konzerns, nicht notwendigerweise auch des Kunden) zuschneiden kann. Microsoft ist kein Einzelfall – auch die anderen großen Anbieter gehen diesen Weg, bei dem es für die Nutzenden immer schwieriger wird, die Kontrolle über ihre Daten zu behalten.

Was ist zu tun?

Wer Windows 10 nutzen möchte, muss sich mit den Datenübertragungen des Systems intensiv auseinandersetzen. Der sich ständig ändernde Funktionsumfang macht Risikoabwägungen volatil: Ein Update kann Funktionen oder Einstellmöglichkeiten modifizieren, hinzufügen oder entfernen. Die am wenigsten invasive Version LTSB bleibt Volumenlizenzkunden vorbehalten. Nicht nur am Beispiel Windows 10 zeigt sich, dass Hersteller und Anbieter umdenken und ihre Systemgestaltung nach den Prinzipien „Datenschutz by Design“ und „by Default“ ausrichten müssen, wie es die Datenschutz-Grundverordnung fordert.

10.4 Metadaten und Schwärzungen in PDF-Dateien

Das PDF-Format wurde 1993 als Papieräquivalent entworfen. Es sollte die gleiche Verlässlichkeit wie ein klassischer Ausdruck bieten und sich unabhängig vom Endgerät stets gleich darstellen lassen. Oberflächlich betrachtet wird dieses Ziel auch erreicht. „Unter der Haube“ jedoch tragen PDF-Dokumente deutlich mehr Informationen, als man es von digitalem Papier erwarten würde. Wird beispielsweise ein Word-Dokument in das PDF-Format überführt, landen in der Regel der Dateiname der Word-Datei sowie der Bearbeiter und die verwendete Software als sogenannte Metadaten im Dokument.

Speziell der Dateiname kann mitunter Informationen enthalten, die besser nicht an den Empfänger des PDF-Dokuments gelangen sollten. Aber auch ganze Dateipfade finden ihren Weg in die Metadaten und lassen so unnötige Rückschlüsse auf die interne Organisationsstruktur zu. Wer ein PDF-Dokument nachträglich in seinen Abmessungen beschneidet, ist eventuell überrascht, dass die weggeschnittenen Bereiche nicht wegfallen, sondern nur ausgeblendet sind. Der Empfänger kann sie dann leicht rekonstruieren.

Metadaten in Dokumenten

Metadaten sind zusätzliche (Verwaltungs-) Informationen in Dokumenten, die über den Inhalt hinausgehen. Beispiele sind Dokumententitel, Verfasser, Thema und Stichwörter, Copyright-Informationen, aber auch Dateinamen und Dateipfade, Berechtigungen, Benutzername des technischen Erstellers der Datei (dies ist nicht immer der Verfasser des Dokuments), der zugrunde liegende Dateiname bei der Konvertierung etwa einer Word-Datei in eine PDF-Datei.

Es gibt eine Reihe von Tools, die versprechen, Dokumente zu bereinigen. Das klappt in der Regel für die eingangs erwähnten Informationen zum Ersteller oder zum ursprünglichen Dateinamen. Aber oft fördert schon ein Öffnen der vermeintlich bereinigten Dokumente mit einem simplen Texteditor diese Informationen wieder zutage. Das zugrunde liegende Problem ist die inkrementelle Speicherung der Metadaten im PDF-Dokument. Vereinfacht gesagt speichern viele Tools die Änderungen lediglich zusätzlich zu den bestehenden, die dann als „gelöscht“ markiert, nicht aber wirklich entfernt werden.

Ein definitiv verlässlicher Weg, PDF-Dokumente für die Weitergabe aufzubereiten, ist die Aktion „Vertrauliche Dokumente veröffentlichen“ von Adobe Acrobat. Hierbei wird das Dokument komplett neu erzeugt und um sämtliche unerwünschten Inhalte bereinigt.

Eine weitere Fehlerquelle bei der Weitergabe von PDF-Dokumenten ist das Schwärzen sensibler Daten. Hier ist darauf zu achten, dass nicht lediglich Objekte vor den Text gelegt werden. Ein schwarzer Kasten über Buchstaben mag diese bei der Bildschirmanzeige verdecken; solange jedoch der Text im Dokument noch existiert, lassen sich diese darüberliegenden Objekte einfach wieder entfernen. Wichtig ist daher, dass Schwärzungen den zu tilgenden Text nicht überlagern, sondern mit diesem verschmolzen werden. Adobe Acrobat bietet hier mit dem Werkzeug „Inhalt schwärzen und entfernen“ eine zuverlässige Funktion.

Was ist zu tun?

Sollen Tools zum Entfernen von Metadaten oder Schwärzen zum Einsatz kommen, ist sicherzustellen, dass dies wirkungsvoll umgesetzt wird. Insbesondere Metadaten-Löscher sind bei unseren Tests negativ aufgefallen.

10.5 Home Smart Home

Vernetzte Elektronik im Haushalt geht zunehmend hinaus über den PC und das Smartphone. Immer mehr Geräte kommunizieren untereinander oder mit externen Dienstleistern, um dem Nutzer mehr oder minder sinnvolle Funktionen zu bieten. Moderne Heizungsanlagen beispielsweise begnügen sich nicht mit einer programmierten Nachtabsenkung oder einer schnöden Urlaubsschaltung. Sensorgesteuert erfassen sie die Anwesenheit der Bewohner und kalkulieren so die beste Zeit zum Heizen. Alle Daten sind von unterwegs per Smartphone einzusehen, alle Funktionen online steuerbar. Und ganz nebenbei erfährt so auch der Hersteller der eigenen Heizung, wann zu Hause jemand duscht.

Ähnlich verhält es sich mit allen Anlagen zur Heimautomation, die serverbasiert Daten der Nutzenden verarbeiten: Die Dienstbetreiber erhalten systematisch Einblick in den Alltag ihrer Kundschaft. Wenig überraschend ist mit der Firma „Nest“ ein Anbieter selbstlernender Heizungsthermostate seit 2014 in der Hand von Google. Dort hat man früh erkannt, dass der Alltag der Menschen noch viele ungenutzte Datenschätze birgt.

Unter dem Stichwort „Smart“ versucht die Industrie seit geraumer Zeit, Produkte an Mann und Frau zu bringen, die durch ihre Lernfähigkeit das Leben vereinfachen sollen. Die Risiken zunehmender Vernetzung werden dabei gern verschwiegen. Zum einen ist der Datenfluss oft unklar und nur durch lange, versteckte Daten-

schutzerklärungen zu entwirren. Zum anderen sind die Datenverbindungen der heimischen Geräte keine Einbahnstraße. Jede Verbindung eines Geräts nach außen bedeutet, dass dieses Gerät potenziell auch von außen angesprochen werden kann. Haben die Schutzmechanismen gegen solchen unbefugten Zugriff von außen Lücken, bietet die Heimautomatisierung Fremden unter Umständen willkommene Informationen und Steuerungsmöglichkeiten. Einen Blick durch die Überwachungskamera im Wohnzimmer oder die Information der Heizung, dass niemand zu Hause ist, möchten die wenigsten Kunden einem Unbekannten gewähren.

https://datenschutzzentrum.de/artikel/1071-1.html

Was ist zu tun?

Vor allem die Abhängigkeit zum Anbieter, in die die Kunden sich zwangsweise begeben, muss hinterfragt werden: Sicherheitslücken in der Software einer Heimautomation können nur vom Hersteller behoben werden. Klare Verantwortlichkeiten sind ebenso nötig wie Aufklärung über die realen Risiken.

10.6 Absicherung von Online-Diensten mit Zwei-Faktor-Authentifizierung

Passwörter sind lästig. Außerdem bedeuten Passwörter ein Sicherheitsrisiko: Wer beispielsweise die Zugangsdaten zu einem Online-Dienst ausspäht, kann diesen nutzen und komplett übernehmen, ohne dass der rechtmäßige Besitzer des Kontos davon erfährt. Beim Online-Banking setzt man schon von Anfang an auf mehrere sogenannte Faktoren. Neben dem „Wissen“, nämlich dem klassischen Passwort, kam hier stets auch der Faktor „Besitz“ zum Einsatz: zu Beginn die klassische TAN-Liste, später dann Varianten wie kleine Bildschirmscanner, TAN-Generatoren bis hin zum heutigen Smartphone. All diesen Techniken ist gemein, dass sie einen Missbrauch deutlich erschweren. Ein Angreifer muss nicht nur das Passwort ausspähen, sondern auch „Hardware“ in Form der TAN-Liste oder des Smartphones in seinen Besitz bringen. Im Unterschied zum Passwort können Betroffene den Verlust eines Stücks Hardware allerdings sofort bemerken.

Inzwischen bieten auch Online-Dienste vermehrt die Möglichkeit an, das eigene Konto zusätzlich durch einen zweiten Faktor zu sichern. Verbreitete Verfahren nutzen den Time-based One-Time Password algorithm (TOTP) der Standardisierungsinitiative Open Authentication (OATH), bei dem eine Smartphone-App zeitbasierte Authenticator-Codes erzeugt, die jeweils nur 30 Sekunden lang gültig sind (sogenannte Einmalpasswörter mit zudem zeitlich beschränkter Gültigkeit).

Initiative for Open Authentication (OATH)

OATH ist eine branchenübergreifende Initiative, die eine offene Referenzarchitektur für Authentisierungsverfahren entwickelt und dabei verschiedene Algorithmen standardisiert, so auch TOTP. Ziel ist es u. a., dass Nutzende sich mit einem einzelnen Gerät oder einer einzelnen Software (z. B. einer Smartphone-App) bei einer Vielzahl von Diensten authentisieren können.

Time-based One-Time Password algorithm (TOTP)

TOTP ist ein Algorithmus, mit dem aus der aktuellen Uhrzeit und einem Initialisierungscode Passwörter mit begrenzter Gültigkeitsdauer berechnet werden können. Dies erfolgt sowohl beim Benutzer (z. B. mit einer Smartphone-App) als auch auf der Serverseite. Der Initialisierungscode ist einmalig, ähnlich der Ersteinrichtung eines Passworts, zwischen Benutzer und Server zu vereinbaren. Bei jeder Authentisierung werden daraus neue, zeitlich befristete Passwörter generiert: auf der Nutzerseite für das Anmelden, auf der Serverseite für die Kontrolle.

Will sich ein Nutzer bei einem so gesicherten Online-Dienst anmelden, muss er zusätzlich zu Nutzernamen und Passwort den aktuellen Authenticator-Code angeben. Wer den Einmal-Code abgreift, kann damit nach Ablauf des 30-Sekunden-Zeitfensters nichts anfangen. Weitere Verfahren setzen auf die Übermittlung des Einmalcodes per SMS oder erfordern die Verwendung eines dedizierten USB-Tokens.

Unabhängig vom verwendeten Verfahren bietet die Zwei-Faktor-Authentifizierung entscheidende Vorteile. Die Kompromittierung eines Online-Kontos wird dadurch erheblich erschwert, sodass derartige Verfahren unbedingt verwendet werden sollten, wenn persönliche Daten auf dem Spiel stehen. Google, Apple und Microsoft bieten inzwischen die Möglichkeit zur Zwei-Faktor-Authentifizierung. Smartphone-Nutzerkonten mit ihren Bezahlfunktionen und Unmengen an personenbezogenen Daten sollten daher unbedingt zusätzlich abgesichert werden. Aber auch für alle anderen Dienste sollte – sofern unterstützt – die entsprechende Option aktiviert werden.

Für digitale Klassenbücher des Landes schreibt § 17 Absatz 3 der Datenschutzverordnung Schule die Nutzung einer Zwei-Faktor-Authentifizierung vor. Das ULD ist in einer Arbeitsgruppe mit Herstellern und Schulen vertreten, um praxistaugliche Umsetzungen zu untersuchen, die auch unter Schulbedingungen funktionieren.

10.7 Datenschutz unter dem Weihnachtsbaum – Tipps gegen Risiken bei Geschenken

Im Dezember 2016 hat das ULD viele Erkenntnisse aus den eigenen Arbeiten, besonders im IT-Labor, zusammengefasst, um Datenschutztipps für typische Weihnachtsgeschenke zu geben. Schließlich beinhalten viele Produkte, die am 24. Dezember unter dem Weihnachtsbaum liegen, eine gewisse Überwachungsfunktionalität. Dazu können Haushaltshelfer, Entertainment-Geräte, Gesundheitsprodukte oder Technik-Gadgets gehören. Die Hinweise des ULD stehen auf der Webseite zur Verfügung:

https://datenschutzzentrum.de/artikel/1071-1.html

Dort erfahren alle Interessierten, worauf sie für ein Weihnachtsfest ohne Datenschutzrisiken besonders achten sollten – vom sicheren Online-Einkauf über die Inbetriebnahme der technischen Geschenke bis hin zum Verschicken von Weihnachtsgrüßen per Messenger. Drohnen, Smart-TV-Geräte und Fitness-Wearables spielen aber nicht nur zu Weihnachten eine große Rolle.

Ob nun Geschenk oder nicht: Bei technischen Produkten sollte man mindestens Folgendes prüfen: Werden Daten gespeichert und übertragen? Wenn ja: An wen und zu welchem Zweck? Kann man solche Datensammlungen und -weiterleitungen verhindern?

Jedes Gerät, das mit dem Internet verbunden ist, muss gegen unberechtigte Zugriffe von außen abgesichert werden. Selbst vernetztes Spielzeug kann Opfer eines Angriffs aus dem Internet werden. Deswegen sollte man nicht auf die vorkonfigurierte Einstellung vertrauen, sondern muss zumindest Standardpasswörter unbedingt ändern und Verschlüsselung einschalten, wo es geht.

Aber dem ULD ist auch wichtig, dass die Verantwortung für Datenschutz und IT-Sicherheit nicht auf die Nutzerinnen und Nutzer abgeladen wird. Stattdessen sind die Hersteller und Anbieter gefragt, die Datenschutzrisiken einzudämmen. Damit wird hoffentlich das Schenken ohne (Datenschutz-)Reue viel einfacher.

Was ist zu tun?

Produkte und Dienste sollen mit datenschutzfreundlichen Voreinstellungen ausgeliefert werden. Der eingebaute Datenschutz ist heutzutage auf dem Markt leider noch nicht verbreitet. Das muss sich aber ändern – spätestens mit der Datenschutz-Grundverordnung, die ab Mai 2018 Datenschutz „by Design“ und „by Default“ fordert.

11

KERNPUNKTE

Safe Harbor und Privacy Shield

Grenzüberschreitende Kooperation bei Datenpannen

Reifegrad datenschutzfördernder Technik

11 Europa und Internationales

11.1 Safe-Harbor-Entscheidung des Gerichtshofs der Europäischen Union

In seinem Urteil vom 06.10.2015, C-362/14 (Schrems) hat der Gerichtshof der Europäischen Union (EuGH) die sogenannte Safe-Harbor-Entscheidung der Europäischen Kommission für ungültig erklärt. Während die darin geregelte Selbstzertifizierung US-amerikanischer Unternehmen bisher als Grundlage für Datenübermittlungen in die USA genutzt werden konnte, ist dies mit Verkündung des Urteils nicht mehr zulässig. Damit wurde einer großen Zahl von Datenübermittlungen in die USA die Rechtsgrundlage entzogen. Weitere mögliche Rechtsgrundlagen für eine grenzüberschreitende Datenübermittlung wie Binding Corporate Rules (BCRs), Standardvertragsklauseln sowie die Einwilligung stehen seitdem auf dem Prüfstand.

Behandlung der Schrems-Beschwerde

Der Österreicher Max Schrems hatte im Juni 2013 beim Datenschutzbeauftragten Irlands Beschwerde gegen das Unternehmen Facebook Inc. eingelegt, mit dem Ziel, dem Unternehmen zu untersagen, seine personenbezogenen Daten in die USA zu übermitteln. Er machte geltend, dass das Recht und die Praxis der USA für die übermittelten Daten keinen ausreichenden Schutz gegen die Überwachungstätigkeiten der dortigen Behörden böten. Er verwies dabei auf die von Edward Snowden enthüllten Tätigkeiten der Nachrichtendienste der USA, insbesondere der National Security Agency (NSA).

Die irische Datenschutzaufsichtsbehörde wies die Beschwerde zurück. Daraufhin erhob Schrems Klage vor dem Irish High Court, der das Verfahren aussetzte und dem EuGH ein Vorabentscheidungsersuchen vorlegte.

Bereits in der Vergangenheit hat das ULD auf Schutzlücken für die Grundrechte der Bürgerinnen und Bürger im Safe-Harbor-Verfahren hingewiesen (35. TB, Tz. 11.3). Auch die Europäische Kommission benannte bereits 2013 diverse Schutzlücken ihrer Safe-Harbor-Entscheidung. Mit Blick auf diese Feststellungen der Kommission macht der EuGH in seinem Urteil deutlich, dass das Safe-Harbor-Verfahren keine ausreichende Begrenzung der Zugriffe von staatlichen Behörden auf personenbezogene Daten aus Europa bewirke. Ebenso fehle es in der Safe-Harbor-Entscheidung an jeder Feststellung über ausreichende Rechtsschutzmöglichkeiten für EU-Bürgerinnen und Bürger. Ohne das Rechtssystem der USA konkret zu bewerten, stellt der EuGH abstrakt fest, dass nationale Regelungen, die es generell gestatten, auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des Grundrechts auf Achtung des Privatlebens verletzen. Zudem schränke die Safe-Harbor-Entscheidung die Aufsichtsbefugnisse der europäischen Datenschutzaufsichtsbehörden zu sehr ein.

Für die Rechtmäßigkeit jeder Übermittlung von personenbezogenen Daten in ein Land außerhalb der EU oder des EWR ist u. a. maßgeblich, dass in diesem Land oder beim Empfänger ein vergleichbares Schutzniveau besteht. Dies ist nach Auffassung des EuGH dann grundsätzlich nicht der Fall, wenn ein genereller, uneingeschränkter Zugriff der staatlichen Behörden auf elektronische Kommunikation erfolgen darf. Ein solcher genereller Zugriff würde gegen den Wesensgehalt von Artikel 7 der Grundrechtecharta der Europäischen Union verstoßen. Haben EU-Bürgerinnen und -Bürger zudem keine Möglichkeit, von dem Zugriff zu erfahren und dagegen gerichtlichen Rechtsschutz in Anspruch zu nehmen, läge ein Verstoß gegen Artikel 47 der Grundrechtecharta vor.

Soll eine Übermittlung in ein sogenanntes Drittland ohne angemessenes Datenschutzniveau auf Basis einer Einwilligung des Betroffenen erfolgen, erfordert dies nicht nur eine Aufklärung über die konkreten Zwecke, sondern auch über die Risiken der Datenverarbeitung bzw. den damit verbundenen Verzicht auf ein gleichwertiges bzw. angemessenes Schutzniveau. Der Betroffene müsste daher zunächst umfassend über das fehlende Schutzniveau, vor allem über US-staatliche Zugriffsbefugnisse, fehlende Rechtsschutzmöglichkeiten und Betroffenenrechte, die Weiterverarbeitung der Daten ohne Zweckgebundenheit, die Nichtgeltung des Erforderlichkeitsgrundsatzes sowie über fehlende staatliche Kontrollmecha-

nismen in den USA aufgeklärt werden. Eine informierte Einwilligung würde erfordern, dass der Betroffene daraufhin abschätzen können müsste, was die anlasslose Massenüberwachung durch Geheimdienste und die US-staatlichen Zugriffsmöglichkeiten für ihn bedeutet. Doch dies ist kaum möglich: Vielleicht gerät er – für ihn unvorhersehbar – aufgrund seiner Bekanntschaften, wegen einer Aussage in sozialen Medien oder durch die Kommunikation seiner Interessen (beispielsweise auf einem „Wunschzettel“ („Wishlist“) bei einem Internetanbieter) in den Fokus und muss mit Nachteilen rechnen.

Sollen personenbezogene Daten auf der Grundlage von Standardvertragsklauseln übermittelt werden, hat der Empfänger im Drittland gegenüber dem europäischen Datenexporteur u. a. zu garantieren, dass er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen. Können US-amerikanische Vertragspartner mit Blick auf das in den USA geltende Recht die Verpflichtung nicht einhalten, so ist der Datenexporteur in derartigen Fällen berechtigt, die Datenübermittlung auszusetzen oder den Standardvertrag zu kündigen. Gleiches gilt für die Übermittlung personenbezogener Daten an Auftragsverarbeiter.

Gegenwärtig ist auch fraglich, ob Standardvertragsklauseln als Grundlage für eine Datenübermittlung dienen können, da deren Status als ausreichende Garantie im Datentransfer mit Drittstaaten derzeit Gegenstand einer gerichtlichen Klärung ist. Auf Initiative der irischen Datenschutzaufsichtsbehörde hin ist der Irish High Court mit dieser Frage befasst. Eine Vorabentscheidung durch den EuGH ist wahrscheinlich.

Es ist darauf hinzuwirken, dass die USA ebenso wie andere Staaten mit Datenimporteuren innerstaatliche Rechtsvorschriften oder internationale Verpflichtungen vorweisen, die ein angemessenes Schutzniveau bei der Verarbeitung personenbezogener Daten für Betroffene bieten. Dazu gehört ein wirksamer gerichtlicher Rechtsschutz gegen Eingriffe in das Grundrecht auf informationelle Selbstbestimmung. EU-Bürgerinnen und EU-Bürger müssen die Möglichkeit haben, Zugang zu ihren personenbezogenen Daten zu erlangen und gegebenenfalls gerichtlichen Rechtsschutz in Anspruch zu nehmen.

Was ist zu tun?

Es ist sicherzustellen, dass der Grundrechtsschutz der Betroffenen bei Übermittlungen in Drittstaaten dem Schutzniveau der EU angemessen ist. Die Safe-Harbor-Entscheidung des EuGH bietet hierfür keine Grundlage. Bezüglich der Verwendung von Standardvertragsklauseln wird von der irischen Datenschutzaufsichtsbehörde derzeit eine gerichtliche Klärung angestrebt. Eine vorbehaltlose Vereinbarung der Standardvertragsklauseln kann daher gegenwärtig nicht empfohlen werden.

11.2 Safe-Harbor-Nachfolger – Privacy Shield

Nachdem der EuGH den Safe-Harbor-Beschluss für nichtig erklärt hatte (Tz. 5.1 und 11.1), schuf die Europäische Kommission eine Ersatzregelung in Form des Privacy Shield. Sie hat mit Beschluss vom 12. Juli 2016 das durch das Privacy Shield in den USA erreichte Datenschutzniveau als angemessen anerkannt.

Da dieser Beschluss bindend ist, kann das Privacy-Shield-Abkommen nun trotz der von den Datenschutzbehörden geäußerten Kritik an den Regelungen von verantwortlichen Stellen als Rechtsgrundlage genutzt werden, um Daten aus der EU an die zertifizierten Unternehmen zu übermitteln. Die für den Datenexport verantwortlichen Stellen müssen darauf achten, dass das Unternehmen, das die Daten empfängt, auch tatsächlich auf der Liste des US-Handelsministeriums eingetragen ist. Es ist zudem sicherzustellen, dass sich die Zertifizierung auch auf die jeweilige Kategorie von Daten (Beschäftigtendaten („HR“) oder sonstige Daten („non HR“)) bezieht, die übermittelt werden soll.

Privacy Shield

Als Nachfolger von „Safe Harbor“ („Sicherer Hafen“) wurde das EU-US-Abkommen „Privacy Shield“ („Datenschutzschild“) ausgehandelt. Darin werden Zusicherungen an den Schutz personenbezogener Daten, die aus einem EU-Mitgliedstaat an die USA übertragen werden, aufgeführt. Ähnlich dem „Safe Harbor“ handelt es sich um eine Selbsterklärung von US-Unternehmen, bestimmte Datenschutzgrundsätze einzuhalten. Die Unternehmen müssen sich beim US-Handelsministerium (Department of Commerce) registrieren. Im Privacy Shield sind auch Regelungen zu Datenzugriffen durch Behörden enthalten. Bei Beschwerden können sich Betroffene an das jeweilige Unternehmen, an eine Ombudsstelle oder an ihre nationalen Datenschutzbehörden wenden.

Die Datenschutzbeauftragten der EU-Mitgliedstaaten hatten im Vorfeld der Angemessenheitsentscheidung der Kommission auf zahlreiche und erhebliche Schwachstellen des Privacy Shields hingewiesen und dessen Eignung zur Sicherstellung eines angemessenen Datenschutzniveaus infrage gestellt.

Die Artikel-29-Datenschutzgruppe, ein Gremium der Datenschutzaufsichtsbehörden der EU, hat die Kritikpunkte in einer Stellungnahme ausführlich erläutert (WP 238, Opinion 1/2016 on the EU – U.S. Privacy Shield draft adequacy decision), abrufbar unter:

http://www.ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

Mit der Entscheidung der Kommission über die Angemessenheit des durch das Privacy-Shield-Abkommen vermittelten Datenschutzniveaus sind diese Kritikpunkte nicht ausgeräumt, auch wenn diese Entscheidung gültig ist. Viele Bedenken bleiben bestehen, worauf auch die Artikel-29-Datenschutzgruppe in einer Pressemitteilung hingewiesen hat.

http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf

Der Angemessenheitsbeschluss selbst enthält eine Überprüfungsklausel. Danach verpflichtet sich die Europäische Kommission, jährlich zu überprüfen, ob die tatsächlichen und rechtlichen Voraussetzungen für die Annahme eines angemessenen Datenschutzniveaus gegeben sind. Die Artikel-29-Datenschutzgruppe hat angekündigt, an dieser Überprüfung teilzunehmen und zu prüfen, ob die noch offenen Kritikpunkte gelöst wurden und die Schutzmaßnahmen des Privacy Shields tatsächlich wirksam sind. Von diesem Ergebnis wird nach Ankündigung der Artikel-29-Datenschutzgruppe nicht nur die Fortgeltung des Angemessenheitsbeschlusses der Kommission abhängen, sondern es wird möglicherweise auch Auswirkungen auf die anderen Instrumente – Standardvertragsklauseln und verbindliche Unternehmensregelungen – haben.

Weitere Informationen zum Privacy Shield stellt das ULD hier zur Verfügung:

https://datenschutzzentrum.de/artikel/1138-1.html

Was ist zu tun?

Es ist nicht unwahrscheinlich, dass die Entscheidung der Europäischen Kommission zum Privacy Shield vom EuGH überprüft wird. Aufgrund der umfassenden Kritik und der Zweifel an der Rechtmäßigkeit des Privacy Shields liegt es nahe, dass im Falle einer gerichtlichen Prüfung auch diese Entscheidung für nichtig erklärt wird. Es kann daher keine Empfehlung gegeben werden, Selbstzertifizierungen US-amerikanischer Unternehmen auf Basis des entsprechenden Beschlusses vorbehaltlos zu akzeptieren.

11.3 Grenzüberschreitende Übung – Umgang mit Datenpannen

Datenpannen können immer vorkommen – aber was ist, wenn mehrere Nationen betroffen sind? Wie stellt man sicher, dass die Kooperation unter den Datenschutzaufsichtsbehörden in Europa funktioniert, um den Vorfall aufzuklären und die geeigneten Maßnahmen zu treffen? Diese Fragen standen im Mittelpunkt der „Pan-European Data Breach Exercise“ („gesamteuropäische Datenschutzvorfallübung“), an der das ULD mitwirkte.

Ausrichter der Übung war das Joint Research Center Ispra, eine Forschungsstelle der Europäischen Kommission. Dort lagen Erfahrungen mit Übungen im Bereich der Informationssicherheit vor. Diese Übungen werden seit mehreren Jahren durchgeführt und beziehen oft Hunderte von Akteuren in ganz Europa oder darüber hinaus ein. Diese Dimensionen haben wir bei der ersten Übung im Jahr 2015 nicht erreicht: Unsere Beteiligten kamen von den Datenschutzbehörden in Frankreich, Griechenland, Irland, Italien, Polen, Spanien und – für Deutschland – aus Schleswig-Holstein. Zu einem verabredeten Tag probten insgesamt 20 Mitarbeiterinnen und Mitarbeiter aus diesen sieben Ländern über mehrere Stunden einen Übungsfall, in dem es um eine Datenpanne und Meldepflichten nach dem jeweiligen nationalen Datenschutzrecht ging. Die Gesamtdauer der Entwicklung dieses Falls von zwölf Tagen wurde auf acht Stunden komprimiert.

Der Fall war zwar fiktiv, aber keineswegs untypisch (siehe auch Tz. 8.4.2): Im Internet taucht eine Datei mit personenbezogenen Daten auf, die Tausende von Kunden aus mehreren Nationen betreffen. Journalisten und besorgte Bürger fragen bei ihrer jeweiligen Datenschutzbehörde nach; eine offizielle Meldung des Datenschutzvorfalls gibt es zu diesem Zeitpunkt nicht. Einige Datenschutzbehörden und Sicherheitsforscher analysieren die Datei und ermitteln die mutmaßliche Quelle des Datenlecks. Das betroffene Unternehmen hat den Hauptsitz in Deutschland – das ULD erhält also als federführende Datenschutzbehörde die „Hauptrolle“ in dieser Simulation –, aber es ist auch in anderen Mitgliedstaaten aktiv. Zuerst bestreitet das Unternehmen, dass ein Datenschutzvorfall vorliegt, doch findet dann heraus, dass aufgrund eines Sicherheitsproblems der Webseite die Daten online ausgelesen werden konnten. Nun werden die notwendigen Informationen bröckchenweise der zuständigen Datenschutzbehörde zur Verfügung gestellt und die betroffenen Kundinnen und Kunden informiert.

Sobald klar ist, dass mehrere Staaten betroffen sind, tauschen sich die Datenschutzbehörden aus. Sie unterstützen sich bei der Aufklärung sowie bei der Information der Betroffenen, um die Risiken eines Missbrauchs der Daten zu reduzieren. Gar nicht so einfach, weil das Unternehmen in Deutsch kommuniziert, aber die Kommunikation unter den Datenschutzbehörden auf Englisch als kleinstem gemeinsamen Nenner stattfindet. Eine sichere Kommunikationsinfrastruktur unter den Datenschutzbehörden in Europa wird für diese Übung als gegeben vorausgesetzt, ist aber auch im Jahr 2017 noch nicht Realität. Davon unabhängig will ein Sicherheitsforscher weitere Informationen verschlüsselt zusenden, und die verschiedenen Datenschutzbehörden verweisen auf ganz verschiedene Wege, wie man sicher mit ihnen kommunizieren kann. Parallel fragt die Presse immer wieder den jeweiligen Informationsstand ab, der sich ständig ändert. Die Erkenntnisse aus den anderen Ländern werden immer wieder zusammengeführt und für die Information der Presse und der Betroffenen in die jeweilige Nationalsprache übersetzt.

Schließlich ist das Sicherheitsloch geflickt; die Kundinnen und Kunden sind informiert und darauf hingewiesen worden, ihre Passwörter zu ändern; das Unternehmen hat alle nötigen Informationen zur Meldung des Sicherheitsvorfalls nachgereicht. Die Simulation endet. In der echten Welt wäre der Fall nun noch nicht vorbei, sondern die zuständige Datenschutzbehörde würde über Sanktionen und das weitere Vorgehen entscheiden.

Wie bei jeder Übung ging es darum, daraus zu lernen. Natürlich lief nicht alles rund – besonders das exakte Übersetzen von einer in eine andere Sprache ist zeitaufwendig. Alle Beteiligten an der Übung hatten immerhin Englischkenntnisse, was nicht an jedem Arbeitsplatz vorausgesetzt werden kann. Außerdem war im Jahr 2015 beim Durchführen der Übung die Datenschutz-Grundverordnung noch nicht in Kraft. Neben dem verschiedenen Recht in den jeweiligen Mitgliedstaaten bestehen auch Unterschiede in der Praxis der Datenschutzbehörden im Umgang mit den Unternehmen und mit der Presse. Schließlich ist nicht jede Dienststelle so aufgestellt, dass die technischen Details bewertet werden können, die von Journalisten, Sicherheitsforschern oder einem Unternehmen in einer Datenschutzvorfallmeldung angeliefert werden.

Erst recht können viele Datenschutzbehörden oft nicht bereitgestellte Daten – im Fall der Übung war das die kopierte Datenbank mit den Kundendaten – mit eigenem Personal und eigenen Mitteln analysieren.

Ein Ergebnisbericht steht unter einer Open-Access-Lizenz im Internet zur Verfügung:

http://www.sciencedirect.com/science/article/pii/S0267364917300808

Was ist zu tun?

Die Kooperation der Datenschutzbehörden innerhalb von Europa ist von großer Bedeutung, auch im Fall von Datenschutzvorfällen. Jede Dienststelle muss künftig neben der rechtlichen Kompetenz auch gutes Technikwissen, Erfahrungen in Presse- und Öffentlichkeitsarbeit und Englischkenntnisse vorhalten. Spezialanforderungen sollten über ein arbeitsteiliges Vorgehen in der Kooperation untereinander erfüllt werden.

11.4 Kooperation im „Internet Privacy Engineering Network“

Bereits im Jahr 2014 war das ULD an der vom Europäischen Datenschutzbeauftragten initiierten Gründung des „Internet Privacy Engineering Network“ (IPEN) beteiligt. Es handelt sich dabei um ein Netzwerk von Datenschutzexperten, Entwicklern und Forschern, das zum Ziel hat, Datenschutz im Internet und in Anwendungen einzubauen. Zu diesem Zweck sollen Datenschutzanforderungen in allen Phasen des Entwicklungsprozesses von Software, Diensten und Infrastruktur Eingang finden.

In der Anfangszeit stand der Informationsaustausch zu wiederverwendbaren Bausteinen, Designmustern und Lösungen für bestimmte Anwendungsfälle mit Risiko für die Betroffenen im Vordergrund. Das Netzwerk IPEN ist mittlerweile auf zahlreichen Veranstaltungen vertreten, um mit anderen relevanten Initiativen zusammenzukommen und Lösungen zu diskutieren. Künftig sollen die Erkenntnisse in Form einer Wissensdatenbank aufbereitet werden und allen Interessierten zur Verfügung stehen.

https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_de

Was ist zu tun?

Initiativen wie IPEN erhalten mit der Datenschutz-Grundverordnung endlich eine größere Relevanz, weil die jahrelangen Forderungen nach eingebautem Datenschutz nun nicht mehr ignoriert werden können. Wer zu diesem Thema beitragen kann, sollte sich in dem Netzwerk einbringen.

11.5 Privacy Engineering und Reifegrad datenschutzfördernder Technik

Artikel 25 Datenschutz-Grundverordnung fordert „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ (englisch: „data protection by design and by default“). Zwar hat sich die Dienststelle schon seit mehr als 20 Jahren mit dem Thema beschäftigt (z. B. bei der Sommerakademie 1996 zu „Datenschutz durch Technik“). Auch hat die Internationale Konferenz der Datenschutzbeauftragten im Jahr 2010 in einer Resolution zu „Privacy by Design“ betont, dass eingebauter Datenschutz ein wichtiger Bestand-

teil des Datenschutzes ist. Jedoch ist Systemgestaltung mit Datenschutz noch immer eine Seltenheit in informationstechnischen Systemen.

Auf europäischer Ebene beschäftigt sich die Europäische Agentur für Netz- und Informationssicherheit (ENISA) nicht nur mit ihrem Schwerpunkt „Sicherheit“, sondern lädt auch Expertinnen und Experten zu Datenschutztechnikthemen ein. Auf diese Weise konnten ULD-Beiträge in die Studie „Privacy and Data Protection by Design“ (Privatheitsschutz und Datenschutz durch Gestaltung) eingebracht werden, in der ausgehend von den datenschutzrechtlichen Anforderungen ein erster Überblick über Möglichkeiten für datenschutzgerechte Systemgestaltung gegeben wird. In der Anfang 2015 erschienenen Studie werden auch die Gewährleistungsziele des Standard-Datenschutzmodells in Bezug auf eingebauten Datenschutz beschrieben.

Im Ergebnis zeigt sich, dass es bereits vielfältige technische und organisatorische Maßnahmen und Bausteine für datenschutzfördernde Systemgestaltung gibt. Die Studie entwickelt die Idee, Maßnahmen und Bausteine für Datenschutz dokumentiert in einer Datenbank zu sammeln und zur Verfügung zu stellen. Das Spektrum reicht von Konzepten über Prototypen bis zu Produkten, auf die eine solche Datenbank verweisen könnte. Hier könnte sogar Code – beispielsweise Programmierbibliotheken – für Softwareentwicklung bereitgehalten werden.

Allerdings ist es für einen Anwender nicht einfach, den Reifegrad dieser Maßnahmen und Bausteine festzustellen. Auch die Qualität und etwaige unerwünschte Nebeneffekte sind schwer für den Laien abschätzbar. Eine intensive Diskussion findet zwar in der Community der „Privacy-Enhancing Technologies“ (datenschutzfördernde Technik) statt, aber ist dort eher auf akademische Forschungsfragen ausgerichtet, statt dass die Praxis mit dem Hintergrund des europäischen Datenschutzrechts behandelt wird. Es fehlt also bislang an einer verlässlichen Bewertungsmethodik.

Dies war der Startpunkt für eine weitere Studie, die ein ULD-Team zusammen mit einem Datenschutzwissenschaftler aus den Niederlanden bis Anfang 2016 erstellt hat: „Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies“ (Reifegradanalyse für die Einführung und Weiterentwicklung von datenschutzfördernder Technik). Hierin schlagen wir eine Methode vor, um verschiedene „Privacy-Enhancing Technologies“ in Bezug auf Reifegrad und Qualität bezüglich des Datenschutzes vergleichen zu können. Wegen der Komplexität des Themas bezieht unsere Methode für die Bewertung ein Expertengremium ein. In zwei kleinen Evaluationen zu existierenden Techniken illustrieren wir die Methode und stellen dar, was nötig wäre, um unsere Idee der Bewertung und Veröffentlichung in die Realität umzusetzen.

Ziel ist nicht nur, diejenigen Maßnahmen und Bausteine zu identifizieren, die definitiv heute schon zum Stand der Technik gehören, sondern es geht uns auch um einen Blick in die Zukunft: Wo sind gute Ansätze am Start, die gefördert werden sollten? Wo ist eine Technik robust genug, dass man sie pilotieren kann? Wie erreicht man den Brückenschlag von der Wissenschaft in die Praxis? Wie können Gesetzgeber, Förderinstitutionen und Aufsichtsbehörden dies optimal unterstützen?

Die Studien liegen auf Englisch vor und sind unter den folgenden Links zu finden:

https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

https://www.enisa.europa.eu/publications/pets

Was ist zu tun?

Sowohl Verantwortliche und Auftragsverarbeiter als auch Datenschutzaufsichtsbehörden müssen sich künftig mehr mit datenschutzgerechter Systemgestaltung beschäftigen und prüfen, wie sie diese Konzepte und Entwicklungen in ihrem Zuständigkeitsbereich einbringen können.

12

KERNPUNKTE

Transparenz für Schleswig-Holstein
NDR-Staatsvertrag
Leitfaden IZG in Bauordnungsbehörden

12 Informationsfreiheit

12.1 Ein Transparenzgesetz für Schleswig-Holstein

In Hamburg, Rheinland-Pfalz und Bremen existieren in den Landesvorschriften zur Informationsfreiheit bereits proaktive Veröffentlichungspflichten für die Verwaltung. In Hamburg sind vorbehaltlich schutzwürdiger Informationen etwa Verträge der Daseinsvorsorge, Globalrichtlinien, Fachanweisungen und Verwaltungsvorschriften, amtliche Statistiken und Tätigkeitsberichte, das Baumkataster, öffentliche Pläne und wesentliche Regelungen von Baugenehmigungen erfasst.

Im Jahr 2016 wurde von den Fraktionen von SPD, BÜNDNIS 90/DIE GRÜNEN und den Abgeordneten des SSW ein „Gesetzentwurf zur Änderung des Informationszugangsgesetzes – IZG“ (Landtagsdrucksache 18/4409) eingebracht, mit dem nun auch der schleswig-holsteinische Gesetzgeber das Ziel verfolgt, für bestimmte Informationen Veröffentlichungspflichten zu normieren. Das ULD hat die Bestrebungen des schleswig-holsteinischen Gesetzgebers unterstützt, im Informationszugangsgesetz Veröffentlichungspflichten zu regeln. Zum Gesetzentwurf hat das ULD Stellung genommen (Landtagsumdruck 18/6732).

Die Veröffentlichungspflichten für Landesbehörden werden stufenweise in Kraft treten. Ab dem 1. Januar 2020 werden etwa Richtlinien und Runderlasse an andere Behörden, amtliche Statistiken, öffentliche Tätigkeitsberichte und Broschüren, Haushaltspläne, Stellenpläne und Wirtschaftspläne sowie Vorlagen der Landesregierung nach Beschlussfassung und Mitteilungen an den Landtag erfasst. Ab dem 1. Januar 2022 werden die Veröffentlichungspflichten erweitert, wobei z. B. von Landesbehörden in Auftrag gegebene Gutachten oder Studien mit einem Auftragswert ab 10.000 Euro, Verträge, soweit es sich nicht um öffentliche Aufträge oder um Kredit- und Finanztermingeschäfte handelt, ab einem Auftragswert von 50.000 Euro sowie Verträge für die Erstellung von Gutachten ab einem Auftragswert von 10.000 Euro einbezogen werden.

Ab dem 1. Januar 2022 sind die Landesbehörden zudem verpflichtet, Verwaltungsvorschriften, Organisations-, Geschäftsverteilungs- und Aktenpläne und weitere Informationen, die ab dem 27. Mai 2017 bei ihnen entstanden, erlassen, bestellt oder beschafft worden sind, ohne Angaben von personenbezogenen Daten und Geschäfts- und Betriebsgeheimnissen allgemein zugänglich zu machen und diese an ein zentrales Informationsregister zu melden.

Kritisch sieht das ULD eine Neuregelung, die als Ausnahme der Finanzbehörden vom Kreis der informationspflichtigen Stellen auch für die eigene Steuerakte verstanden werden kann, soweit Vorgänge der Steuerfestsetzung und Steuererhebung betroffen sind. Das OVG Schleswig hat mit Urteil vom 6. Dezember 2012, Az.: 4 LB 11/12 entschieden, dass der Zugang zur eigenen Einkommensteuerakte im Rahmen von abgeschlossenen Steuerverfahren zulässig ist. Kritisiert hat das ULD auch, dass hinsichtlich der Veröffentlichung von Informationen vor dem Jahr 2022 geregelt ist, dass die Landesbehörden die aufgeführten Informationen nur veröffentlichen „sollen“. Dies widerspricht aus Sicht des ULD einer generellen Verpflichtung zur Veröffentlichung von Informationen.

Was ist zu tun?

Die Berücksichtigung proaktiver Veröffentlichungspflichten im IZG ist vom ULD unterstützt worden und wird begrüßt. Die Landesbehörden müssen seit dem 27. Mai 2017 bei ihnen entstandene, erlassene, bestellte und beschaffte Informationen nach Maßgabe der neuen Vorschriften für eine Veröffentlichung ab dem 1. Januar 2022 vorbereiten.

12.2 Informationsfreiheit im NDR-Staatsvertrag verankern

Mit der Presseerklärung vom 26. September 2016 setzten sich die Landesbeauftragte für den Datenschutz Niedersachsen, der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit sowie das ULD – allesamt zuständig für Informationsfreiheit in ihrem Bundesland – für die Änderung des NDR-Staatsvertrags ein, um dort in Anlehnung an die bestehenden Landesvorschriften zur Informationsfreiheit eine Transparenzregelung zu schaffen (Landtagsumdruck 18/6634).

Die Informationsfreiheitsbeauftragten kamen zu dem Schluss, dass die vom NDR bereits veröffentlichten Informationen nicht annähernd für die Feststellung ausreichen würden, der NDR erfülle die Transparenzvorgaben nach dem Transparenzgesetz Hamburg bereits auf freiwilliger Basis. Nur eine rechtliche Verpflichtung ist daher geeignet, für den NDR eine angemessene Basis zur Umsetzung von Informationsfreiheit zu schaffen.

Anlässlich eines Gesetzgebungsvorhabens im Landtag von Schleswig-Holstein aus dem Jahr 2013 zur Verankerung der Informationsfreiheit im NDR-Staatsvertrag (Landtagsdrucksache 18/1288) stellten die Fraktionen der SPD, BÜNDNIS 90/DIE GRÜNEN und die Abgeordneten des SSW im September 2016 einen Antrag zur Weiterentwicklung des NDR-Staatsvertrags, mit welchem u. a. erreicht werden sollte, dass „eine feste Regelung zur Informationsfreiheit im NDR nach dem Vorbild des Hamburger Transparenzgesetzes unter Berücksichtigung der dann aktuellen Gesetze der NDR-Länder und Ausschluss journalistisch-redaktioneller Informationen“ geschaffen wird (Landtagsumdruck 18/6612).

Für den WDR wurde etwa in § 55a des WDR-Gesetzes bereits eine vergleichbare Bestimmung hinsichtlich der Anwendung des Informationsfreiheitsgesetzes Nordrhein-Westfalen geschaffen. In einem Urteil des OVG Münster vom 9. Februar 2012, Az.: 166/10 wurde auf jene Bestimmung Bezug genommen und ausgeführt, dass eine Verpflichtung zur Auskunft nicht die Rundfunkfreiheit des WDR berührt und auch dessen Wettbewerbsfähigkeit im Verhältnis zu privaten Anbietern gewahrt wird.

Was ist zu tun?

Es sollte eine Bestimmung zur Informationsfreiheit im NDR-Staatsvertrag aufgenommen werden.

12.3 Zugang zu Unterlagen des Wissenschaftlichen Dienstes

Der Schleswig-Holsteinische Landtag verweigerte wiederholt die Herausgabe vollständiger Aufstellungen der Ausarbeitungen des Wissenschaftlichen Dienstes. Zur Begründung wurde vor allem darauf verwiesen, dass der Wissenschaftliche Dienst keine Verwaltungstätigkeit, sondern parlamentarische Aufgaben wahrnehme und somit nicht dem Informationszugangsgesetz Schleswig-Holstein unterfalle.

Der Landtag selbst ist zwar keine Behörde, sondern vielmehr das auf Landesebene vom Volk gewählte oberste Organ der politischen Willensbildung und damit Verfassungsorgan. Zu den Kernkompetenzen des Landtages zählt etwa seine Gesetzgebungsfunktion. Gleichwohl ist der Landtag nach den Vorgaben des IZG zum Informationszugang verpflichtet, soweit dieser außerhalb seiner Gesetzgebungstätigkeiten handelt.

Die Tätigkeit des Wissenschaftlichen Dienstes des Landtages ist nach Auffassung des ULD nicht als Gesetzgebungstätigkeit, sondern als Verwaltungstätigkeit anzusehen. Der Wissenschaftliche Dienst ist Teil der Landtagsverwaltung und erledigt keine parlamentarischen Aufgaben. Er ist gerade nicht der Mandatsausübung von Landtagsabgeordneten zugeordnet. Der Wissenschaftliche Dienst arbeitet weder Gesetzgebungsentwürfe aus noch fertigt er Plenarvorlagen an. Seine gutachterliche Tätigkeit ist Verwaltungstätigkeit und geht einer mandatsbezogenen Aufgabenerfüllung voraus.

Mit Urteil vom 25.06.2015, Az.: 7 C 1/14 hat das Bundesverwaltungsgericht für den Deutschen Bundestag festgestellt, dass es sich bei der Arbeit des Wissenschaftlichen Dienstes um Information und Wissensvermittlung und damit um die Wahrnehmung einer typischen Verwaltungsaufgabe handelt.

Das ULD hat im Rahmen seiner rechtlichen Einschätzung gegenüber dem Landtag darauf hingewiesen, dass sich die Frage, ob und in welchem Umfang die Ausarbeitungen des Wissenschaftlichen Dienstes des Schleswig-Holsteinischen Landtages nach dem IZG herauszugeben sind, danach richtet, ob Ausschlussgründe nach § 9 IZG (Schutz öffentlicher Belange) oder nach § 10 IZG (Schutz privater Belange) vorliegen. Sollten in den Unterlagen des Wissenschaftlichen Dienstes des Schleswig-Holsteinischen Landtages im Einzelfall schutzbedürftige Informationen vorhanden sein, wie etwa personenbezogene Daten, so wäre ein Informationszugang nach dem IZG nur beschränkt zulässig.

In der Folge wurde fraktionsübergreifend – mit Ausnahme der PIRATEN – ein Gesetzentwurf zur Änderung des IZG eingebracht, der darauf abzielt, die gutachterliche Tätigkeit des Wissenschaftlichen Dienstes im Auftrag einer oder mehrerer Fraktionen von dem Anwendungsbereich des IZG auszunehmen (Landtagsdrucksache 18/4465). Im Gesetzentwurf wurde ausgeführt, dass zur parlamentarischen Aufgabenwahrnehmung des Landtages auch die gutachterliche oder rechtsberatende Tätigkeit im Auftrag einer oder mehrerer Fraktionen zähle, wodurch die vom Wissenschaftlichen Dienst erstellten Unterlagen vom Informationszugang nach dem IZG generell ausgeschlossen sein sollen. Diese Bestimmung ist im Mai 2017 in Kraft getreten.

Was ist zu tun?

Das Bundesverwaltungsgericht hat deutlich ausgeführt, dass die Tätigkeit eines Wissenschaftlichen Dienstes zur Verwaltungstätigkeit zählt. Ein Wissenschaftlicher Dienst erledigt gerade keine Aufgaben der Gesetzgebung oder gar parlamentarische Aufgaben. Eine Landesregelung, die die Tätigkeit des Wissenschaftlichen Dienstes des Schleswig-Holsteinischen Landtages pauschal als parlamentarische Tätigkeit ausweist und damit einen Informationszugang nach dem IZG vermeiden soll, begegnet rechtlichen Bedenken.

12.4 Einsicht in Prüfberichte der Heimaufsichten

Ein Antragsteller bat mehrere Heimaufsichten in Schleswig-Holstein jeweils um die Herausgabe des aktuellen Prüfberichts. Einige der in Anspruch genommenen Stellen gaben teilweise geschwärzte Berichte heraus. Andere Heimaufsichten hielten vor allem mit dem Hinweis auf fehlende Regularien zur Veröffentlichung nach dem Selbstbestimmungsstärkungsgesetz (SbStG) an ihrer Ablehnung fest, einen Informationszugang zu den Prüfberichten zu gewähren.

Das ULD wies darauf hin, dass etwaige fehlende Regularien für eine Veröffentlichung nach dem SbStG einer Herausgabe nach dem IZG nicht entgegenstehen. Bei der Veröffentlichung nach dem SbStG geht es um eine proaktive Veröffentlichungspflicht. Das IZG dagegen bezieht sich auf eine antragsbezogene Gewährung des Informationszugangs. Weiterhin werden die Bestimmungen des IZG nicht durch die Vorschriften des SbStG ausgeschlossen. Grenzen findet der Informationszugang nach dem IZG nur durch die Ausschlussgründe, die in Form von öffentlichen oder privaten Belangen vorliegen können.

Im Nachgang prüften auch diejenigen Heimaufsichten, die den Informationszugang zunächst unter Hinweis auf das SbStG abgelehnt hatten, die gestellten Anträge nach den Bestimmungen des IZG und gaben die Prüfberichte nach Anhörung der betroffenen Heimleitungen teilweise geschwärzt an den Antragsteller heraus.

Was ist zu tun?

Das SbStG enthält keine das IZG verdrängenden Bestimmungen. Bei Anträgen auf Informationszugang gegenüber den Heimaufsichten ist zu prüfen, ob und in welchem Umfang die Berichte herauszugeben sind.

12.5 Anhörungsverfahren bei Informationen zu Emissionen

Das IZG sieht nach § 10 Satz 3 IZG ein Anhörungsverfahren vor, wenn Dritte durch die Informationserteilung betroffen sein könnten. Das ist beispielsweise dann der Fall, wenn sich das Informationsbegehren auf personenbezogene Daten oder Betriebs- und Geschäftsgeheimnisse bezieht.

Bei Vorliegen dieser geschützten privaten Belange dürfen die Informationen grundsätzlich nur erteilt werden, wenn der Betroffene eingewilligt hat oder wenn das öffentliche Interesse gegenüber dem privaten Geheimhaltungsinteresse überwiegt. Auch um dies abschätzen zu können, sind die Betroffenen anzuhören. Eine Besonderheit ergibt sich dann, wenn es bei den begehrten Informationen um Informationen zu Emissionen geht. Dann dürfen bestimmte private und öffentliche Belange nicht als Ablehnungsgrund herangezogen werden. Eine Berufung auf den Schutz personenbezogener Daten und von Betriebs- und Geschäftsgeheimnissen ist dann nicht möglich.

Gleichwohl sind die Betroffenen auch in dieser Situation vor einer Entscheidung über das Informationsersuchen anzuhören, da eine Beeinträchtigung schutzwürdiger Belange möglich erscheint. Dies kann beispielsweise dann der Fall sein, wenn die informationspflichtige Stelle irrtümlich das Vorliegen von Emissionen annimmt und den Informationszugang vor diesem Hintergrund ungeachtet des Vorliegens von beispielsweise Betriebs- und Geschäftsgeheimnissen gewähren will (vgl. dazu EuGH-Urteil vom 08.10.2013, Rs.T – 545/11). Anderenfalls würde der Wille des Gesetzgebers, dem Gebot des effektiven Rechtsschutzes Rechnung zu tragen (vgl. Landtagsdrucksache 14/2374, S. 18, zum 2. Absatz des § 11 und zum 2. Absatz des § 12 IFG-SH; Landtagsdrucksache 17/1610, S. 24, 25), nicht beachtet werden.

Was ist zu tun?

Soweit eine Beeinträchtigung schutzwürdiger Belange möglich erscheint, hat die informationspflichtige Stelle die Betroffenen vor einer Entscheidung über einen IZG-Antrag anzuhören.

12.6 Kammersatzungen versus Informationsfreiheit?

Mitunter kommt es vor, dass Anfragen nach dem IZG von Bürgern, die an Kammern in Schleswig-Holstein gerichtet sind, von diesen mit dem Hinweis auf Geheimhaltungs- und Verschwiegenheitspflichten abgelehnt werden, die in den Kammersatzungen geregelt sind. Das ULD war in einer entsprechenden Bürgeranfrage mit der Prüfung befasst, inwieweit interne Regelungen der Steuerberaterkammer einem Anspruch nach dem IZG entgegenstehen können.

Kammersatzungen sind den Landesgesetzen dem Rang nach untergeordnet. Das IZG als ein Landesgesetz geht den internen Satzungsbestimmungen der Kammern vor. Die Regelungen in den Satzungen können daher nicht dem allgemeinen Zugangsrecht nach dem IZG ent-

gegenstehen. Auch begründen etwaige in den Kammersatzungen enthaltene Geheimhaltungs- und Vertraulichkeitsregelungen keinen Ausschlussgrund nach dem IZG. Anders als in einigen anderen Informationsfreiheitsrechten enthält das IZG keine Regelung, nach der die Erteilung von Informationen zu versagen ist, wenn die erbetenen Informationen einer durch Rechtsvorschrift geregelten Geheimhaltungs- oder Vertraulichkeitspflicht unterliegen. Die Prüfung, ob und wenn ja wie die erbetenen Informationen zu erteilen sind, hat daher anhand der im IZG geregelten Ausschlussgründe zum Schutz öffentlicher bzw. privater Belange (§§ 9, 10) zu erfolgen.

Was ist zu tun?

Die in Satzungsbestimmungen der Kammern geregelten Geheimhaltungs- und Verschwiegenheitspflichten stehen einer Anwendung des IZG nicht entgegen. Eine etwaige Beschränkung des Informationszugangs ist allein anhand der im IZG vorhandenen Ausschlussgründe zu beurteilen.

12.7 Keine Pflicht zur Informationsbeschaffung und zur Beantwortung von Rechtsfragen

Häufig stellen Bürgerinnen oder Bürger einen IZG-Antrag bei der informationspflichtigen Stelle in der Weise, dass sie Fragen stellen und um deren Beantwortung bitten. Der gewünschte Informationszugang wird damit in Form von Auskünften begehrt. Grundsätzlich hat die informationspflichtige Stelle die Fragen zu beantworten, da die Auskunftserteilung von dem IZG erfasst ist.

Dies gilt jedoch nicht, wenn es sich bei den Fragen um Rechtsfragen handelt (vgl. OVG Schleswig, Urteil vom 11.10.2002, 21 A 391/02; VG Frankfurt a. M., Urteil vom 23.01.2008, 7 E 1487/07). Dies ist beispielsweise dann der Fall, wenn ein Bürger eine informationspflichtige Stelle fragt, warum eine Genehmigung für das Fällen eines Baumes erteilt worden ist. Diese Frage zielt auf eine rechtliche Bewertung ab und unterliegt damit nicht dem Anwendungsbereich des IZG. Immer dann, wenn für die Beantwortung der Frage eine rechtliche Prüfung oder Bewertung erforderlich ist (z. B.: Welche Rechtsgrundlage liegt der hinterfragten Handlung zugrunde? Welche Rechtsfolgen sieht die gesetzliche Grundlage vor?), handelt es sich um Rechtsfragen, die die informationspflichtige Stelle nach dem IZG nicht beantworten muss.

Eine weitere Ausnahme liegt dann vor, wenn die Beantwortung der Fragen nicht aufgrund der bei der informationspflichtigen Stelle vorhandenen Informationen möglich ist, sondern die dafür erforderlichen Informationen erst beschafft werden müssten. Die informationspflichtige Stelle hat keine Informationsbeschaffungspflicht. Ob sich die begehrte Auskunft aus den vorhandenen Informationen ergibt oder erst beschafft werden muss, kann im Einzelfall schwierig zu beurteilen sein. Ein derartiger kritischer Fall kann dann vorliegen, wenn sich das Auskunftsbegehren auf eine Zusammenstellung von Informationen bezieht. Wird beispielsweise eine Aufstellung begehrt, die zunächst eine Auswertung erfordert, ist dies als nicht vom IZG erfasste inhaltliche Aufbereitung von Informationen zu erachten (vgl. BVerwG, Urteil vom 27.11.2014, 7 C 2012). Eine solche Auswertung kann als nicht verpflichtende „Informationsbeschaffung“ gewertet werden. Geht es dagegen beispielsweise darum, eine vorhandene Auflistung bestimmter Sachverhalte zu erhalten, ist dies nicht als Informationsbeschaffung zu werten.

Was ist zu tun?

Rechtsfragen müssen nach dem IZG nicht beantwortet werden. Es besteht nach dem IZG auch keine Verpflichtung zur Informationsbeschaffung. Die informationspflichtigen Stellen verfügen über Informationen nur dann, wenn diese bei ihnen vorhanden sind oder an anderer Stelle für sie bereitgehalten werden. Ein Bereithalten setzt voraus, dass die informationspflichtige Stelle gegenüber der aufbewahrenden Stelle einen Übermittlungsanspruch hat.

12.8 Ausschluss des Informationszugangs durch Spezialgesetze

Die Anwendung des IZG scheidet dann aus, wenn es Spezialgesetze gibt, die den Zugang zu Informationen regeln oder sogar explizit ausschließen. Die in Anspruch genommenen Stellen müssen dann prüfen, ob oder inwieweit eine solche Spezialregelung vorliegt. So ist etwa die Einsicht in Personalakten bei öffentlichen Stellen speziell in § 88 des Landesbeamtengesetzes normiert. Das IZG wird von vornherein ausgeschlossen, sodass insbesondere die dort geregelten Fristen für einen Informationszugang, die Modalitäten der Zugangsgewährung (z. B. Einsicht, Herausgabe von Kopien, Auskunft), die Ausschlussgründe und die Kostenfrage nicht nach den Bestimmungen des IZG zu beurteilen sind. Gleiches gilt bei der Beantragung einer Akteneinsicht nach § 49 OWiG oder § 12 der Grundbuchordnung. Auch dann findet das IZG keine Anwendung.

Für die Prüfung einer vorrangigen Regelung ist etwa zu untersuchen, ob der Gesetzgeber in einem anderen Gesetz bereits einen Informationszugang geregelt hat und ob dies als abschließende Bestimmung gedacht war. Weiterhin ist zu prüfen, welche Zwecke die unterschiedlichen Zugangsrechte verfolgen. Beispiel: Einsichten in ein Baulastenverzeichnis werden von Antragstellern gewöhnlich aus dem Grunde begehrt, um für die eigene Rechtsposition hilfreiche Informationen zu erhalten. Der Zugang zu den Informationen des Baulastenverzeichnisses wird nach § 80 Abs. 5 der Landesbauordnung an das Vorliegen eines berechtigten Interesses geknüpft. Die Vorschrift stellt eine Spezialregelung dar, die gegenüber der Anwendung des voraussetzungslosen Zugangs nach dem IZG eine Sperrwirkung entfaltet.

Was ist zu tun?

Die informationspflichtige Stelle muss in jedem Einzelfall prüfen, ob das IZG anwendbar oder aufgrund vorrangiger bereichsspezifischer Regelungen ausgeschlossen ist.

12.9 Privates Handeln einer informationspflichtigen Stelle

Das ULD kann von den Bürgern kontaktiert werden, wenn diese der Auffassung sind, dass ihrem Informationsgesuch nach dem IZG nicht ordnungsgemäß nachgekommen wurde. In diesem Sinne wandte sich ein Bürger an das ULD, da die angerufene öffentliche Stelle seinen Antrag auf Informationszugang unter Hinweis auf ihr privatrechtliches Handeln abgelehnt hatte.

Die Ablehnung des Informationsersuchens kann nicht darauf gestützt werden, dass sich die begehrten Informationen auf privatrechtliches Handeln einer öffentlichen Stelle beziehen. Privatrechtliches Handeln öffentlicher

Stellen führt nicht zur Beschränkung des Anwendungsbereichs des IZG. Anderenfalls würde der Gesetzeszweck unterlaufen werden. Das IZG dient u. a. der Stärkung der demokratischen Beteiligungsrechte der Bürger. Beispielsweise muss die Einhaltung der Verpflichtung öffentlicher Stellen zur Sparsamkeit und Wirtschaftlichkeit der Haushaltswirtschaft durch den Bürger als zusätzliches Kontrollorgan überprüft werden können (vgl. VG Schleswig, Urteil vom 31.08.2004, 6 A 245/02; VG Köln, Urteil vom 07.04.2011, 13 K 822/10; BVerwG, Urteile vom 03.11.2011, 7 C 3.11 und 7 C 4.11). Wäre das IZG bei privatrechtlichem Handeln öffentlicher Stellen nicht anwendbar, bestünde zudem die Gefahr, dass die öffentlichen Stellen sich ihrer Verpflichtung zur Informationserteilung durch eine „Flucht ins Privatrecht“ entziehen könnten.

Der Staat und seine Einrichtungen sind daher auch bei privatrechtlichem Handeln als Zuordnungsobjekte von Normen des öffentlichen Rechts zu erachten (vgl. VG Köln, Urteil vom 07.04.2011, 13 K 822/10), sodass das IZG auch in diesem Fall auf öffentliche, informationspflichtige Stellen in Schleswig-Holstein Anwendung findet.

Was ist zu tun?

Die informationspflichtige Stelle unterliegt auch dann dem IZG, wenn sich der Antrag auf Informationen zu einem privatrechtlichen Handeln der öffentlichen Stelle bezieht. Die informationspflichtige Stelle ist daher auch bei eigenem privatrechtlichen Handeln gehalten zu prüfen, ob und inwieweit der beantragte Informationszugang zu gewähren ist.

12.10 Beanstandung wegen Nichtbeantwortung von Fragen

Ein Schwerpunkt bei der Tätigkeit des ULD im Bereich der Informationsfreiheit bildet die Beratungs- und Mediationsleistung, um so langfristig auf eine ordnungsgemäße Handhabung des IZG hinzuwirken. Liegen jedoch erhebliche Verstöße oder sonstige erhebliche Mängel in einem Verfahren einer informationspflichtigen Stelle über die Gewährung oder Ablehnung eines Informationszugangs vor, kann das ULD eine Beanstandung aussprechen. Eine Beanstandung wird nur in seltenen Ausnahmefällen ausgesprochen. Ein derartiger Anwendungsfall ist beispielsweise dann gegeben, wenn die informationspflichtige Stelle untätig bleibt.

So verhielt es sich in einem Fall, in dem ein Bürger von einem Abwasserzweckverband aus Schleswig-Holstein eine Auskunft nach dem IZG begehrte. Der Abwasserzweckverband ist eine „sonstige juristische Person des öffentlichen Rechts“ im Sinne des IZG und damit eine informationspflichtige Stelle. Obwohl der Bürger der nicht gebotenen Aufforderung der informationspflichtigen Stelle zur Konkretisierung seines IZG-Antrags nachkam und das ULD bereits einbezogen war, wurde sein Antrag nicht beschieden. Auch kam die informationspflichtige Stelle weder der Aufforderung nach Stellungnahme des ULD noch der Möglichkeit nach, sich im Anhörungsverfahren zu der dort angedrohten Beanstandung zu äußern. Wegen der schlichten Untätigkeit der informationspflichtigen Stelle lagen aus Sicht des ULD erhebliche Verstöße gegen die Vorgaben des IZG vor. Das ULD hat daher eine Beanstandung ausgesprochen. Von der Beanstandung wurden neben der informationspflichtigen Stelle sowohl der Bürger als auch das Ministerium für Energiewende, Landwirtschaft, Umwelt und ländliche Räume Schleswig-Holstein als oberste Aufsichtsbehörde nach dem Wassergesetz des Landes Schleswig-Holstein, dem Wasserverbandsgesetz und dem Landesverwaltungsgesetz Schleswig-Holstein unterrichtet.

Was ist zu tun?

Soweit ein Anspruch nach dem IZG besteht, muss die informationspflichtige Stelle innerhalb eines Monats nach Antragstellung die begehrten Informationen zugänglich machen. Im Ausnahmefall kann die informationspflichtige Stelle auch innerhalb von zwei Monaten antworten. Dies hat sie dem Bürger jedoch unverzüglich, zumindest jedoch innerhalb des ersten Monats seit Antragstellung, mitzuteilen.

12.11 Leitfaden zur Anwendung des IZG in Bauordnungsbehörden

Häufig richtet sich das Antragsbegehren der Bürger auf Informationen, die bei Bauordnungsbehörden vorhanden sind. Oft geht es um die Einsicht in Bauakten oder in Baulastenverzeichnisse. Das ULD hat aus diesem Grund einen Leitfaden entwickelt, der den informationspflichtigen Stellen in diesem Tätigkeitsfeld eine Hilfestellung bei der Prüfung eines IZG-Antrags bietet. Auch für Bürger stellt dieser Leitfaden viele Informationen bereit.

Der Leitfaden beantwortet Fragen zu den anspruchsberechtigten Personen, zum Verhältnis des IZG zu anderen gesetzlichen Vorgaben in baurechtlichen Vorschriften, zur Qualifizierung von Umweltinformationen nach der Umweltinformationsrichtlinie, zur Verfügbarkeit einer Information bei einer informationspflichtigen Stelle, zu formalen Anforderungen bei der Antragsbearbeitung, zur Stellung anonymer Anträge sowie zu den Ausschlussgründen und der etwaigen Betroffenheit Dritter.

Bei IZG-Anfragen im Bereich der Bauordnungsbehörden bietet der Leitfaden eine Hilfestellung. Der Leitfaden ist abrufbar unter:

https://www.datenschutzzentrum.de/uploads/informationsfreiheit/ULD-Leitfaden-Bauakten-IZG_SH_November_2015.pdf

12.12 Anonyme Anfragen über das Internetportal „FragDenStaat“

Immer häufiger werden über das Portal „FragDenStaat“ Anfragen an informationspflichtige Stellen gerichtet. Das Portal wird von einem Verein mit Sitz in Berlin betrieben, der die Bürgerinnen und Bürger bei der Stellung von Anträgen nach den Bestimmungen zur Informationsfreiheit deutschlandweit unterstützt. Die Antragsteller sind in den meisten Fällen den informationspflichtigen Stellen nicht unter ihrem echten Namen bekannt. Das wirft bei den informationspflichtigen Stellen die Frage auf, ob derartige anonyme Anfragen zu beantworten sind.

Das IZG sieht keine bestimmte Form der Antragstellung vor. Daher dürfen diese Anträge nicht deshalb abgelehnt werden, weil sie anonym gestellt worden sind (35. TB, Tz. 12.3). Von diesem Grundsatz gibt es nach Auffassung des ULD aber zwei Ausnahmen:

Erstens ist eine Identitätsabfrage durch die informationspflichtige Stelle zulässig, wenn anderenfalls die Gefahr besteht, dass ohne die Kenntnis von der Person des Antragstellers und dessen Anschrift eine Gebührenpflicht nicht durchsetzbar ist (Gefährdungslage). Dies setzt voraus, dass ein kostenauslösender Verwaltungsaufwand entsteht und der Antragsteller nicht zahlungswillig ist (35. TB, Tz. 12.3) (vgl. auch OVG Berlin-Brandenburg, Beschluss vom 26.05.2014, OVG 12 B 22.12).

Zweitens ist die Identitätsabfrage zulässig, wenn Dritte von der begehrten Informationsherausgabe betroffen wären (Drittbetroffenheit). Das IZG darf nicht dazu führen, dass datenschutzrechtliche Anforderungen unterlaufen werden. Um das datenschutzrechtliche Dokumentationserfordernis erfüllen bzw. einem etwaigen datenschutzrechtlichen Auskunftsanspruch des betroffenen Dritten nachkommen zu können, muss in solchen Fällen die Identität des Antragstellers abgefragt werden können.

Was ist zu tun?

Grundsätzlich sind die informationspflichtigen Stellen gehalten, einer IZG-Anfrage auch im Falle einer anonymen Antragstellung ohne Identitätsabfrage nachzugehen. Bei Vorliegen einer Gefährdungslage und/oder Drittbetroffenheit kann die Identitätsabfrage zulässig sein.

13

KERNPUNKTE

Seminarangebote für Datenschutz und Informationsfreiheit
Schulungen und Fortbildungen
Sommerakademien

13 DATENSCHUTZAKADEMIE Schleswig-Holstein

Das Landesdatenschutzgesetz Schleswig-Holstein formuliert in § 43 Abs. 3 als Auftrag, dass „das Unabhängige Landeszentrum für Datenschutz Fortbildungsveranstaltungen zu den Themen Datenschutz und Datensicherheit durchführt“. Konzeption und Organisation dieser Veranstaltungen übernimmt seit 1993 die DATENSCHUTZAKADEMIE Schleswig-Holstein.

13.1 Kurse im Programm der DATENSCHUTZAKADEMIE

Im Schulungsjahr 2015 wurden in der DATENSCHUTZAKADEME 24 reguläre Kurse angeboten. 372 Teilnehmende ließen sich von 17 Dozenten und Dozentinnen der DATENSCHUTZAKADEMIE zu vielfältigen Themen von Datenschutz, Datensicherheit und Informationsfreiheit schulen. 2016 waren es 415 Teilnehmende in 26 Kursen.

Die seit 24 Jahren durchgeführten behördlichen Grundlagenkurse der DATENSCHUTZAKADEMIE werden kontinuierlich gut angenommen und bilden damit eine solide Grundlage für datenschutzkonformes Handeln in schleswig-holsteinischen Landesbehörden, kommunalen Verwaltungen und Schulen. Diese sind:

- Datenschutzrecht/Datensicherheit für behördliche Datenschutzbeauftragte
- Informationszugangsgesetz SH
- Datenschutz im E-Government
- Datenschutz im Schulsekretariat (Grund- und Aufbaukurs)
- Führung von Personalakten
- Rechtsfragen des Landesdatenschutzgesetzes

Die letzten drei Kurse werden in Kooperation mit KOMMA, dem Kompetenzzentrum der Verwaltungsakademie Bordesholm, durchgeführt.

Der dreitägige Lehrgang „Betrieblicher Datenschutz Kompakt“ bietet in handlungsoptimierter und praxisbezogener Form betrieblichen Datenschutzbeauftragten eine gute Grundlage für ihre Tätigkeit.

Zum Angebot für Wirtschaft, Vereine und Verbände gehörten im Berichtszeitraum ebenso:

- Beschäftigtendatenschutz
- Kundendatenschutz
- Social Media und Datenschutz
- Das Standard-Datenschutzmodell (Tz. 6.3)

Zu den Themenschwerpunkten „Technischer Datenschutz und Datensicherheit“ gehören die Kurse:

- IT-Grundschutz nach BSI
- Datenschutzkontrolle, Sicherheitschecks und Datenschutzaudits
- Einführung in IT-Systeme und IT-Komponenten für Anfänger
- Mit dem Grundschutztool „Verinice“ zum IT-Sicherheitskonzept

Diese Kurse befähigen die Absolventen, die Sicherheit von Verfahren oder Geschäftsprozessen und die Verwaltung von IT-Verbünden von Organisationen mithilfe der IT-Grundschutzmethode umzusetzen. Neu hinzugekommen in diesem Bereich sind die Kurse „Datenschutzlecks in Behörden und Unternehmen“ und „Grundlagen der Dokumentation nach DSVO“.

Die Schulungstätigkeit im Medizin- und Sozialbereich konnte bislang nicht ausgebaut werden, da nicht immer die Kostenträger entsprechende Mittel für Datenschutzfortbildungen bereitstellen. Insofern ist die Einschätzung der vergangenen Jahre weiter aktuell: Trotz zunehmender Datenschutzsensibilisierung im medizinischen Bereich und trotz erheblichen Bedarfs erfahren die Kurse vermutlich nicht die ihnen zustehende Beachtung seitens der Verantwortlichen. Dies trifft sowohl auf den Kurs „Datenschutz im Medizinbereich“ als auch auf die Kurse „Datenschutz in Pflegeheimen und Pflegediensten“ sowie „Datenschutz in der Jugendhilfe“ zu.

Dagegen werden Sonderkurse mit speziell auf den Auftraggeber zugeschnittenen Themen im

Sozialbereich regelmäßig nachgefragt: Jobcenter, Pflegedienste und Behinderteneinrichtungen buchen für ihre Mitarbeiterinnen und Mitarbeiter Fortbildungsveranstaltungen zu Themen des Sozialdatenschutzes – wenngleich dies aus Kostengründen oft nur halbtägige Informationsveranstaltungen sind.

Als „DATENSCHUTZAKADEMIE vor Ort“ nahmen in Inhouse-Sonderkursen 2015/2016 insgesamt 524 Personen an Fortbildungen zu folgenden Themen teil:

- Einführung in die DSGVO
- Datenschutz und Informationszugang
- E-Government
- Dokumentation nach DSVO und LDSG
- Behördlicher Datenschutz bei der Staatsanwaltschaft
- Das Informationszugangsgesetz SH
- Einführung in das Datenschutzrecht
- Datenschutz in Pflegeheimen und Pflegediensten
- Einführung in den Sozialdatenschutz
- Datenschutz im Tätigkeitsfeld der Heimaufsicht für Kinder- und Jugendhilfeeinrichtungen
- Datenschutz und Datensicherheit in Zahnarztpraxen
- Datenschutz in der Kinder- und Jugendhilfe
- Datenschutz in der Beratungsstelle
- Datenschutz im Betreuungsalltag
- Datenschutz im Landesjugendamt
- DSVO Schule
- Rechtliche Aspekte der IT-Sicherheit
- Datenschutz und Datensicherheit/Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für den Grundschutz
- Grundlagen der IT-Sicherheit und IT-Sicherheit am Arbeitsplatz
- IT-Grundschutz nach BSI
- Mit dem Grundschutztool „Verinice“ zum IT-Sicherheitskonzept
- Datenschutzrecht für Systemadministratoren
- IT-Grundschutz/Einführung und Umsetzung

Diese Inhouse-Veranstaltungen wurden von den folgenden Stellen in Auftrag gegeben:

- AOK Bundesverband, Berlin, azv Südholstein, Hetlingen
- Brücke SH gGmbH, Kiel
- Deutsche Gesellschaft für Cybersicherheit mbH & Co. KG, Schuby
- DRK-Kreisverband Flensburg-Stadt e. V., Flensburg
- DRK-Landesverband Schleswig-Holstein e. V., Kiel
- Frauenhaus Kiel/Beratungsstelle Die Lerche, Kiel
- Gemeinde Flintbek
- Hansestadt Lübeck
- IEA Data Processing Research Center, Hamburg
- Interessengemeinschaft Kleine Heime & Jugendhilfeprojekte Schleswig-Holstein e. V., Schleswig
- Kreis Herzogtum Lauenburg, Ratzeburg
- Kommunales Forum für Informationstechnik e. V. (KOMFIT), Kiel
- Landesbetrieb Straßenbau und Verkehr Schleswig-Holstein, Kiel
- Ministerium für Energiewende, Landwirtschaft, Umwelt und ländliche Räume Schleswig-Holstein (MELUR), Kiel
- Ministerium für Inneres und Bundesangelegenheiten Schleswig-Holstein (MIB)/ Landespolizeiamt, Kiel
- Ministerium für Soziales, Gesundheit, Wissenschaft und Gleichstellung Schleswig-Holstein (MSGWG)/Landesjugendamt – Heimaufsicht, Kiel
- Mürwiker Werkstätten GmbH, Flensburg
- PARITÄTISCHER Wohlfahrtsverband Schleswig-Holstein e. V., Kiel
- Regionales Berufsbildungszentrum Soziales, Ernährung und Bau (RBZ1), Kiel
- Staatsanwaltschaft bei dem Schleswig-Holsteinischen Oberlandesgericht, Schleswig
- Staatskanzlei des Landes Schleswig-Holstein/Informationssicherheitsmanagement, Kiel
- Stadt Norderstedt

Die 2011 eingeführten Schülerkurse „Entscheide DU – sonst tun es andere für dich!“ haben sich in der schleswig-holsteinischen Schulwelt mit großem Erfolg etabliert.

Insgesamt 1.500 Schülerinnen und Schülern der Mittelstufenklassen aller Schultypen wurde im Berichtszeitraum vermittelt, dass und wie sie mit ihren persönlichen Daten achtsam umgehen können.

In der Informationsveranstaltung für Eltern „Entscheiden SIE – sonst tun es andere für Ihre Kinder!“ ließen sich 2015/2016 55 interessierte Eltern in puncto Medienkompetenz weiterbilden (Tz. 7.6).

Das aktuelle Jahresprogramm der DATENSCHUTZAKADEMIE finden Sie unter

https://datenschutzzentrum.de/akademie/programm/

13.2 Datenschutz-Sommerakademien

Die alljährlich an einem Montag im Spätsommer stattfindenden Sommerakademien der DATENSCHUTZAKADEMIE waren mit jeweils knapp 500 Gästen im Atlantic Hotel Kiel sowohl 2015 als auch 2016 sehr gut besucht. Mit den Themen „Vertrauenswürdige IT-Infrastruktur – ein (un?)erreichbares Datenschutzziel“ und „Datenschutz neu denken! Werkzeuge für einen besseren Datenschutz“ wurden aktuelle und wichtige Fragen aufgegriffen und fachkundig diskutiert.

Am 18. September 2017 wird sich die Sommerakademie 2017 unter dem Motto „Datenschutz neu denken!“ einem weiteren Thema widmen: „Herausforderung ‚Informationelle Nichtbestimmung‘ – Privacy by Default für Technik, Wirtschaft und Politik“. Expertinnen und Experten aus verschiedenen Disziplinen werden mit uns diskutieren, wie wir mit (Nicht-)Bestimmung umgehen können und wie „Privacy by Default“ – hoffentlich! – zu einem besseren Datenschutz führt.

Index

A

AG Zertifizierung **110**
Akteneinsichtsrecht **40**
AN.ON-Next **94**
AppPETs **94**
Arbeitskreis Technik **72**
Artikel-29-Datenschutzgruppe **57**, **131**
Arztpraxen **47**, **48**
Ausländerverwaltung **43**

B

BAföG **77**
Banken **61**
Beschäftigtendaten **64**
Big Data **100**, **101**, **103**
Browser **119**
Bundesdatenschutzgesetz (BDSG) **58**

C

CANVAS **100**
Cloud Computing **97**
Cybersicherheit **97**, **100**

D

Dataport **72**
Datei „Fußball SH“ **32**
Datenpannen **132**
DATENSCHUTZAKADEMIE Schleswig-Holstein **147**
Datenschutzaudit **113**
  Beratungen **115**
  Forschungsinstitut IEA **116**
  Kernkraftfernüberwachung (KFÜ) **115**
  SafeMail-Dienst der KVSH **114**
Datenschutzbeauftragter **58**, **72**
Datenschutz-Folgenabschätzung **75**
Datenschutzgremium **25**
Datenschutz-Grundverordnung **109**
Datenschutz-Gütesiegel **110**
  Rezertifizierung **111**
  Sachverständige **112**
  Zertifizierung **110**
Datenschutz-Sommerakademie **149**
digitales Klassenbuch **52**, **126**
Digitalisierung **11**, **12**, **27**
Dopingkontrolle **96**

E

eBeihilfe **78**
E-Government **28**, **29**, **73**
EIDI **99**
Einwilligung **45**, **48**, **59**, **63**
elektronische Signatur **27**
E-Mail **41**, **45**
Ende-zu-Ende-Verschlüsselung **95**
EU-Richtlinie **18**
Europa **129**
Europäische Datenschutz-Grundverordnung **17**
Europaratsausschuss **40**

F

Facebook **83**, **85**
Falldatei Rauschgift (FDR) **31**
Finanzämter **38**
Forward Secrecy **121**
Fotos **39**, **52**, **63**
FragDenStaat **144**
Funkzellenabfragen **41**, **42**
FutureID **93**

G

Gefahrengebiete **30**
Geflüchtete **43**, **44**
Gesundheitsmanagement **79**

H

Heimaufsicht **139**

I

IBAN **62**
Identitätenmanagement **92**
Identitätsdiebstahl **99**
Identity Brokerage **93**
iKoPA **104**
Informationsfreiheit **9**, **137**, **138**, **140**, **143**
Informationssicherheit **20**
Informationszugangsgesetz (IZG) **139**, **140**, **141**, **142**, **143**, **144**
Initiative for Open Authentication (OATH) **125**
Integriertes Sicherheitsmanagementsystem (ISMS) **71**
Internet der Dinge **104**, **105**
Internet Privacy Engineering Network (IPEN) **133**

IT-Beauftragten-Konferenz (ITBK) **71**
iTESA **101**
IT-Grundschutz **115**, **116**
IT-Labor **119**
ITS.APT **98**
IT-Sicherheit **71**, **98**

J

JI-Richtlinie **18**
Jugendhilfe **46**
Justiz **37**, **41**

K

Kammersatzungen **140**
Kernkraftfernüberwachung (KFÜ) **115**
Kliniken **48**
KoPers kommunal **76**
Kundenkarten **60**

L

Landes-IT-Rat **71**
Landesjugendamt **46**
Landesmeldegesetz **28**
Landesverwaltungsgesetz **28**
Landtag **25**
Lehrer-Apps **53**

M

Medienkompetenz **87**
Meldedatenabgleich **84**
Messenger-Dienste **51**
Metadaten **123**, **124**
Mindestlohngesetz **58**
Mobile Apps **94**

N

NDR-Staatsvertrag **138**

O

Online-Dienste **125**
Online-Zugangssysteme **60**
Ortsinformationen **86**
Outsourcing **37**, **48**

P

PARADISE **96**
Patientendaten **49**
Patientengeheimnis **47**
Personalakten **27**
Personaldaten **46**
Phishing **98**
Pokémon Go **86**
Polizei **30**, **35**, **41**, **103**
Polizeilicher Informations- und Analyseverbund (PIAV) **31**, **33**
Privacy by Design **133**
Privacy Shield **130**, **131**
Privacy&Us **105**
Privacy-Forum **91**
Projekte
- AN.ON-Next **94**
- AppPETs **94**
- CANVAS **100**
- EIDI **99**
- FutureID **93**
- iKoPA **104**
- iTESA **101**
- ITS.APT **98**
- PARADISE **96**
- Privacy&Us **105**
- SeDaFa **104**
- SPECIAL **102**
- SPLITCloud **97**
- VALCRI **103**
- VVV **95**

Q

Quartiersmanagement **43**

R

Reichsbürger **35**
Rundfunkbeitragsstaatsvertrag **84**

S

Safe Harbor **57**, **129**, **130**
Schadsoftware **20**
Schrems-Beschwerde **129**
Schule **50**, **52**, **87**
Schulverwaltungssoftware **49**
Secure Socket Layer (SSL) **121**
SeDaFa **104**
Selbst-Check **47**
Selbstdatenschutz **92**, **96**
semantisches Netz **102**
Smart Cars **104**
Smart Home **124**
Sozialleistungsbereich **45**
Sparkassen **63**
SPECIAL **102**

SPLITCloud **97**
Standard-Datenschutzmodell (SDM) **74**
Steuerverwaltung **53**
Strafverfahren **38**
Systemdatenschutz **71**

T

Telekommunikationsüberwachung **34**
Telemetriedaten **122**
Time-based One-Time Password algorithm (TOTP) **125**
Tracking **119**
Transparenzgesetz **137**
Transport Layer Security (TLS) **121**

U

ULD **9**
ULD-Innovationszentrum (ULD-i) **91**

V

VALCRI **103**
Verfahrensdokumentation **76**
Verfassungsschutz **30**
Verwaltung **27**
Videoüberwachung **65**
  auf Toiletten **68**
  im Fitnessstudio **67**
  im Landtag **25**
  in Schwimmbädern **67**
  mit Wildkameras **66**
Vorabkontrolle **76**, **77**
VVV **95**

W

Wearables **87**
Webcams **65**
Webseitenverschlüsselung **120**
Werbeeinwilligungen **60**
WhatsApp **45**, **85**
Windows 10 **122**
Wirtschaft **57**
Wissenschaftlicher Dienst **138**
Wolfsmonitoring **66**

X

XTA **73**

Z

Zentrale E-Governmentstelle **29**
Zwei-Faktor-Authentifizierung **125**
Zweitwohnungssteuer **54**