6. Tätigkeitsbericht

des Bayerischen Landesamtes
für Datenschutzaufsicht
für die Jahre
2013 und 2014

Vorwort

Datenschutz und Datensicherheit waren und sind, wenn man die Resonanz in den Medien als Gradmesser heranzieht, absolute Topthemen in den letzten beiden Jahren. Die Berichte von Edward Snowden haben Menschen weltweit – auch uns – vertiefte Erkenntnisse darüber gebracht, wie mit personenbezogenen Daten umgegangen wird. Ob diese neuen Erkenntnisse und die in diesem Zusammenhang verdienstvolle Arbeit der Medien dazu geführt haben, dass Datenschutz und Datensicherheit auch bei den Bürgerinnen und Bürgern als besonders bedeutsame Themen wahrgenommen werden, wäre eine vertiefte sozialwissenschaftliche Untersuchung wert. Nach unseren täglichen Erfahrungen als Datenschutzaufsichtsbehörde werden diese Themen weiterhin eher mit Zurückhaltung wahrgenommen.

Wie sich aus den im Folgenden dargestellten statistischen Angaben ergibt, haben die Anfragen und Beschwerden im Berichtszeitraum zwar zugenommen, jedoch nicht in dem von uns auf Grund der genannten Enthüllungen erwarteten – und zugegebenermaßen auch befürchteten – Umfang. Kontrollen, die wir bei Unternehmen sowohl im Rahmen von Großprüfungen als auch fokussierten Prüfungen vorgenommen haben, zeigen, dass viele Unternehmen insbesondere die Fragen der Datensicherheit vielfach noch nicht mit der gebotenen Bedeutung angehen. Dies hatten wir nach den Medienberichten über die umfassenden Möglichkeiten der Geheimdienste und natürlich auch krimineller Hacker eigentlich erwartet. Nicht immer wird dabei gesehen, dass das Leitungspersonal von Unternehmen, die mit personenbezogenen Daten von Kunden und Mitarbeitern umgehen, nicht nur für das ökonomische Wohlergehen ihres eigenen Unternehmens Verantwortung tragen, sondern auch für den Grundrechtsschutz der betroffenen Kunden und Mitarbeiter verantwortlich sind. Personenbezogene Daten von Kunden und Mitarbeitern sind eben nicht nur Wirtschaftsgüter, wie Baustoffe oder Maschinen, sondern nach wie vor Bestandteile des Persönlichkeitsrechts der Betroffenen, für deren Umgang andere Maßstäbe gelten. Dieses Bewusstsein bei den „verantwortlichen Stellen“ zu schaffen, d. h. bei denjenigen, die mit personenbezogenen Daten Dritter umgehen, ist eine gewaltige Herausforderung für alle Datenschutzbehörden, aber auch und insbesondere für alle betrieblichen Datenschutzbeauftragten.

Die Erfahrungen und insbesondere die Rückmeldungen zu unserer ersten wirklichen Großprüfung - die Untersuchung des Einsatzes von Google Analytics auf 13.404 Webseiten bayerischer Unternehmen (siehe Seite 20 des 5. Tätigkeitsberichts 2011/2012) - haben uns veranlasst, der Prüfungstätigkeit eine noch größere Bedeutung beizumessen. Grundsätzlich richten wir die Prioritäten unserer Arbeit danach aus, dass die Bearbeitung von Beschwerden Vorrang vor allen anderen Tätigkeiten hat, da hierbei konkrete Datenschutzverstöße behauptet, und, wie unsere Bearbeitung zeigt, in deutlich mehr als der Hälfte aller Fälle auch begründet behauptet wird. Soweit unsere Kapazitäten es erlauben, können wir darüber hinaus Beratungen anbieten und Prüfungen vornehmen. Insbesondere von betrieblichen Datenschutzbeauftragten wurden wir „gebeten“, in verstärktem Umfang Prüfungen vorzunehmen. Diese hätten laut ihrer Aussage zur Folge, dass bei den Geschäftsführungen der Unternehmen bekannt wird, dass es überhaupt eine Datenschutzaufsichtsbehörde gibt und dass diese hoheitliche Kompetenzen hat, die im Einzelfall auch wehtun können. Das führe im konkreten Fall dazu, dass den Anregungen und Forderungen der betrieblichen Datenschutzbeauftragten deutlich mehr Beachtung beigemessen wird. Da uns bewusst ist, dass die Prüfung von einigen hunderten Unternehmen bezogen auf den Gesamtbestand in Bayern immer nur ein Tropfen auf den heißen Stein sein kann, informieren wir bei zahlreichen Vortragsveranstaltungen wie z. B. bei Industrie- und Handelskammern, Verbänden der Datenschutzbeauftragten oder sonstigen Berufsverbänden über die Prüfungen und deren wesentliche Ergebnisse, d. h. festgestellte Mängel, um die Anwesenden zu motivieren, daraus ihre eigenen Schlüsse für das eigene Unternehmen zu ziehen.

Bei der Bearbeitung der Beschwerden, bei Prüfungen oder auch Beratungen versuchen wir deutlich zu machen, auf welcher Rechtsgrundlage wir konkrete Forderungen erheben. Dabei beschränken wir uns in aller Regel darauf, nur solche Forderungen zu erheben, die wir, wenn ihnen nicht Rechnung getragen wird, durch hoheitliche Maßnahmen auch durchzusetzen versuchen. „Fundamentalistische" Forderungen zu erheben und dann nicht durchzusetzen, schafft Rechtsunsicherheit und entspricht nicht dem Leitbild unseres Landesamtes.

Die letzten beiden Jahre waren auch geprägt durch die Diskussion um den Entwurf einer Datenschutz-Grundverordnung, den die Europäische Kommission am 25. Januar 2012 vorgelegt, zu dem das Europäische Parlament mit Beschluss vom 12. März 2014 Stellung genommen hat und der Europäische Rat noch intensiv darum ringt, seinen Standpunkt zu finden. Konnte man vor einigen Monaten noch den Eindruck haben, dass die Auffassungen in den Mitgliedstaaten so kontrovers sind, dass das gesamte Projekt einer neuen Datenschutzreform in Europa auf der Kippe stand, zeigte sich in den letzten Monaten insbesondere unter der italienischen Ratspräsidentschaft eine gewaltige Zunahme der Dynamik der Beratungen, so dass heute niemand mehr ernsthaft daran zweifelt, dass diese Datenschutz-Grundordnung kommen wird – sei es Ende 2015 oder Anfang 2016. Die ergebnisorientierte Dynamik der Beratungen, die insbesondere im formellen Trilog zwischen EU-Kommission, EU-Parlament und dem Rat zum Ausdruck kommen wird, wenn der Rat sich auf (s)eine Auffassung verständigt hat und damit sprechfähig ist, darf nicht darüber hinwegtäuschen, dass es nach wie vor in den Mitgliedstaaten erhebliche unterschiedliche Auffassungen darüber gibt, wie die datenschutzrechtliche Regelung in Zukunft aussehen soll. Schon heute steht fest, dass die Bezeichnung: „Grundverordnung", wenn sie denn so bestehen bleibt, leider zutreffend zum Ausdruck bringt, dass hier, jedenfalls im Vergleich zum Bundesdatenschutzgesetz und zahlreichen bereichsspezifischen datenschutzrechtlichen Regelungen, keine sehr detaillierte Rechtsgrundlage geschaffen werden soll. Dies wird dazu führen, dass die zwei Jahre, die derzeit als Übergangszeit nach Verabschiedung der Verordnung bis zu deren Inkrafttreten vorgesehen sind, nicht nur intensiv dafür genutzt werden müssen, die nationalen Normen anzupassen, sondern dass auch verantwortliche Stellen und Datenschutzbehörden, ohne dass Letztere ihre Entscheidungskompetenz aufgeben, sich darüber verständigen sollten, wie bestimmte Regelungen der Verordnung in der Praxis umzusetzen sind. Dies gilt insbesondere für die Bereiche der Videoüberwachung, der Werbung, des Adresshandels und der Auskunfteien, für die es keine konkreten Regelungen mehr geben wird, sondern lediglich eine allgemeine Grundlage für Interessensabwägungen. Dass diese Entscheidungen dann nicht mehr nur im Fokus des nationalen Rechtsverständnisses und der nationalen Rechtskultur getroffen werden können, sondern bei der Auslegung auch das Verständnis in den anderen Mitgliedstaaten der Europäischen Union heranzuziehen sein wird, ist eine Herausforderung, bei der uns zu gegebener Zeit der Europäische Gerichtshof in Luxemburg sagen wird, ob und inwieweit wir dieser gewachsen waren oder nicht.

Ernsthafte Anzeichen dafür, dass Datenschutz und Datensicherheit an Bedeutung verlieren werden, gibt es keine. Wir werden uns deshalb auch in Zukunft mit Nachdruck dafür einsetzen, dass Datenschutzverstöße im nicht-öffentlichen Bereich in Bayern möglichst gar nicht entstehen, oder, wenn wir doch welche erkennen, diese abgestellt werden. Dabei verstehen wir uns wie in der Vergangenheit nicht nur als Interessenvertreter der betroffenen Bürgerinnen und Bürger, sondern haben auch die berechtigten Interessen der Unternehmen im Auge, um beim Umgang mit personenbezogenen Daten eine für alle Beteiligten angemessene Praxis sicherzustellen.

Ansbach, im März 2015

Thomas Kranig
Präsident

Inhaltsverzeichnis

1

Datenschutzaufsicht im nicht-öffentlichen Bereich

1 Datenschutzaufsicht im nicht-öffentlichen Bereich

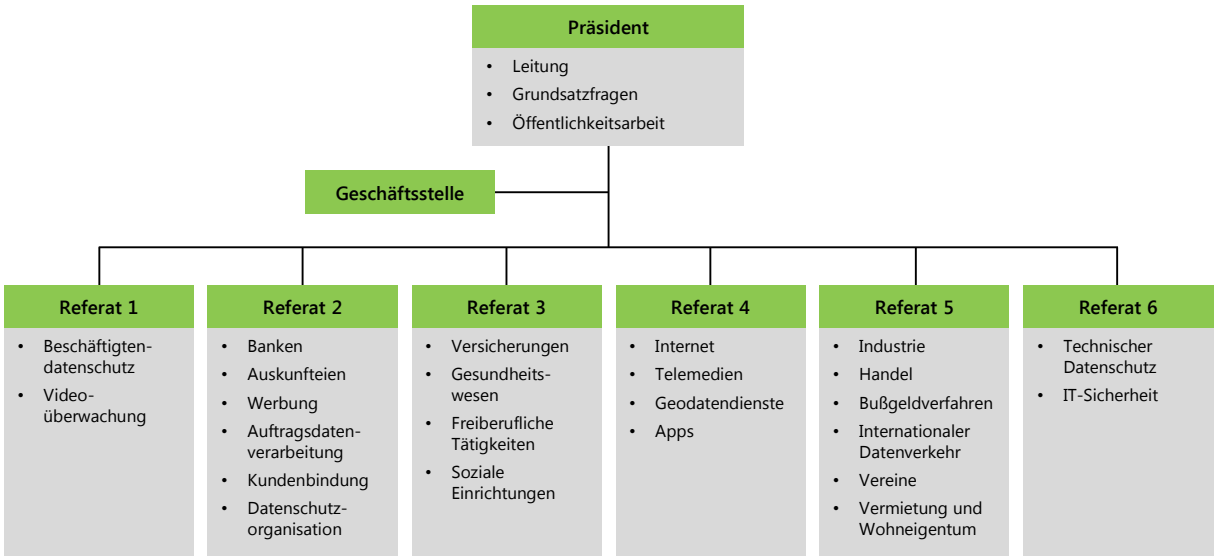
1.1 Die bayerische Datenschutzaufsichtsbehörde

Wir, das Bayerische Landesamt für Datenschutzaufsicht (BayLDA), sind für die Datenschutzaufsicht im nicht-öffentlichen Bereich in Bayern zuständig. Wir üben diese Aufgabe neben dem Bayerischen Landesbeauftragten für den Datenschutz, der für die Kontrolle und Beratung im öffentlichen Bereich zuständig ist, als eigenständige unabhängige Datenschutzbehörde aus.

Personelle Änderungen haben sich im Berichtszeitraum nicht ergeben. Es sind nach wie vor auf 16 Planstellen 17 Mitarbeiterinnen und Mitarbeiter beschäftigt.

1.2 Gesetzliche Grundlage für die Erstellung des Tätigkeitsberichts

Gemäß § 38 Abs. 1 Satz 7 des Bundesdatenschutzgesetzes (BDSG) hat die Aufsichtsbehörde regelmäßig, spätestens alle zwei Jahre, einen Tätigkeitsbericht zu veröffentlichen. Der letzte Tätigkeitsbericht für die Jahre 2011 und 2012 wurde der Öffentlichkeit am 21. März 2013 vorgestellt.



2

Allgemeiner Überblick über die Tätigkeit des BayLDA

2 Allgemeiner Überblick über die Tätigkeit des BayLDA

2.1 Statistik

Die Anzahl der bei uns eingegangenen Beschwerden ist im Vergleich zu den früheren Jahren deutlich gestiegen, aber nicht in einem ungewöhnlichen Ausmaß.

	2013	2014
Beschwerden	925	953
Beratungen Bürger	799	991
Beratungen Unternehmen	1733	1821
Bußgeldverfahren	53	64

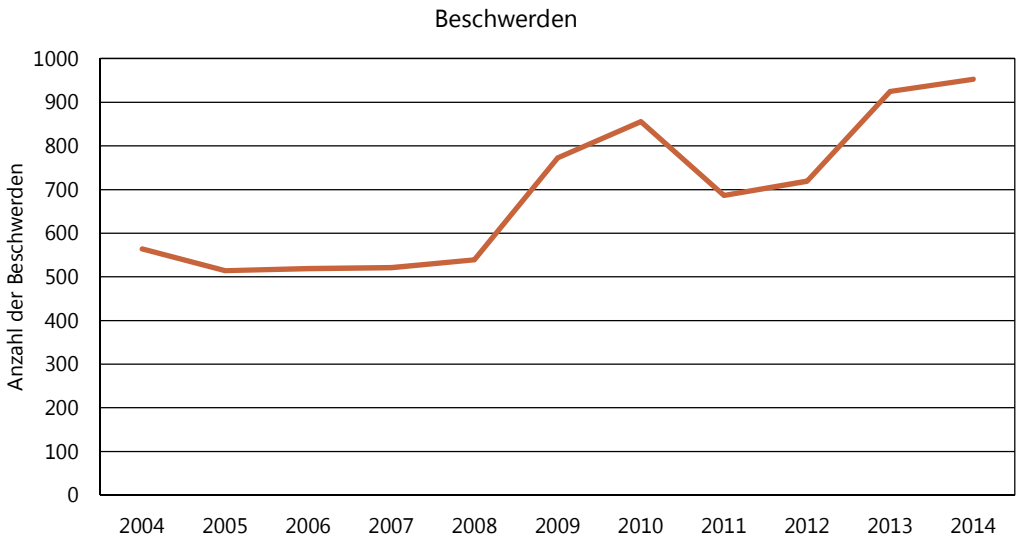
Erkennbar ist, dass das Bedürfnis an Beratung sowohl für Unternehmen als auch Privatpersonen nach wie vor sehr ausgeprägt ist. Selbst wenn dies gelegentlich zu einer grenzwertigen Belastungssituation bei den Mitarbeiterinnen und Mitarbeitern führt, betrachten wir diesen anhaltenden Trend als grundsätzlich positiv, weil wir ihn für uns so verstehen, dass diejenigen, die um Beratung nachsuchen, das Ziel haben, sich darüber zu informieren, wie sie sich gesetzeskonform verhalten können.

Nicht bei allen Eingaben lässt sich zu Beginn eindeutig feststellen, ob es sich um eine Beschwerde oder eine Beratungsanfrage handelt, da sich bei manchen Beschwerden erst im Lauf des Verfahrens herausstellt, dass sie lediglich als Anfrage über die Zulässigkeit eines bestimmten Datenumgangs gemeint war. Ebenso stellt sich in anderen Fällen bei Beratungsanfragen heraus, dass diese als konkrete Beschwerde gedacht waren. Nicht immer klar ist auch bei Eingängen von Polizeibehörden, die in den letzten Jahren deutlich zugenommen haben, ob es sich dabei um neutrale Ereignismeldungen im Sinne der Anregung für ein aufsichtliches Tätigwerden oder um ein bereits eingeleitetes Ordnungswidrigkeitenverfahren handeln soll. In der Praxis bereitet dies keine Probleme, da im Laufe der Bearbeitung relativ schnell erkannt werden kann, mit welcher Zielrichtung man sich an uns gewandt hat, um dann das Verfahren in der richtigen Art und Weise weiter zu betreiben.

2.1.1 Beschwerden

Die Zahl der bei uns eingegangenen Beschwerden ist in den letzten beiden Jahren doch ein großes Stück angestiegen, aber nicht in dem außergewöhnlichen Umfang, wie wir es nach den Veröffentlichungen von Edward Snowden und den bekannt gewordenen zahlreichen Datenpannen in der ganzen Welt erwartet haben.

Wir führen dieses Ansteigen einerseits auf eine etwas gesteigerte Sensibilität der Bürgerinnen und Bürger zurück und andererseits als Erfolg



unseres Bemühens, im Rahmen unserer Öffentlichkeitsarbeit publik zu machen, dass es uns gibt, welche Aufgabe wir haben und dass wir im Einzelnen durchaus helfen können.

Wie schon in den vergangenen Berichten ist auch hier wieder festzustellen, dass die Beschwerden viele unterschiedliche Bereiche betreffen. Die prozentuale Zuordnung der betroffenen Themen hat sich dabei im Verhältnis zu den früheren Aufstellungen nicht wesentlich geändert.

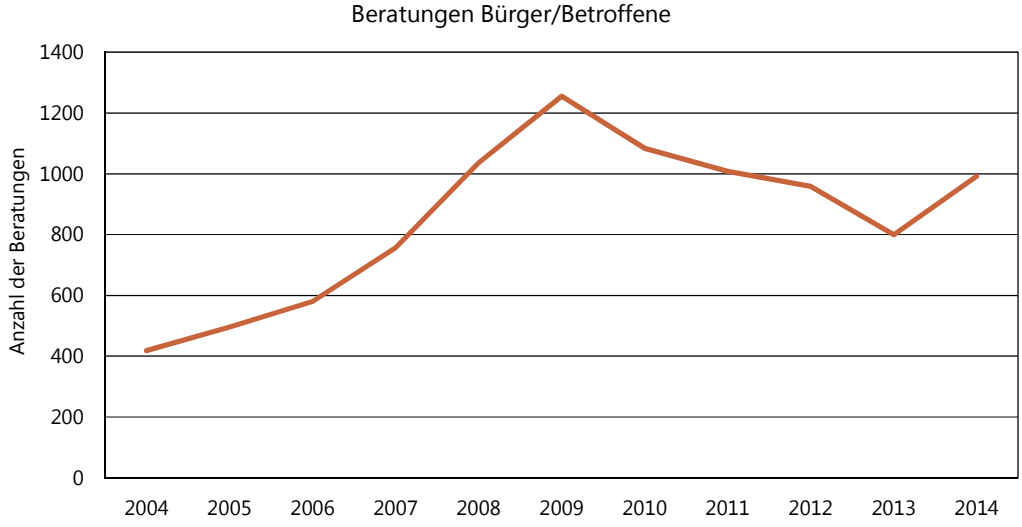
2.1.2 Beratung

Beratungen erfordern, wie sich aus den folgenden Aufstellungen ergibt, den größten Arbeitsaufwand. Wir versuchen dabei nicht nur unsere Auffassung bekanntzugeben, sondern weisen, sofern einschlägig, auf Beschlüsse des Düsseldorfer Kreises hin, so dass die Anfragenden insoweit von einer etwas gefestigten einheitlichen Auffassung der Datenschutzaufsichtsbehörden ausgehen können.

2.1.2.1 Beratung der Bürger/Betroffenen

Die Beratung von Betroffenen ist nicht ausdrücklich im Aufgabenkatalog des § 38 BDSG für die Datenschutzaufsichtsbehörden genannt. Selbst wenn diese Beratungen, wie gerade ausgeführt, mit einem erheblichen Aufwand verbunden sind, hielten wir es für unzumutbar, diese Beratungsleistung gegenüber den Betroffenen nicht zu erbringen, zumal das Ergebnis dieser Beratungen in sehr vielen Fällen an die verantwortlichen Stellen weitergetragen und dort zu einer Änderung ihrer Praxis führen dürfte.

Die unten stehende Grafik zeigt, dass im Jahr 2014 erstmals seit fünf Jahren wieder ein deutlicher Anstieg dieser Beratungsanfragen zu verzeichnen ist, so dass wir derzeit von einer nicht unerheblichen Anzahl an Beratungsleistungen unserseits für Betroffene bzw. Bürger sprechen können.

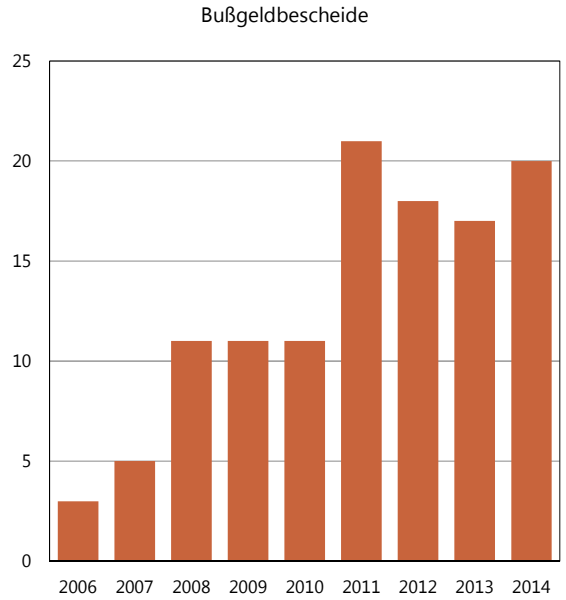


2.1.2.2 Beratung der verantwortlichen Stellen und der betrieblichen Datenschutzbeauftragten

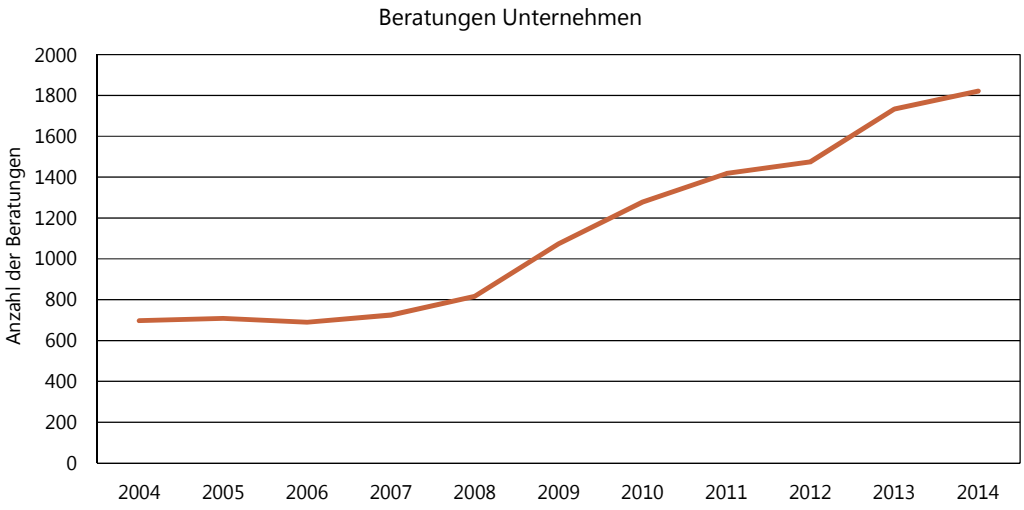
Nicht nur die Anzahl der geleisteten Beratungen von verantwortlichen Stellen und betrieblichen Datenschutzbeauftragten, sondern auch die Bandbreite der Art der Anfragen ist sehr groß. Manche Fragen lassen sich mit einem Telefonanruf oder einer E-Mail rasch klären. Nach wie vor erreichen uns aber in vielen Fällen Anfragen insbesondere von Anwaltskanzleien, die neue Produkte oder Verfahren vorstellen und unsere Auffassung dazu kennen lernen wollen. Eine fundierte Beratung in diesen Fällen würde ein intensives Durcharbeiten der vorgelegten Unterlagen und eine vertiefte Auseinandersetzung mit den datenschutzrechtlichen Fragestellungen erfordern. Vor allem bei der technischen Begutachtung stoßen wir dabei zunehmend an Kapazitätsgrenzen. Um für uns den Aufwand vertretbar zu halten und dennoch eine auch uns selbst zufriedenstellende Beratung anbieten zu können, sind wir in vielen Fällen dazu übergegangen, die Anfragenden aufzufordern, uns ihre eigene Bewertung beziehungsweise ihre Antwort auf von uns gestellte Fragen zum Beratungsgegenstand schriftlich zuzuschicken. Dadurch können wir unsere Beratung in dem einen oder anderen Fall darauf beschränken, dass wir uns dieser Beurteilung anschließen oder kurz darstellen, inwieweit wir davon abweichen. Einige Anwaltskanzleien kommunizieren schon sehr lange auf diese Art und Weise mit uns und haben bislang auch durchaus Verständnis für diese begründete Verfahrensweise gezeigt.

2.1.3 Bußgeldverfahren und Strafanträge

Im Berichtszeitraum haben wir insgesamt 117 Bußgeldverfahren geführt und abgeschlossen, davon 37 mit Erlass eines Bußgeldbescheides. Die Höhe der insgesamt festgesetzten Bußgelder betrug rund 200.000,- EUR (nähere Angaben siehe Kapitel 23).



Konkrete Angaben über die Höhe einzelner Bußgelder machen wir nicht öffentlich, da sie zu Fehldeutungen führen könnten. Bei der Festsetzung des Bußgeldes fließen der Unrechtsgehalt und die wirtschaftlichen Verhältnisse des Adressaten zusammen, so dass gleiche Bußgeldsachverhalte mit deutlich unterschiedlichen Bußgeldern belegt werden können. Zudem ist zu beachten: Für vorsätzlich



begangene Ordnungswidrigkeiten ist der eröffnete Bußgeldrahmen doppelt so hoch wie für lediglich fahrlässige Verstöße.

Geldbußen wurden sowohl gegen natürliche Personen als auch – bei Vorliegen der entsprechenden gesetzlichen Voraussetzungen – gegen Unternehmen als solche verhängt. Geldbußen gegen Unternehmen haben wir insbesondere in einer Reihe von Fällen verhängt, in denen festzustellen war, dass es an hinreichenden organisatorischen oder sonstigen Vorkehrungen der innerbetrieblichen Aufsicht im Unternehmen fehlte und es als Folge eines solchen Mangels im Unternehmen zu einem Verstoß gegen bußgeldbewehrte datenschutzrechtliche Vorschriften gekommen ist. Unternehmen sind daran zu erinnern, dass sie die Pflicht haben, durch organisatorische Vorkehrungen dafür Sorge zu tragen, dass es bei der betrieblichen und unternehmerischen Tätigkeit nicht zu Verstößen gegen bußgeldbewehrte Vorschriften kommt. Wie es vom Gesetz ermöglicht wird, haben wir in solchen Fällen Geldbußen gegen Unternehmen verhängt, wenn Verstöße gegen die betriebliche Aufsichtspflicht Personen zur Last zu legen waren, denen im Unternehmen oder Betrieb Leitungsaufgaben zukamen.

Strafanträge wurden von uns auch in diesem Berichtszeitraum lediglich in fünf Fällen gestellt. Festzustellen war aber, dass zahlreiche datenschutzrechtliche Strafverfahren bei Staatsanwaltschaften anhängig waren, die dann nach Feststellung, dass ein Straftatbestand nicht erfüllt war, an uns als Verwaltungsbehörde zur Durchführung eines Bußgeldverfahrens in eigener Zuständigkeit abgegeben wurden.

2.2 Öffentliches Register der nach § 4d meldepflichtigen automatisierten Verarbeitungen

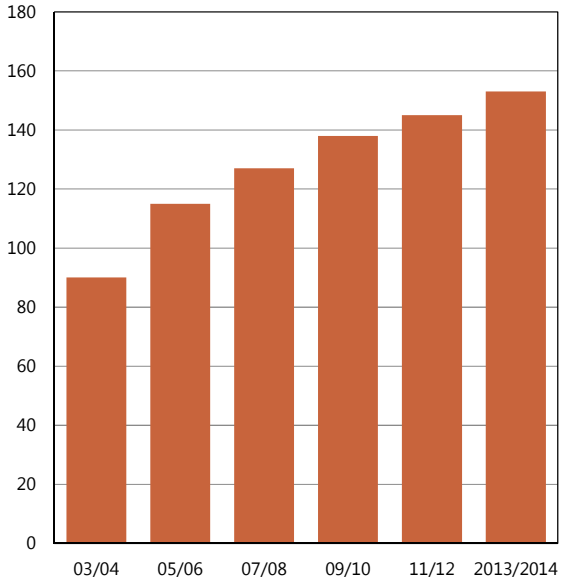
Nach § 38 Abs. 2 BDSG führen wir ein Register der nach § 4d BDSG meldepflichtigen automatisierten Verarbeitungen bei verantwortlichen Stellen in Bayern.

Im Wesentlichen sind die folgenden zwei Geschäftsfelder gegenüber uns als Datenschutzaufsichtsbehörde meldepflichtig:

- Datenspeicherung zum Zweck der Übermittlung, also der Handel mit personenbezogenen Daten, wie es bei Wirtschaftsauskunfteien und Adresshändlern der Fall ist, und
- Datenspeicherung zum Zweck der anonymisierten Übermittlung, also die Tätigkeit der Markt-, Meinungs- und Sozialforschungsinstitute.

Uns lagen zum Ende des Berichtszeitraums insgesamt 153 Anmeldungen aus Bayern vor. Wie auch zum Zeitpunkt des letzten Tätigkeitsberichts entfällt etwa die Hälfte dieser Anmeldungen auf Auskunfteien und Adresshändler, die andere Hälfte auf die analysierenden Institutionen der Markt-, Meinungs- und Sozialforschung.

Angemeldete Unternehmen nach § 4d (Meldepflicht)



Das bei uns geführte Register über die meldepflichtigen Unternehmen kann nach § 38 Abs. 2 Satz 2 BDSG von jedem eingesehen werden.

2.3 Zusammenarbeit mit den anderen Datenschutzaufsichtsbehörden

Mit den anderen Datenschutzaufsichtsbehörden arbeiten wir insbesondere in dem in der Regel zweimal jährlich tagenden „Düsseldorfer Kreis" zusammen, um uns dort über Auslegung und Vollzugsfragen zu verständigen. Ferner nehmen wir an den ebenfalls zweimal jährlich stattfindenden Konferenzen der Datenschutzbeauftragten des Bundes und der Länder (Datenschutzkonferenz) teil, selbst wenn dort ganz überwiegend datenschutzpolitische Fragestellungen diskutiert werden.

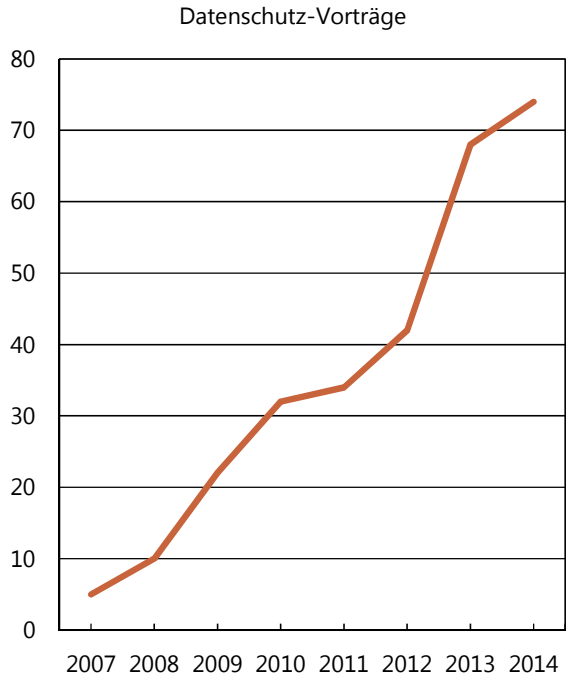
Bemühungen, diese Arbeit besser zu strukturieren und transparent zu machen, ob und in welchem Umfang gemeinsame Beschlüsse als verbindlich angesehen werden, haben ihren Niederschlag in einer Arbeitsgruppe gefunden, die eine Geschäftsordnung für die Gremien der Datenschutzbehörden erstellen soll. Möge ihr Erfolg beschieden sein.

2.4 Teilnahme und Mitwirkung bei Veranstaltungen der Wirtschaft und anderer Berufsgruppen

Weiterhin als Gewinn bringend für alle Seiten betrachten wir den Erfahrungsaustausch mit den betrieblichen Datenschutzbeauftragten in den „Erfa-Kreisen", die unter der Federführung der Gesellschaft für Datenschutz und Datensicherung e. V. (GDD) in München, Nürnberg, Würzburg und Coburg zwei- bis dreimal jährlich stattfinden.

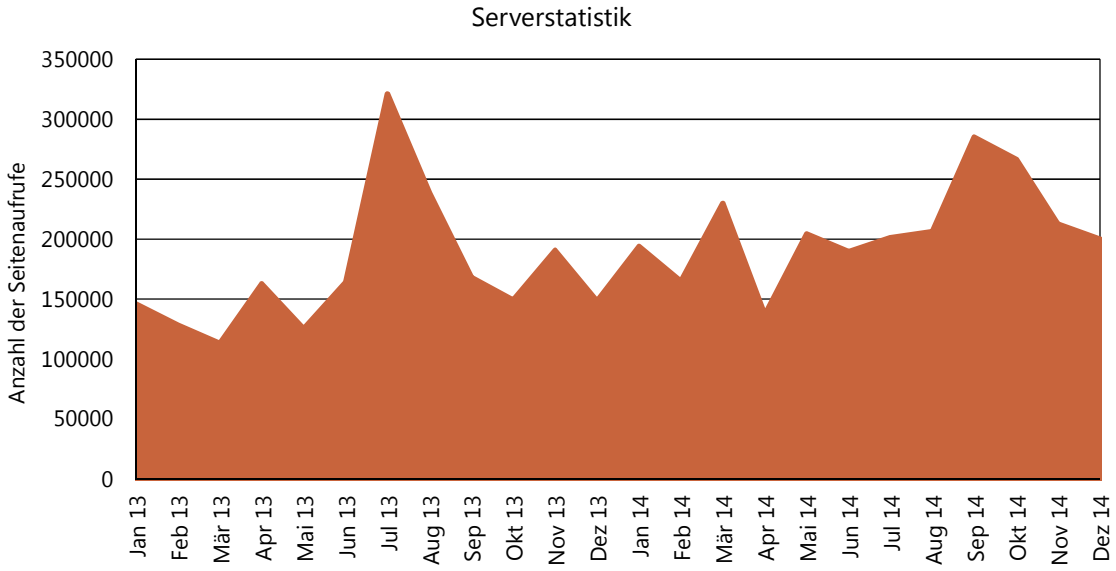
Schon fast traditionell unterstützen wir die Aktivitäten des Berufsverbandes der Datenschutzbeauftragten Deutschlands e.V. (BvD) bei dem Projekt „Datenschutz geht zur Schule", dessen Hauptveranstaltung jährlich am zweiten Dienstag im Februar, d. h. dem Safer Internet Day, stattfindet.

Zu Vorträgen und Teilnahme an Podiumsdiskussionen wurden wir zu 142 Veranstaltungen eingeladen. Diese Einladungen, die zwar mit einem nicht unerheblichen Vorbereitungsaufwand verbunden sind, nehmen wir in aller Regel gerne an, weil wir dabei die Möglichkeit haben, unsere Sicht der Dinge darzustellen und uns in den Diskussionen ein Bild darüber zu verschaffen, ob das, was wir uns für den Umgang mit personenbezogenen Daten vorstellen, in der Praxis ankommt und akzeptiert wird.



2.5 Öffentlichkeitsarbeit

Die Öffentlichkeitsarbeit betrachten wir als einen wichtigen Teil unserer Tätigkeit, in dem wir versuchen, sehr verantwortungsbewusst umzugehen. Selbstverständlich nehmen wir zu Fragen der Medien Stellung, wenn es unseren eigenen Aufgabenbereich betrifft und verweisen ansonsten an die zuständige Datenschutzaufsichtbehörde. Pressemitteilungen geben wir im Wesentlichen zum Ergebnis durchgeführter größerer Prüfungsaktionen heraus, ohne die geprüften Unternehmen namentlich zu benennen. Wir bemühen uns darüber hinaus, Informationen über datenschutzrechtliche Vollzugsfragen auf unserer Homepage darzustellen und freuen uns über das relativ große Interesse daran.



Um erkennen zu können, ob und in welchem Umfang unsere Homepage wahrgenommen wird, erfassen wir ohne sonstige weitere Daten die bloße Zahl der Zugriffe und stellen fest, dass sich diese zwar mit bestimmten Schwankungen, aber dennoch auf einem hohen Niveau eingependelt hat.

3

Kontrollen und Prüfungen

3 Kontrollen und Prüfungen

Nach § 38 Abs. 1 BDSG ist es Aufgabe der Datenschutzbehörde, die Ausführung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz zu kontrollieren. Eine derartige Kontrolle findet bei der Bearbeitung jeder plausiblen Beschwerde statt, die im Einzelfall auch mit einer Ortseinsicht verbunden sein kann. Daneben haben wir uns in den letzten Jahren zum Ziel gesetzt, dass unter der Federführung aller Referate sog. Großprüfungen durchgeführt werden, um das Bewusstsein für die Belange des Datenschutzes in möglichst viele Branchen und alle Teile Bayerns hineinzubringen.

Durch entsprechende Vorbereitungen ist es uns gelungen, die Einleitung vieler Prüfungen weitestgehend automatisiert durchzuführen. In der Praxis zeigte sich dabei, dass in einigen Fällen aber trotzdem ein erheblicher nachfolgender Verwaltungsaufwand erforderlich war, weil eine große Anzahl der geprüften Unternehmen gar nicht oder nur unzulänglich auf die Prüfungsfragen reagiert hat. Aufgrund unseres selbst gesteckten Ziels, dass wir das, was wir aktiv eingeleitet haben, auch konsequent zu Ende bringen, mussten wir diesen Aufwand stemmen.

In einer nicht zu vernachlässigenden Anzahl von Fällen war es erforderlich, unserem Auskunftsbegehren durch Erlass von Zwangsgeldandrohungen und gelegentlich auch Einleitung von Bußgeldverfahren Nachdruck zu verleihen. Eine andere, im Rahmen der vorangegangenen Prüfung des Einsatzes von Google Analytics gemachte Erfahrung hat sich erneut bestätigt, dass selbst sehr detaillierte Hinweise auf unserer Webseite zur Behebung festgestellter Mängel bei Prüfungen nicht in dem Umfang gelesen werden, wie wir es uns wünschen. Vielmehr greifen viele Adressaten lieber zum Telefon, um eine persönliche und individuelle Beratung zu bekommen.

Die von uns durchgeführten Kontrollen lassen sich grundsätzlich durch die Merkmale Prüfungsanlass, Prüfungsform und Prüfungsgröße klassifizieren. Die Ausprägungen dieser einzelnen Merkmale stellen wir nachfolgend kurz vor.

3.1 Prüfungsanlass

3.1.1 Anlassbezogene Prüfungen

Anlassbezogene Prüfungen unserer Aufsichtsbehörde finden statt, wenn wir durch Beschwerden und Anfragen von Betroffenen, Informationen Dritter oder der Medien auf einen möglichen Datenschutzverstoß hingewiesen werden.

3.1.2 Anlasslose Prüfungen

Anlasslose Prüfungen sind dagegen dann gegeben, wenn wir eigeninitiativ im Rahmen von Stichprobenkontrollen Unternehmen oder ganze Branchen prüfen, ohne dass bereits im Vorfeld konkrete Anhaltspunkte für Datenschutzverstöße gegeben sind.

Unabhängig davon, dass es im Ergebnis der anlasslosen Prüfungen meist nur sehr wenige Fälle gibt, bei denen kein Verbesserungsbedarf im Umgang mit personenbezogenen Daten festzustellen ist, erfordern diese Kontrollen

Merkmale von Prüfungen

Prüfungsanlass	Prüfungsform	Prüfungsgröße
anlassbezogen	schriftlich	einzeln
anlasslos	online bzw. im Labor	groß
	vor Ort (fokussiert)	

dennoch einen bestimmten Begründungsaufwand bei den untersuchten Unternehmen, warum gerade diese Ziel unserer Prüfung sind. Dies gelingt uns in den allermeisten Fällen problemlos. In keinem einzigen Fall war es bis heute erforderlich, sich mit Hilfe von Zwangsmitteln Zugang zum Unternehmen verschaffen zu müssen.

3.2 Prüfungsform

3.2.1 Schriftliche Prüfungen

Bei schriftlichen Prüfungen erhalten die kontrollierten Unternehmen i. d. R. ein Schreiben und einen Fragenkatalog, den sie üblicherweise innerhalb von sechs Wochen – teilweise mit Vorlage relevanter Dokumente – beantworten und an uns zurücksenden müssen. Darüber hinaus legen wir unserem Schreiben meist umfangreiche Informationsblätter bei, die die abgefragten Sachverhalte den Geprüften detailliert erläutern.

Solche branchenübergreifende, zum Teil sehr umfangreiche schriftliche Prüfungsaktionen haben wir in den Jahren 2013 und 2014 in ganz Bayern durchgeführt, um den Stand der Umsetzung datenschutzrechtlicher Vorschriften abzufragen.

Exemplarisch stellen wir nachfolgend einen Teil unseres Fragenkatalogs der vergangenen schriftlichen Prüfungen dar:

- Die Erlaubnis-Rechtsvorschriften für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten, auf die sich das betreffende Unternehmen stützt.
- Den Datenschutzbeauftragten, seine Stellung und seine konkrete Tätigkeit.
- Das öffentliche Verfahrensverzeichnis.
- Die Verpflichtungen auf das Datengeheimnis.
- Die Verträge über Auftragsdatenverarbeitung.
- Ausgewählte Punkte zum Beschäftigtendatenschutz, wie z. B. die Regelungen zur privaten Nutzung von Internet und E-Mail und zur Verwendung privater Kommunikationsmittel am Arbeitsplatz.
- Die Videoüberwachung, einschließlich der konkreten Zweck-Festlegungen im Sinne von § 6b Abs. 1 Nr. 3 BDSG.
- Die bestehenden Regelungen zur Sperrung bzw. Löschung von Daten.
- Das Konzept zu den getroffenen technischen und organisatorischen Maßnahmen nach § 9 BDSG und der Anlage zu § 9 BDSG.
- Den Maßnahmenplan für eventuelle Datenpannen nach § 42a BDSG.

Im Ergebnis der schriftlichen Prüfungen haben wir festgestellt, dass etwa fünf Prozent der geprüften Unternehmen erst aufgrund unseres Prüfungsanschreiben mit der Umsetzung der gesetzlichen Datenschutzanforderungen begonnen haben. Viele Unternehmen hatten dagegen schon grundlegende Vorgaben aus dem BDSG erfüllt, wie z. B. die Bestellung eines Datenschutzbeauftragten oder die Verpflichtung der Beschäftigten auf das Datengeheimnis. Es gab aber oft auch noch deutliche Lücken bei der Umsetzung des BDSG, die im Rahmen der Prüfung aufgearbeitet wurden. Nur bei sehr wenigen Unternehmen konnte die Prüfung ohne jede Anmerkung oder Hilfestellung unserseits abgeschlossen werden.

Häufiger wurden Mängel bei folgenden Themen festgestellt:

- Die Bestellung und Tätigkeit des Datenschutzbeauftragten, z. B. nicht vertretbare Interessenkollision (Datenschutzbeauftragter gleichzeitig Personalchef, IT-Administrator, Vorstand oder ähnliches), oder zu wenig Aktivität als Datenschutzbeauftragter.
- Vorhandene Videoüberwachung ohne schriftliches Konzept.
- Keine geregelte Gestattung der privaten Internet- und E-Mail-Nutzung oder des Einsatzes privater Geräte am Arbeitsplatz.

- Die (fehlende) Erstellung des im BDSG vorgesehenen öffentlichen Verzeichnisses der DV-Verfahren.
- Unzureichende oder überhaupt nicht vorhandene Verträge zu Auftragsdatenverarbeitung.

In Einzelfällen wurden im Nachgang hierzu noch Vor-Ort-Prüfungen durchgeführt, um nicht nur auf schriftliche Antworten und Unterlagen vertrauen zu müssen, sondern auch zu zeigen, dass gemachte Angaben auch im Praxisbetrieb überprüft werden.

Das Ergebnis dieser aufsichtlichen Kontrolle im schriftlichen Verfahren hat insgesamt gezeigt, dass solche Prüfungsaktionen eine geeignete Möglichkeit sein können, um in kürzerer Zeit eine größere Zahl von Unternehmen, Freiberuflern, Vereinen etc. zu erreichen. Wir planen deshalb für die Zukunft, weitere schriftliche Prüfungsaktionen durchzuführen. Die zufällige Auswahl der in eine Prüfungsaktion einbezogenen Stellen wird dabei einerseits relevante Branchen mit umfangreicherer oder kritischer Verarbeitung personenbezogener Daten betreffen, darüber hinaus aber auch wieder die gesamte Breite der Wirtschaft erfassen. Unser Hauptziel ist dabei stets durch Information und Beratung einen gesetzeskonformen Umgang mit den persönlichen Daten z. B. von Mitarbeitern, Kunden, Mandanten, Patienten, usw. sowie eine angemessene Datenschutz- und Datensicherheitsorganisation zu erreichen und folglich die Anzahl der Datenschutzbeschwerdefälle und Datenpannen zu reduzieren.

3.2.2 Online- und Laborprüfungen

Bereits seit 2012 können wir Prüfungen – zum Teil auch weitestgehend automatisiert – in unserem technischen Prüflabor durchführen. Diese dort stattfindenden Kontrollen zeichnen sich dadurch aus, dass wir im Vorfeld und während der Durchführung dieser Prüfungen keinen direkten Kontakt zu den verantwortlichen Stellen haben, sondern erst dann auf diese zugehen, wenn die in erster Linie technische Prüfung abgeschlossen ist und wir insbesondere Datenschutzverstöße als Ergebnis der Kontrolle festgestellt haben. So ist es uns möglich, einerseits Geräte an sich (wie z. B. Smartphones, Tablets, Spielekonsolen oder Smart-TVs) zu untersuchen, anderseits auch Datenflüsse der darauf laufenden Software (z. B. Apps, Betriebssysteme) zu begutachten. Ebenso kann aus dem Labor heraus eine herkömmliche Onlineprüfung von Internetangeboten bezüglich festgelegter Kriterien (z. B. bei Reichweitenmessung oder Transportverschlüsselung) automatisiert durchgeführt werden.

Bei den Laborprüfungen einzelner Geräte geht es uns hierbei insbesondere darum, zu erkennen, welche Daten bei der Nutzung des jeweiligen Gerätes zu welchem Zweck erhoben und an wen sie übermittelt werden, sowie herauszufinden, welche Möglichkeit der Nutzer hat, diese Datenflüsse zu erkennen und darauf Einfluss zu nehmen.

3.2.3 Vor-Ort-Prüfungen (fokussiert)

Erstmals im Jahr 2013 haben wir vor Ort auch fokussierte Prüfungen durchgeführt. Fokussiert nennen wir die Prüfung deshalb, weil wir die Prüfung auf in der Regel zehn (unternehmensbezogene) Fragen beschränken, die wir den Unternehmen vorab zuschicken und dann im Rahmen einer Prüfung vor Ort vertiefen. Diese Prüfungen finden im Wesentlichen unter Federführung unseres technischen Referates statt und sollen auch in Zukunft mindestens einmal im Monat mit mindestens zwei geprüften Unternehmen fortgeführt werden.

Durch die straffe Strukturierung dieser Prüfungen stellen wir sicher, dass wir in aller Regel unmittelbar nach der Prüfung den Prüfbericht fertigstellen und an den Folgetagen verschicken können. Die Resonanz auf diese Prüfungen bei den Unternehmen ist durchweg positiv, weil sie meist schnell erkennen, dass es uns nicht darum geht, Sachverhalte für die Durchführung eines Bußgeldverfahrens zu ermitteln, sondern Erkenntnisse über den Datenumgang im bestimmten Unternehmen und Branchen zu erlangen und zu beraten, wie man es im einen oder anderen Bereich noch besser machen kann.

So fanden im Berichtszeitraum bei folgenden Unternehmenskategorien derartige fokussierte Vor-Ort-Prüfungen statt:

- Onlineshop
- Großkonzern
- Steuerberatungsgesellschaft
- Rechtsanwalt
- Sportverein
- Arztpraxis
- Verlag
- Hotel
- Apotheke
- Modehersteller
- Reisebüro

Die Fragen, die im Rahmen einer fokussierten Prüfung behandelt werden, variieren in Abhängigkeit vom untersuchten Unternehmen. Beispielhaft listen wir nachfolgend einige Punkte, die zum Teil auch im Berichtszeitraum vor Ort abgefragt wurden, hierfür auf:

- Übersicht über Art personenbezogener Daten des Unternehmens
- Art des Web- und Mailhostings (inklusive ADV-Verträge nach § 11 BDSG)
- Passwortsicherheitsrichtlinien (Art der Speicherung und Komplexität)
- Einsatz von Verfahren zur Nutzungsprofilbildung (Reichweitenmessung)
- Maßnahmen zum Schutz vor Webhacking-Angriffen
- Datenschutzerklärung auf der Webseite
- Datenschutzkonforme Datenträgervernichtung nach DIN 66399
- Umgang mit Kundendaten zu Marketing- und Retargeting-Zwecken
- Videoüberwachung
- Auftragsdatenverarbeitung (Einsatz externer Dienstleister zur Datenverarbeitung)
- HTTPS-Konfiguration der Webseite
- STARTTLS-Konfiguration bei eingesetzten Mailservern
- Versand und Auswertung von Newsletter
- IT-Sicherheitsleitlinie und -richtlinie
- Netzwerktopologie des Unternehmens (zur Prüfung verschiedener Punkte der Anlage zu § 9 BDSG)
- Informationen zu Schulungen der Mitarbeiter bezüglich Datenschutz und IT-Sicherheit
- Berechtigungskonzept
- Patch-Management
- Einsatz von Verschlüsselungsverfahren (Web, E-Mails, ggf. Cloud Dienste)
- Verfahrensverzeichnis
- Beschreibung zur Umsetzung der Verpflichtung des Datengeheimnisses nach § 5 BDSG

3.3 Prüfungsgröße

3.3.1 Einzelprüfungen

Sofern sich die Prüfung auf einzelne oder zumindest wenige verantwortliche Stellen bezieht, bezeichnen wir diese Art der Kontrollen als Einzelprüfung. Zwar erfolgen diese Prüfungen nicht automatisiert und bedeuten daher grundsätzlich einen etwas höheren Aufwand je verantwortliche Stelle für uns, jedoch kann die Ausrichtung des Prüfungsschwerpunkts deutlich individueller gestaltet werden als bei einer Großprüfung.

Übliches Beispiel für Einzelprüfungen sind die von uns durchgeführten fokussierten Vor-Ort-Kontrollen.

3.3.2 Großprüfungen

Als Großprüfungen bezeichnen wir Prüfungen, bei denen in einem Prüflauf mehr als ca. 20 Unternehmen geprüft werden und der Ablauf dabei möglichst automatisiert unterstützt wird.

3.4 Durchgeführte Prüfungen

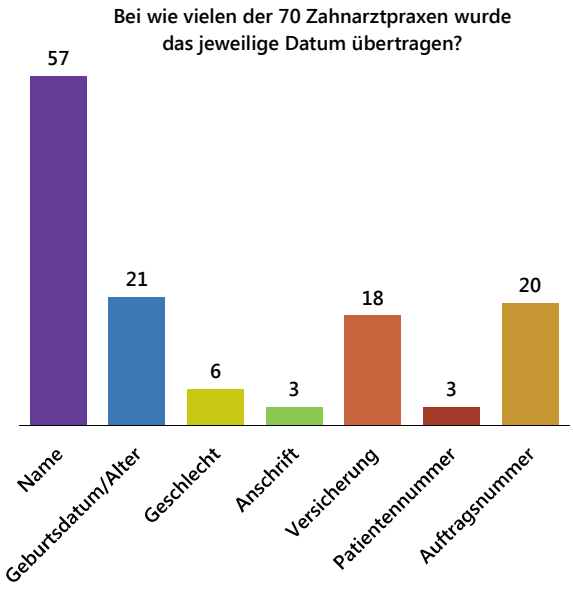
In den nachfolgenden Abschnitten stellen wir jeweils in einer kurzen Zusammenfassung dar, welche Großprüfungen wir im Berichtszeitraum durchgeführt haben. Neben den Hintergründen und den mit den Prüfungen verbundenen Zielen halten wir hier auch das datenschutzrechtliche Ergebnis fest. Weitere Details zu den einzelnen Prüfungen finden sich teilweise in den jeweiligen Fachkapiteln dieses Tätigkeitsberichts.

3.4.1 Zahnarztpraxen und Dentallabore

Uns wurde vorgetragen, dass Dentallabore dem Auftrag erteilenden Zahnarzt einen elektronischen Abrechnungsdatensatz zur Verfügung stellen würden, der in vielen Fällen unverschlüsselt versendet werde. Dies haben wir im Jahr 2013 zum Anlass genommen, den Datenaustausch zwischen Zahnarztpraxen und Dentallaboren im Rahmen einer schriftlichen Prüfung näher zu beleuchten.

Um nähere Informationen darüber zu erhalten, welche Daten zwischen den Zahnarztpraxen und ihren Dentallaboren ausgetauscht werden, in welcher Form der Datenaustausch erfolgt und welche Datensicherheitsmaßnahmen bei der elektronischen Datenübermittlung getroffen werden, haben wir stichprobenartig 70 Zahnarztpraxen angeschrieben und insbesondere um Antwort gebeten, welche konkreten Patientendaten (z. B. Name, Anschrift, Geburtsdatum, medizinische Daten, usw.) an ein externes Dentallabor übermittelt werden.

Die Auswertung der Antworten hat einerseits gezeigt, dass die Zahnärzte in den meisten Fällen neben dem Laborauftrag selbst (welcher z. T. auch Fotos oder Modelle/Abdrücke enthält) auch personenbezogene Daten des Patienten direkt an das Dentallabor übermitteln. Auffällig ist dabei, dass gerade einmal 10% der von uns angeschriebenen Zahnärzte einen solchen Laborauftrag ausschließlich auf der Grundlage einer Auftragsnummer erteilen. Die einheitlich generierte Auftragsnummer wurde eigentlich von den beteiligten Stellen eingeführt, um eine Laborbeauftragung ohne Preisgabe des Patientennamens zu ermöglichen. In den meisten von uns geprüften Fällen enthält der Laborauftrag neben weiteren persönlichen Angaben jedoch auch den Namen des jeweiligen Patienten, so dass der datenschutzrechtliche Gedanke der Auftragsnummer zur Vermeidung persönlicher Patientendaten dadurch untergraben wird. Dies wird besonders bei den 13 Zahnarztpraxen deutlich, die angegeben haben, neben der vom System generierten Auftragsnummer auch persönliche Daten des Patienten zu übermitteln. Insgesamt fällt auf, dass die Auftragsnummer generell nur von relativ wenigen Zahnarztpraxen verwendet wird.



Andererseits hat unsere Prüfung auch ergeben, dass die Datenübermittlung selbst oftmals nicht ausreichend verschlüsselt war. Hier haben wir es deshalb für die Versendung von pseudonymisierten Laborabrechnungsdaten als erforderlich angesehen, den Übertragungskanal zu verschlüsseln (SSL-/TLS mit Perfect Forward Secrecy) oder eine sichere Inhaltsverschlüsselung zu nutzen.

Auf Grund des – aus Datenschutzsicht – schlechten Prüfungsergebnisses werden wir den Datenaustausch zwischen Arztpraxen und Laboren auch künftig im Blick behalten.

Weitere Ausführungen zu dieser Prüfung befinden sich in Kapitel 16.9.

3.4.2 Fitnessstudios

In Fitnessstudios, Gesundheitscentern oder Trainingszentren – unabhängig davon, wie sich diese Einrichtungen heutzutage bezeichnen – werden neben den allgemeinen Daten der Trainierenden wie z. B. Name, Geburtsdatum und Anschrift oftmals auch besonders sensible Gesundheitsdaten erfasst. Zusätzlich werden Kommen- und (z. T.) Gehen-Zeiten (Check-In/Check-Out) erhoben. In einigen Studios sind zudem Videokameras im Einsatz. Auf Grund dieser Datenerhebungen und der zusätzlichen Tatsache, dass wir gelegentlich Beschwerden über vermutete Datenschutzverstöße erhalten hatten, haben wir uns dazu entschieden, gerade bei Fitnessstudios eine großflächige anlasslose Prüfung durchzuführen.

Ziel unserer Prüfung war es, gerade kleine und mittelständische Studios in die Prüfung miteinzubeziehen, um auch diese auf die datenschutzrechtlichen Anforderungen hinzuweisen und für den Datenschutz zu sensibilisieren.

Die geprüften 100 Unternehmen wurden ausschließlich per Zufallssuche ausgewählt. Der Prüffokus lag neben den allgemeinen datenschutzrechtlichen Vorgaben (z. B. Verpflichtung der Mitarbeiter auf das Datengeheimnis, Auftragsdatenverarbeitung, Bestellung eines Datenschutzbeauftragten) hauptsächlich auf der Videoüberwachung, der Erfassung der Check-In/Check-Out-Zeiten sowie dem Umgang mit besonders sensiblen Daten.

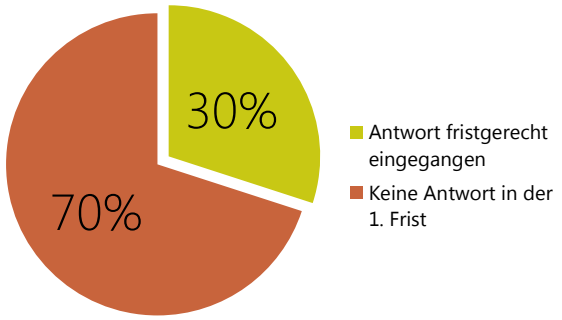
Ergebnis unserer Prüfung war, dass etwa 90 % der 2013 geprüften Fitnessstudios erst durch unser Prüfungsanschreiben überhaupt mit der Datenschutzumsetzung im Sinne der gesetzlichen Anforderungen begonnen haben. Obwohl wir – nach unserer Auffassung – die entsprechenden Fragebögen sehr einfach strukturiert hatten, mussten wir überwiegend feststellen, dass viele Betreiber solcher Studios das Thema Datenschutz bislang noch kaum beachtet hatten. Zudem mussten einige Betreiber mit erheblichem Aufwand unsererseits zur Beantwortung der Fragen „motiviert“ werden.

Lediglich 10 % der kontrollierten Fitnessstudios hatten die grundlegenden Anforderungen umgesetzt und waren entsprechend organisiert.

Mängel waren über den gesamten Fragenkatalog festzustellen. Besonders gravierend war, dass oftmals keine Verträge zur Auftragsdatenverarbeitung vorlagen. Vielen Studiobetreibern war nicht einmal bekannt, dass diese Verträge erforderlich sind bzw. dass das Fehlen der solchen einen bußgeldbewehrten datenschutzrechtlichen Verstoß darstellt. Darüber hinaus haben wir festgestellt, dass die Kommen- und Gehen-Zeiten sehr häufig weit über die gesetzlich erlaubten Zwecke hinaus erfasst und gespeichert wurden.

Diese Prüfung hat uns bestätigt, dass auch bei kleineren Einrichtungen Kontrollen dieser Art sehr sinnvoll sind, um das dort praktizierte Datenschutzniveau anzuheben. Allerdings ist für uns neben dem erheblichen Verwaltungsaufwand (durch z. T. umfangreichen Schriftverkehr) auch ein hoher Beratungsaufwand entstanden, da viele Studiobetreiber weder unsere Behörde noch grundlegende Anforderungen des Datenschutzrechts kannten. Möglicherweise werden wir bei künftigen Prüfungen dieser Art den Fragenkatalog im Sinne der Praktikabilität noch stärker eingrenzen.

Anteil der Fitnessstudios, die innerhalb der ersten Frist geantwortet haben



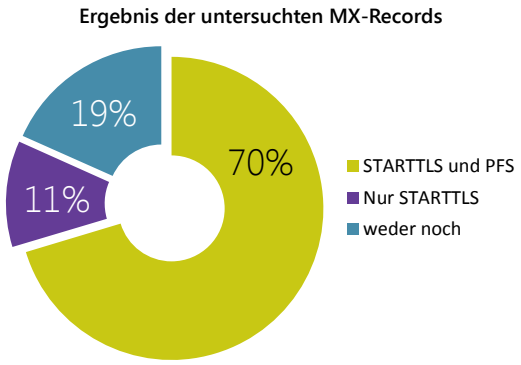
3.4.3 Mailserver

Bei der Diskussion um E-Mails wird häufig der Vergleich zur gewöhnlichen Postkarte gezogen, der darauf abzielt, dass jeder, der Zugriff auf eine versendete E-Mail hat, auch deren Inhalt lesen (und verändern) kann. Obwohl dieser Vergleich nicht falsch ist, bestehen unabhängig von den sinnvollen und notwendigen Formen der Inhaltsverschlüsselung von E-Mails (Stichwort PGP, S/MIME) bereits technische Möglichkeiten, eine TLS-Verschlüsselung beim Transport zwischen Mailservern einzurichten. Die Enthüllungen von Edward Snowden haben gezeigt, dass es mittlerweile starke Anhaltspunkte dafür gibt, dass jegliche Internetkommunikation systematisch ausgeleitet und erfasst wird. Im Frühjahr 2014 haben die Datenschutzaufsichtsbehörden in Deutschland mit der gemeinsamen Entschließung „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation" zu einer besseren und flächendeckenderen Verschlüsselung der Kommunikation aufgefordert. Dieses Schreiben, das auch in unserem Namen publiziert wurde, hat uns bewogen, den Worten Taten folgen zu lassen.

Hierzu haben wir 2236 verantwortliche Stellen in Bayern zufällig ausgewählt – anhand heuristischer und manueller Verfahren legten wir den Schwerpunkt auf größere und mittlere Unternehmen. Im Fokus der Prüfung standen die Unterstützung von STARTTLS, Perfect Forward Secrecy (PFS) und die Behebung der Heartbleed Lücke (siehe Kapitel 22.5 und 22.8).

Bei unserem ersten Prüfdurchlauf im September 2014 hatten wir positiv zur Kenntnis genommen, dass eine überwältigende Mehrheit bereits STARTTLS eingesetzt hatte. Von diesen hatten auch sehr viele Perfect Forward Secrecy unterstützt – ohne dieses Verfahren bietet eine Transportverschlüsselung heutzutage keinen wirksamen Schutz mehr. Erschreckend war jedoch, dass 44 Unternehmen die Heartbleed-Lücke, über die zu dem Zeitpunkt bereits seit einem halben Jahr in den Medien berichtet wurde, immer noch nicht auf Ihren Mailservern geschlossen hatten.

Die meisten Unternehmen hatten keine Schwierigkeiten, die von uns bemängelten IT-Sicherheitsanforderungen umzusetzen, da diese im Allgemeinen durch eine Anpassung der Mailserver-Konfiguration mit wenigen Zeilen Code sehr einfach durchzuführen ist.



Äußerst erstaunlich fanden wir dabei, dass es einige große deutsche IT-Dienstleister gab, die STARTTLS (und somit auch PFS) nicht unterstützten und sich dann auch erst mal "quer" gestellt hatten – zum Teil mit der Begründung, dass dies über dem derzeitigen Stand der Technik liege und somit überzogene Forderungen wären. Wenn dann auf den Webseiten dieser Dienstleister noch mit „E-Mail-Sicherheit Made in Germany" geworben wurde, löste dies bei uns durchaus Verwunderung aus. Mittlerweile können aber auch die meisten dieser Anbieter die von uns geforderten Mindestanforderungen für deren Kunden erfüllen.

Interessant war zudem, dass es einige führende und internationale Appliance-Hersteller gab, die Perfect Forward Secrecy nicht unterstützten, die sich aber auf Grund unserer Prüfung rasch persönlich bei uns meldeten und in kürzester Zeit neue Firmware-Versionen für ihre Kunden bereitstellten, um auch diesen Sicherheitsbaustein anbieten zu können.

Vom Ergebnis sehen wir unser Vorgehen, auch IT-Sicherheitsanforderungen bezüglich Verschlüsselungsverfahren nach dem Stand der Technik zu prüfen, als richtige und wegweisende Entscheidung an. Aus diesem Grund werden wir weiterhin automatisierte Onlineprüfungen im Bereich der IT-Sicherheit durchführen und unserer Prüfmethoden gezielt ausbauen.

3.4.4 Autohäuser

Unter anderem aufgrund von mehreren Beschwerden bezüglich des Kopierens von Personalausweisen bei verschiedenen Kfz-Händlern sahen wir uns veranlasst, im Jahr 2014 bei Autohändlern eine großflächige Prüfung durchzuführen. Ziel dieser Prüfung war es in erster Linie, kleine und mittelständische Unternehmen auf die Anforderungen des Datenschutzes hinzuweisen und für erforderliche Datenschutzmaßnahmen in konkreten Anwendungsfällen zu sensibilisieren.

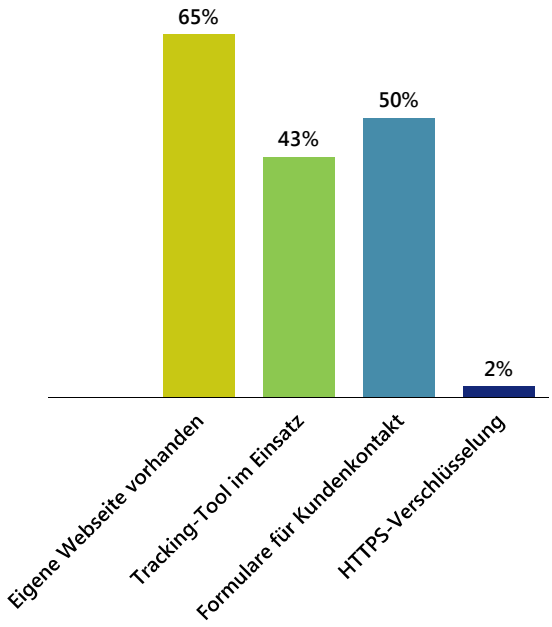
Insgesamt haben wir 107 Autohäuser bayernweit nach dem Zufallsprinzip ausgewählt. Neben grundsätzlichen datenschutzrechtlichen Anforderungen lag unser Fokus hierbei auf dem Kopieren von Personalausweisen, der Weitergabe personenbezogener Daten an Dritte (z. B. an Autohersteller) und IT-Sicherheitsmaßnahmen im Bereich der Unternehmens-Webseiten.

Im Ergebnis mussten wir feststellen, dass immerhin rund 70% der Kfz-Händler Ausweiskopien anfertigten und ungefähr 50% der Unternehmen personenbezogene Daten an Dritte weitergeleitet haben.

Kfz-Händler, welche Ausweiskopien anfertigten, wurden von uns darauf hingewiesen, dass das Kopieren von Personalausweisen, soweit kein Gesetz dies ausdrücklich vorschreibt, häufig Bedenken begegnet, da hier neben den Identifikationsdaten (Name, Adresse, Geburtsdatum) darüber hinausgehende Daten (wie Bild, Unterschrift, Ausweisnummer, Staatsangehörigkeit, Größe, Augenfarbe, etc.) erhoben werden, die in der Regel für die angestrebten Zwecke nicht erforderlich sind. Als Alternative wurde unsererseits vorgeschlagen, lediglich die notwendigen Identifikationsdaten aus den Ausweispapieren händisch abzuschreiben oder beim Kopieren z. B. mit Schablonen zu arbeiten, die alle nicht erforderlichen Daten abdecken.

Bei den festgestellten Datenübermittlungen an Dritte haben wir die betroffenen Autohäuser über die denkbaren Rechtsgrundlagen (z. B. Einverständniserklärung) informiert und auf die Umsetzung der gesetzlichen Anforderungen hingewirkt.

Im Bereich der IT-Sicherheit haben wir mehrere gravierende Mängel entdeckt. So hatten zwar zahlreiche Kfz-Händler eigene Webseiten mit der Möglichkeit, gezielt personenbezogene Daten der Webseitenbesucher in Formularen zu erfassen (z. B. bei Interesse an einem Wagen aus der Fahrzeugbörse), jedoch besaßen lediglich zwei Händler die dafür erforderliche HTTPS-Verschlüsselung. Auch unterstützten die eingesetzten Mailserver nur bedingt die von uns geforderten Einstellungen zu STARTTLS und PFS. Darüber hinaus setzten einige Autohäuser auch Werkzeuge zur Reichweitenmessung in einer unzulässigen Art und Weise ein, so dass wir auch dort auf Nachbesserungen hinwirken mussten.



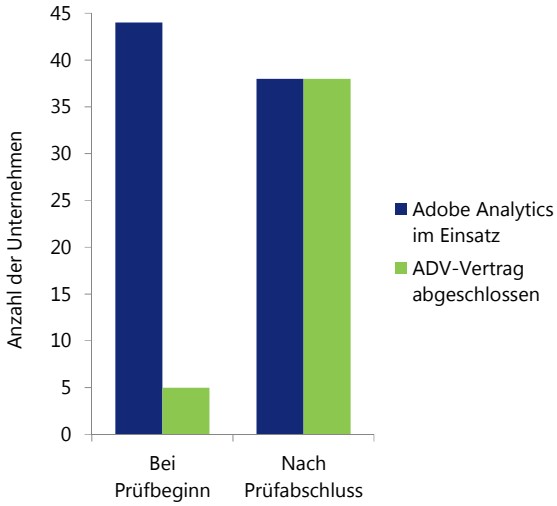
Zusammenfassend können wir festhalten, dass die grundlegenden datenschutzrechtlichen Vorgaben im Allgemeinen bei den Autohäusern meist eingehalten werden, jedoch insbesondere im Bereich der Ausweiskopien keine ausreichende Sensibilität und datenschutzrechtliche Kenntnisse vorhanden waren. Insbesondere das schlechte Abschneiden im technischen Bereich der Prüfung stimmt bedenklich und veranlasst uns dazu überzugehen, diese Punkte künftig noch stärker in den Prüffokus unserer Kontrollen zu nehmen.

3.4.5 Adobe Analytics

Nachdem wir 2012 eine Onlineprüfung bei 13.404 Webseiten hinsichtlich des Einsatzes von Google Analytics durchgeführt hatten, kündigten wir bereits damals die Prüfung weiterer Verfahren zur Reichweitenmessung an. Für diese Prüfung haben wir uns im Jahr 2013 das Verfahren Adobe Analytics (vormals Omniture SiteCatalyst) der Adobe Inc. ausgesucht, da dieses Werkzeug auch bei bayerischen Unternehmen zum Einsatz kommt und zudem Adobe eine Niederlassung in unserem Zuständigkeitsbereich besitzt. Vor der Durchführung unserer Prüfung haben wir uns deshalb mit Adobe über die datenschutzrechtlichen Anforderungen an den Einsatz des angebotenen Verfahrens in Verbindung gesetzt. Diese ergeben sich auch aus dem Beschluss des Düsseldorfer Kreises vom 26./27. November 2009 „Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten". Diskussionsschwerpunkte waren bei den Gesprächen der auf Anfrage zur Verfügung gestellte Auftragsdatenverarbeitungsvertrag, die Lebensdauer des Tracking-Cookies und die geforderte Anonymisierung der IP-Adressen.

Nachdem die Möglichkeit eines beanstandungsfreien Einsatzes durch die Webseitenbetreiber bei Vornahme verschiedener Einstellungen sichergestellt war, wurden 10.238 bayerische Webseiten online daraufhin geprüft, ob das Verfahren Adobe Analytics eingesetzt wird. Wir fanden so heraus, dass das Verfahren bei 44 Webseiten bzw. Unternehmen eingesetzt wurde. Da die Vornahme der erforderlichen Datenschutzeinstellungen und Vorkehrungen nicht ausschließlich in einer Onlineprüfung von uns durchgeführt werden konnte, wurden die betroffenen Webseitenbetreiber mit einem Fragebogen angeschrieben.

Im Ergebnis teilten uns sechs Webseitenbetreiber mit, dass sie das Verfahren Adobe Analytics zukünftig nicht mehr einsetzen, die anderen 38 Webseitenbetreiber nahmen unser Schreiben zum Anlass, entsprechende Anpassungen für einen beanstandungsfreien Einsatz des Verfahrens vorzunehmen, soweit unsere Forderungen noch nicht umgesetzt waren. So mussten beispielsweise noch zahlreiche Unternehmen den erforderlichen Vertrag zur Auftragsdatenverarbeitung abschließen.



Im Ergebnis müssen wir etwas überraschend feststellen, dass – obwohl ein Beschluss des Düsseldorfer Kreises zur Reichweitenmessung existiert und im Rahmen der vorangehenden „Google Analytics"-Prüfung die datenschutzrechtlichen Anforderungen an ein solches Verfahren in der breiten Öffentlichkeit bekannt gemacht wurden – diese oftmals nicht auf das konkrete Verfahren, in diesem Fall Adobe Analytics, übertragen werden. Dies bestärkt uns weiterhin das Gespräch mit Anbietern solcher Verfahren und vor allem mit den verantwortlichen Stellen zu suchen.

Weitere Angaben zum Verlauf der Prüfung und den rechtlichen Rahmenbedingungen befinden sich im Kapitel 7.3.

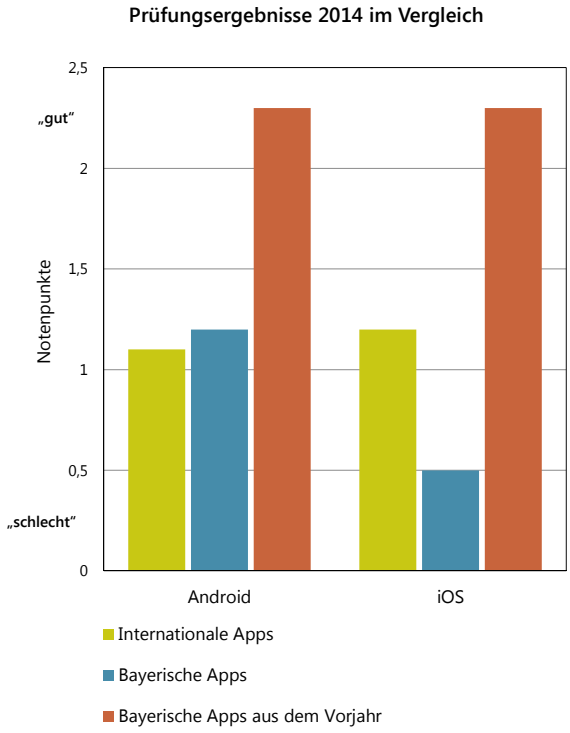
3.4.6 Mobile Applikationen (Apps)

Seit zwei Jahren führen wir größer angelegte Prüfungen bayerischer mobiler Applikationen (Apps) durch. Im Jahr 2013 hatten wir uns insbesondere durch technische Prüfungen von Apps (siehe Kapitel 22.1) und einer daraufhin rechtlichen Bewertung den speziellen technischen und rechtlichen Gegebenheiten im Zusammenhang mit Apps angenähert. Veranlasst durch den „GPEN International Sweep Day 2013", einer international angelegten Prüfaktion, führten wir dann auf der Grundlage unserer bis dahin erworbenen Kenntnisse eine größer angelegte Prüfung von 30 zufällig ausgewählten bayerischen Apps (jeweils 15 iOS- und Android-Apps) durch, wenngleich die weiteren teilnehmenden Datenschutzaufsichtsbehörden ihren Fokus bei dieser Prüfung noch auf herkömmliche Webseiten setzten.

Im Rahmen dieser koordinierten Prüfung des Global Privacy Network (GPEN) wurden mit vorab festgelegten (internationalen) Prüfkriterien die Transparenz der Apps überprüft. Ziel war es, zunächst einen Überblick über die jeweiligen Angebote zu erhalten, eine Vergleichbarkeit herzustellen und insbesondere datenschutzrechtliche Mängel festzustellen.

Nach Durchführung des „Sweeps" ist es den Aufsichtsbehörden freigestellt, weitergehende Prüfungen auf Basis des jeweils nationalen Rechts durchzuführen. Einer solchen weitergehenden Prüfung haben wir die Apps auch aufgrund des erschreckenden Prüfungsergebnisses, dass nur 25% der geprüften Apps über eine App-spezifische Datenschutzerklärung verfügten, unterzogen. Die 30 von uns behandelten Apps wurden dabei nicht allein auf die Prüfung der Transparenz limitiert, sondern zum Teil auch technisch überprüft.

2014 wurde ein weiterer Sweep-Day organisiert, bei dem diesmal explizit Apps und deren Transparenz im Prüffokus standen. Auch hieran haben wir uns beteiligt. Aus Gründen der Vergleichbarkeit beschränkten wir uns bei der Prüfung nach den internationalen Kriterien jedoch nicht mehr nur auf bayerische Apps (jeweils 15 iOS- und Android-Apps), sondern prüften auch internationale Apps (ebenfalls jeweils 15 iOS- und Android-Apps). Darüber hinaus kontrollierten wir nochmals die von uns im Vorjahr geprüften Apps nach den vorgegebenen Kriterien. Im Ergebnis wurden bei einer Punktevergabe (Note) von 0 bis 3 Punkten – wobei 0 die schlechteste und 3 die beste Note war –, folgende Ergebnisse erzielt:



Zwar war auch bei der Prüfung 2014 das Ergebnis der erstmalig geprüften Apps eher schlecht, jedoch konnten wir uns zumindest darüber freuen, dass bei den im Vorjahr negativ geprüften Apps mittlerweile – auch dank unserer Kontrolle und aufsichtlichem Tätigwerden – deutlich nachgebessert und ein gutes Prüfergebnis erzielt wurde.

In vielen Fällen, in denen Dienstleister bei der Entwicklung von Apps eingesetzt werden, müssen wir leider immer noch feststellen, dass sich App-Anbieter (Auftraggeber) zum Teil blind darauf verlassen, dass die datenschutzrechtlichen Anforderungen „automatisch" (d. h. ohne Anweisung und Kontrolle) vom Dienstleister bei der Programmierung berücksichtigt bzw. umgesetzt werden – was sich in manchen Fällen als tückischer Trugschluss erweist.

3.4.7 Arztpraxen

Im Tätigkeitsbericht 2011/2012 hatten wir über unsere Vor-Ort-Prüfungen in Arztpraxen berichtet. Diese verstärkte Prüfungstätigkeit im Gesundheitswesen haben wir nun im Rahmen von schriftlichen Prüfungen in den vergangenen Jahren fortgeführt. Dabei haben wir 16 Arztpraxen verschiedener Fachrichtungen ausgewählt – teils zufällig, teils aufgrund von Missständen, die durch anonyme Eingaben bekannt wurden.

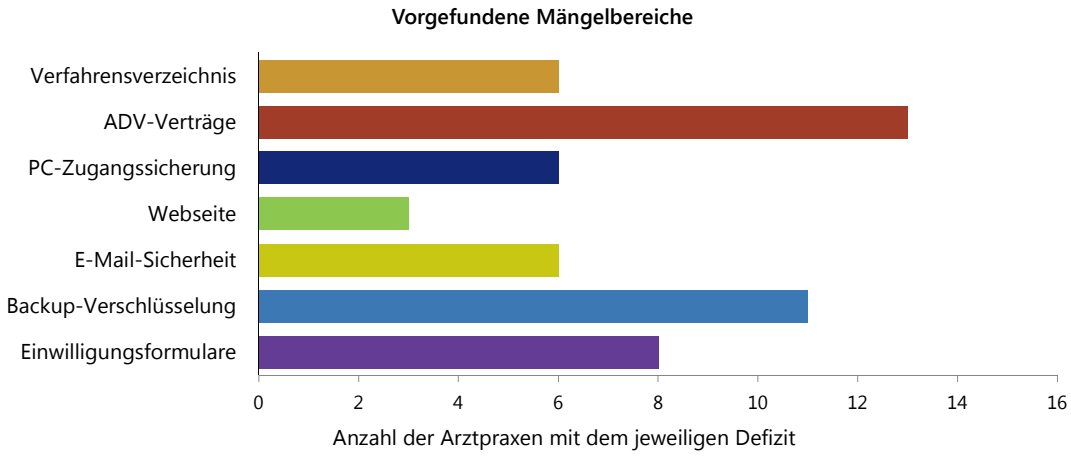
Inhalte unseres umfangreichen Fragebogens waren Fragen der Praxisorganisation (z. B. Praxisstruktur, Empfangs- und Wartebereich), materiell-rechtliche Themen des Datenschutzes (u. a. Verfahrensverzeichnis, Datenweitergabe an externe Stellen) und Aspekte der Datensicherheit (insbesondere Backup-Konzept und E-Mail-Kommunikation).

Um ausführliche Antworten auf die umfassenden Fragen erhalten zu können, haben wir den Ärzten, deren Hauptaufgabe bei der Versorgung und Betreuung ihrer Patienten liegt, lange Fristen und auch großzügig Fristverlängerungen gewährt. Trotzdem trafen wir manchmal auf Unverständnis und sogar auf Ignoranz unserer Schreiben. Zum Teil wurden die Fragen erst beantwortet, als ein Zwangsgeld angedroht worden war.

Da Ärzte unweigerlich im Alltag mit Gesundheitsdaten und damit mit besonders sensiblen Daten umgehen müssen und zudem der strafrechtlich bewehrten Schweigepflicht unterliegen, kommt der Beachtung datenschutzrechtlicher Vorgaben in Arztpraxen besondere Bedeutung zu. Allerdings zeigte unsere Prüfung, dass in vielen Bereichen erheblicher Nachbesserungsbedarf bestand (siehe Grafik).

Bei den meisten überprüften Praxen wurde inzwischen nachgebessert, so dass der Abschluss der letzten Prüfungen unmittelbar bevorsteht. Wir gehen davon aus, dass wir das Ziel unserer Prüfung, den Ärzten und ihren Mitarbeitern die Sensibilität der Patientendaten und die erforderliche Sorgfalt beim täglichen Umgang mit diesen nochmals bewusst zu machen, erreicht haben. Außerdem haben wir den Eindruck, dass wir nicht nur die geprüften Praxen, sondern durch die Streuwirkung auch andere Praxen erreicht, auf uns aufmerksam gemacht und sensibilisiert haben.

Weitere Ausführungen zu dieser Prüfung befinden sich im Kapitel 16.1.



3.4.8 Smart-TV

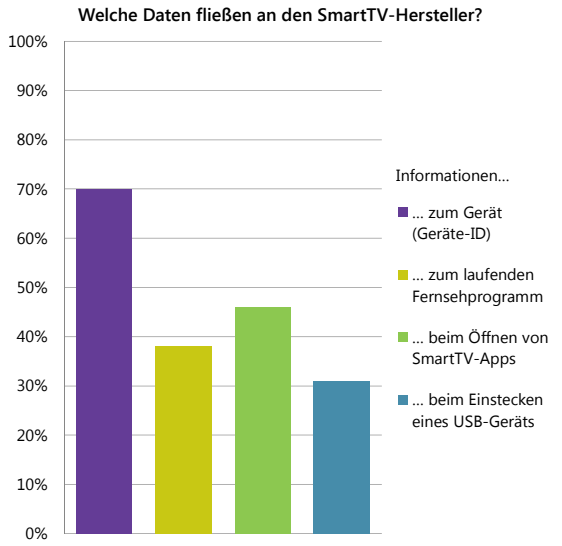
„Der Spion im eigenen Wohnzimmer", „TV mit Augen" oder schlichtweg „ein heimlicher Schnüffler" – Smart-TVs wurde 2013 in den Medien einiges unterstellt, z. B. im Hintergrund heimlich das Umschaltverhalten des Fernsehzuschauers zu übertragen und gar mittels eingebauter Kamera den Nutzer gezielt zu Hause zu überwachen. Da die Berichterstattung zu diesem Zeitpunkt nur sehr wenige technische Fakten präsentierte – und diese ggf. meist undifferenziert –, wollten wir wissen, welche Wahrheiten sich tatsächlich hinter diesen Schlagzeilen verbergen. Daher haben wir uns des Themas bereits Ende 2013 angenommen und auf Basis der – leider sehr wenigen – vorhandenen wissenschaftlichen Untersuchungen den Smart-TVs allmählich technisch angenähert.

Im Laboraufbau haben wir bei unserem ersten Testgerät unter anderem festgestellt, dass nicht nur beim Umschalten eines Senders, sondern bereits beim Einschalten des Fernsehgeräts an zahlreiche unterschiedliche Server weltweit Daten übertragen werden. Dies hat uns dazu veranlasst, das Thema gezielt technisch aufzuarbeiten und sowohl an die verantwortlichen Stellen selbst als auch an die Datenschutzaufsichtsbehörden der anderen Bundesländer mit dem erarbeiteten Wissen heranzutreten.

Während wir 2014 zuerst damit begonnen haben, die verschiedenen Akteure und unterschiedlichen Verantwortungssphären bei Smart-TV-Nutzung aus rechtlicher Sicht abzugrenzen, d. h. auch unsere Zuständigkeit für ein mögliches aufsichtliches Tätigwerden zu definieren, konnten wir auch durch verschiedene technische Testszenarien Erfahrung sammeln und zur Vorbereitung einer Großprüfung nutzen. Parallel dazu haben wir begonnen, auch HbbTV-Angebote in unserer Zuständigkeit zu begutachten und die verantwortlichen Stellen bei festgestellten Mängeln zu kontaktieren.

Ende 2014 konnten wir in Absprache mit und in Amtshilfe für die Datenschutzaufsichtsbehörden in Berlin, Hamburg, Hessen, Nordrhein-Westfalen und Rheinland-Pfalz Smart-TV-Geräte von insgesamt 13 Herstellern prüfen. Diese haben ihren Sitz in Deutschland (oder zumindest eine deutsche Niederlassung) und decken gleichzeitig mehr als 90% des Marktes in Deutschland ab. Der Fokus der gerätebezogenen Prüfung lag dabei auf dem Verhalten des jeweiligen Geräteherstellers, z. B. wie er den Zuschauer/Nutzer über die Datennutzung am Smart-TV informiert und welche Datenflüsse er im Hintergrund initiiert (Inhalt und Ablauf dieser Prüfung siehe Kapitel 22.11).

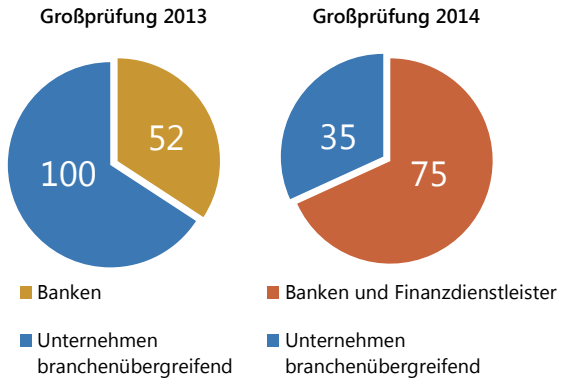
Das hierbei festgestellte Ergebnis war äußerst vielfältig und zum Teil auch überraschend. So haben wir bei Szenarien der gewöhnlichen TV-Nutzung Datenflüsse festgestellt, die nicht direkt zu erwarten waren. Abgesehen vom vorhandenen Informationsdefizit (keine Datenschutzhinweise bei vielen Herstellern) war auffällig, dass gerade die Zusatzdienste der Smart-TVs das Fernseherlebnis persönlicher gestalten wollten, hierfür jedoch viele Nutzeraktionen z. B. wie Umschalten auf einen anderen Sender, Aufnehmen von Sendungen, Abspielen von Inhalten eines USB-Sticks, etc. an den Hersteller übertrugen.



Die Ergebnisse dieser technischen Prüfung werden nun als Basis für eine rechtliche Bewertung dienen, die ab Frühjahr 2015 beginnen kann. Danach wird sich zeigen, welche aufsichtlichen Maßnahmen wir ergreifen können und werden. Ausführliches zu dieser Prüfung befindet sich im Kapitel 22.11.

3.4.9 Datenschutzorganisation

Auf Grund unserer durchweg positiven Erfahrungen im Umgang mit präventiven Maßnahmen und Prüfungen hatten wir uns auch im vergangenen Berichtszeitraum wieder entschlossen, anlasslos 262 Unternehmen (Banken, Finanzdienstleister und Unternehmen anderer Branchen) in Bayern im Rahmen zweier Großprüfungen zu kontrollieren. Die Auswahl dieser Unternehmen erfolgte zum Teil regional, d. h. nach Regierungsbezirken, da bereits in den vergangenen Jahren Kontrollen speziell bei Banken bestimmter Regionen stattgefunden hatten. Die Unternehmen, die nicht aus dem Finanzsektor stammten, wurden aus dem Verzeichnis einer branchenübergreifenden Dachorganisation nach dem Zufallsprinzip ausgewählt.



Die verantwortlichen Stellen erhielten hierfür neben Informationsblättern einen Fragebogen, um uns ein Bild des aktuellen Umsetzungsstandes datenschutzrechtlicher Vorschriften in den geprüften Unternehmen machen zu können.

Der Fragenkatalog umfasste zahlreiche allgemeine Prüfpunkte zur Datenschutzorganisation (z. B. Verpflichtung auf das Datengeheimnis, Bestellung und Aufgabenerfüllung des Datenschutzbeauftragten, Auftragsdatenverarbeitung, Videoüberwachung, private Verwendung von Kommunikationsmitteln am Arbeitsplatz) sowie einige Sicherheitsmaßnahmen aus dem technischen Bereich.

Als Ergebnis der Prüfung haben wir erkannt, dass bei einem Großteil der Unternehmen die grundlegenden Vorgaben aus dem BDSG, wie z. B. die Bestellung eines Datenschutzbeauftragten oder die Verpflichtung der Beschäftigten auf das Datengeheimnis, erfüllt waren. Lediglich ca. fünf Prozent der geprüften Unternehmen haben erst aufgrund unseres Anschreibens mit der Datenschutzumsetzung im Sinne der gesetzlichen Anforderungen begonnen. Bei manchen Unternehmen gab es jedoch im Detail noch mehr oder weniger deutliche Lücken, die erst aufgrund der Prüfungsinitiative aufgearbeitet wurden.

Die häufigsten Mängel waren festzustellen bei der Bestellung und Tätigkeit des Datenschutzbeauftragten, z. B. wegen nicht vertretbarer Interessenkollision (Datenschutzbeauftragter gleichzeitig DV-Administrator, Personalchef, Vorstand oder ähnliches), bei der (zu langen) Speicherdauer der Videoüberwachungsdaten oder einer fehlenden Regelung der privaten Internet- und E-Mail-Nutzung am Arbeitsplatz.

In Einzelfällen haben wir im Nachgang zur schriftlichen Großprüfung zusätzlich noch eine Vor-Ort-Prüfung durchgeführt, um gewisse Bereiche einer vertieften Kontrolle zu unterziehen und in Stichproben die Angaben der Unternehmen zu überprüfen.

Die anlasslosen Kontrollen mittels einer schriftlichen Abfrage dieser Art empfinden wir als eine gut geeignete Möglichkeit, in kurzer Zeit eine große Anzahl Unternehmen, Freiberufler, Vereine etc. zu erreichen. Aus diesem Grund planen wir auch in Zukunft in dieser oder ähnlicher Form solche Datenschutzorganisationsprüfungen durchzuführen.

3.4.10 Videoüberwachung

Eine Münchner Tageszeitung berichtete im April 2013 unter der Überschrift „Die Fußgängerüberwachungszone“ über Videokameras in Geschäften der Münchner Fußgängerzone. In dem Bericht waren die Standorte vieler Kameras aufgeführt und mögliche Verstöße gegen das Datenschutzrecht benannt. So wurde z. B. vermutet, dass über die Türschwelle hinaus auf den Gehweg gefilmt werden würde, weil bei den teilweise eingesetzten Domekameras die Ausrichtung nicht klar zu erkennen war. Darüber hinaus wurden die fehlenden aber gem. § 6b Abs. 2 BDSG erforderlichen Hinweise auf die Videoüberwachung moniert.

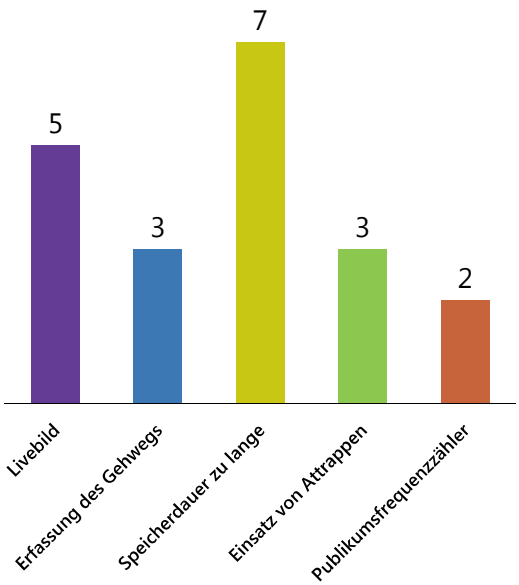
Angeregt durch diesen Bericht haben wir die Zulässigkeit der Videoüberwachung in zahlreichen Geschäften innerhalb der Münchner Fußgängerzone überprüft. Kontrolliert wurde dabei, ob die Vorschriften zur Videoüberwachung von öffentlich zugänglichen Räumen nach § 6b BDSG eingehalten werden. Nach dieser Bestimmung ist die Beobachtung öffentlich zugänglicher Räume (z. B. Ladenflächen und Verkaufsräume) mit optisch-elektronischen Einrichtungen (Videoüberwachung) für private Stellen nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Insgesamt wurde die Videoüberwachung in 27 Unternehmen anhand verschiedenster Kriterien wie z. B. Zweck der Videoüberwachung, Speicherdauer, Zugriffsrechte, Löschungskonzept, etc. überprüft. Festgestellt haben wir, dass es zwar einige Unzulänglichkeiten bei der Videoüberwachung gegeben hat, gravierende Verstöße oder nachhaltiges Verweigern, den Anforderungen der Datenschutzaufsicht Rechnung zu tragen, haben wir jedoch nicht festgestellt. Die Prüfung hatte deshalb weder den Erlass von Anordnungen zur datenschutzkonformen Nutzung von Videoüberwachungsanlagen noch den Erlass von Bußgeldbescheiden zur Folge.

Bei der absoluten Anzahl der installierten Kameras wurden wir jedoch überrascht: bis zu 70 Kameras waren alleine in einem großen Geschäft montiert. Befürchtungen, dass weite Flächen der Fußgängerzone von den Geschäften aus videoüberwacht würden, haben sich in den meisten Fällen aber nicht bestätigt. Lediglich einzelne Unternehmen wurden aufgefordert, die Einstellungen der Kameras entsprechend abzuändern.

Nicht ganz zu erwarten war zudem das Ergebnis, dass die Daten nur bei gut der Hälfte der überprüften Unternehmen tatsächlich gespeichert werden – die anderen verzichteten auf diese Art der Datenverarbeitung. Bei den Speicherfristen gab es hierbei noch größere Spannen: manche Stellen speicherten die Aufzeichnungen teilweise sogar länger als 14 Tage. In der Regel sind diese Daten jedoch, außer in begründeten Ausnahmefällen, nach zwei bis drei Arbeitstagen zu löschen. Wir haben deshalb veranlasst, dass die Löschfristen entsprechend angepasst werden.

Feststellungen bei den 27 geprüften Stellen



Weitere Angaben zu dieser Prüfung befinden sich in Kapitel 19.2.

4

Der betriebliche Datenschutzbeauftragte

4 Der betriebliche Datenschutzbeauftragte

4.1 Auditierung der Arbeit des Datenschutzbeauftragten

Eine Auditierung der DSB-Tätigkeit ist nur in allgemeiner Form möglich.

Anlässlich von Auditierungsverfahren durch externe Prüfer eines Unternehmens haben sich Datenschutzbeauftragte an uns mit der Frage gewandt, ob sie sich in ihrem Aufgabenbereich als betriebliche Datenschutzbeauftragte solchen Audits uneingeschränkt unterziehen lassen müssen.

Aufgrund der besonderen Rechtsstellung eines Datenschutzbeauftragten nach § 4f BDSG, insbesondere der weisungsfreien Ausübung der Fachkunde auf dem Gebiet des Datenschutzes gemäß § 4f Abs. 3 Satz 2 BDSG und der besonderen Verschwiegenheitspflicht gemäß § 4f Abs. 4 BDSG, ist eine Auditierung der Tätigkeit eines Datenschutzbeauftragten nach unserer Auffassung nur in allgemeiner Form und unter Berücksichtigung der besonderen Rechtsstellung des Datenschutzbeauftragten möglich. So muss z. B. die Möglichkeit einer inhaltlichen Kenntnisnahme von den beim Datenschutzbeauftragten anhängigen oder bearbeiteten Eingaben und Beschwerden ausgeschlossen sein.

4.2 Keine Meldepflicht für die Bestellung eines Datenschutzbeauftragten

Das BDSG regelt für die verantwortliche Stelle keine Mitteilungs-, Veröffentlichungs- oder Meldepflicht zur Person des Datenschutzbeauftragten.

Des Öfteren beschweren sich unzufriedene Kunden oder per Werbung angesprochene Personen bei uns darüber, dass ihnen zu ihrer Nachfrage von der verantwortlichen Stelle nicht der Name und die Kontaktdaten des bestellten Datenschutzbeauftragten genannt werden und wollen diese Information von uns bekommen.

Das BDSG regelt für die verantwortliche Stelle jedoch keine Mitteilungs-, Veröffentlichungs- oder Meldepflicht zur Person und den direkten Kontaktdaten des Datenschutzbeauftragten, so dass die betroffenen Personen insoweit keine konkrete datenschutzrechtliche Anspruchsgrundlage haben.

Andererseits bestimmt das BDSG, dass sich Betroffene jederzeit an den Datenschutzbeauftragten wenden können (§ 4f Abs. 5 Satz 2 BDSG) und dass der Datenschutzbeauftragte die Verfahrensübersicht jedermann in geeigneter Weise verfügbar macht (§ 4g Abs. 2 Satz 2 BDSG).

Manche verantwortliche Stellen wollen durch zurückhaltende Informationen nach außen ihren Datenschutzbeauftragten und seine tägliche Arbeit vor Querulanten etc. schützen.

Ungeachtet dessen sehen wir es als datenschutzfreundlich an, die Person des Datenschutzbeauftragten eines Unternehmens grundsätzlich auch extern angemessen publik zu machen, z. B. durch Nennung auf der Homepage des Unternehmens, oder zumindest mit einer Funktions-E-Mail-Adresse eine direkte Kontaktaufnahme zu ermöglichen.

4.3 Langfristige Erkrankung eines Datenschutzbeauftragten (Zuverlässigkeit)

Kann der bestellte Datenschutzbeauftragte seine Aufgaben wegen einer langfristigen Erkrankung auf unabsehbare Zeit nicht erfüllen, besteht Handlungsbedarf für die verantwortliche Stelle.

Einige Anfragen von Unternehmen betrafen Sachverhalte des längeren krankheitsbedingten Ausfalls des Datenschutzbeauftragten und der sich daraus ergebenden Folgerungen.

Die längerfristige krankheitsbedingte Abwesenheit des Datenschutzbeauftragten kann in

Unternehmen zunächst regelmäßig mit einer Stellvertreter-Regelung überbrückt werden, wenn die Rückkehr des Datenschutzbeauftragten absehbar ist (siehe dazu auch unseren 3. Tätigkeitsbericht (2008) unter Nr. 3).

Eine über viele Monate andauernde langfristige Erkrankung mit nicht absehbarem Rückkehrzeitpunkt kann jedoch die zuverlässige Aufgabenerfüllung des Datenschutzbeauftragten im Sinne von § 4f Abs. 2 Satz 1 BDSG ausschließen, so dass für die verantwortliche Stelle zum Schutz der Betroffenen (siehe § 4g Abs. 1 und § 4f Abs. 5 Satz 2 BDSG) ein Widerruf der Bestellung aus wichtigem Grund (§ 4f Abs. 3 Satz 4 BDSG) und eine folgende Neubestellung einer anderen Person geboten sein kann.

Zum arbeitsrechtlichen Vorgehen beim Widerruf der Bestellung mittels Teil-Kündigung siehe das Urteil des Bundesarbeitsgerichts vom 13. März 2007, Az. 9 AZR 612/05.

4.4 Einsichtnahme in Personalakten durch den Datenschutzbeauftragten

Auch Personalakten können vom Datenschutzbeauftragten im Rahmen seiner Aufgabenerfüllung nach datenschutzrechtlichen Gesichtspunkten überprüft werden.

Uns wurde ein Fall geschildert, in dem einem Datenschutzbeauftragten die datenschutzrechtliche Prüfung von Personalakten in seinem Unternehmen verweigert werden sollte. Diesen Schutz der Personalakten auch ihm gegenüber hielt der Datenschutzbeauftragte als zu weitgehend und sah sich in der Erfüllung seiner gesetzlichen Aufgaben beeinträchtigt.

Aufgrund seiner Aufgabenstellung nach § 4g Abs. 1 Satz 1 BDSG – Hinwirkung auf die Einhaltung des BDSG und anderer Vorschriften über den Datenschutz – ist der Datenschutzbeauftragte nach unserer Auffassung auch berechtigt, stichprobenartig zum Zweck der Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften Einsicht in Personalakten zu nehmen, z. B. um die Frage der Erforderlichkeit gespeicherter Daten zu den Beschäftigten im Rahmen von § 32 Abs. 1 BDSG zu prüfen.

Wir orientieren uns insoweit am Bundesarbeitsgericht, das z. B. für den Fall der Revision entschieden hat, dass für deren Prüfungszwecke im Einzelfall Einsicht in Personalakten genommen werden kann und dies nicht von einer Zustimmung des betroffenen Beschäftigten abhängig ist (Urteil vom 4. April 1990, Az. 5 AZR 299/89). Gleiches muss aufgrund seiner Funktion auch für den Datenschutzbeauftragten gelten, sonst könnte er seiner Aufgabenstellung in Bezug auf Personalakten und -daten im Sinne des Schutzes der Beschäftigten nicht hinreichend nachkommen.

4.5 Keine DSB-Bestellpflicht bei normaler Videoüberwachung (Tankstelle)

Auch bei Tankstellen ist ein Datenschutzbeauftragter regelmäßig erst dann zu bestellen, wenn mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, nicht aber schon, wenn eine normale Videoüberwachung installiert wird.

Verschiedentlich wurden wir von Tankstelleninhabern angefragt, ob sie auch mit weniger als zehn beschäftigten Personen wegen der bei ihnen eingesetzten Videokameras von Gesetzes wegen einen Datenschutzbeauftragten bestellen müssen.

Wir sehen bei kleinen Tankstellen mit weniger als zehn beschäftigten Personen (§ 4f Abs. 1 BDSG) allein wegen der dort üblicherweise eingesetzten Videoüberwachung keine Pflicht zur Bestellung eines Datenschutzbeauftragten. Wir gehen beim Einsatz einer Videoüberwachung nicht generell von einer Vorabkontrollpflicht nach § 4d Abs. 5 und 6 BDSG aus. Für eine Vorabkontrollpflicht wegen des Einsatzes von Videokameras müssen aus unserer Sicht weitere Umstände hinzukommen, dass von

besonderen Risiken für die Rechte und Freiheiten der Betroffenen im Sinne von § 4d Abs. 5 BDSG durch die Videoüberwachung gesprochen werden kann, z. B. besonders intensive Überwachungsformen.

Unabhängig davon verbleiben für die Tankstelleninhaber als verantwortliche Stellen im Sinne des BDSG natürlich die allgemein geltenden Pflichten aus dem BDSG, wie die Beschäftigten bei der Verpflichtung auf das Datengeheimnis nach § 5 BDSG über die Datenschutzanforderungen in ihrem Arbeitsbereich zu unterrichten und die Videoüberwachung insgesamt datenschutzkonform nach §§ 6b und 9 BDSG durchzuführen.

5

Auftragsdatenverarbeitung oder Funktionsübertragung allgemein

5 Auftragsdatenverarbeitung oder Funktionsübertragung allgemein

5.1 Miete von Räumen und Rechnern (Housing) ist keine Auftragsdatenverarbeitung

Die reine Miete von Räumen und Rechnern ist keine Auftragsdatenverarbeitung.

Aus Platz- und Infrastrukturgründen mieten inzwischen wieder häufiger Unternehmen extern Räume und Rechner an, um dort ihre (auch personenbezogenen) Daten zu verarbeiten. Dabei stellt sich die Frage, wie solche Sachverhalte datenschutzrechtlich einzuordnen sind.

Die reine Miete von Räumen mit Infrastruktur (Strom, Kühlung/Heizung, TK-Anbindungsmöglichkeit etc.) als Standort von gemieteten Rechnern („Housing", d. h. „Zurverfügungstellung der Hülle") ohne konkrete Verarbeitungsvorgänge bezüglich der Daten (keine Netz-, Support-, Wartungs- und Datensicherungsleistungen bezüglich der Datenverarbeitung durch den Vermieter) ist nach unserer Auffassung keine nach § 11 BDSG zu regelnde Auftragsdatenverarbeitung; es fehlt dabei an einem Vorgang der Verarbeitung personenbezogener Daten im Sinne des BDSG durch den Vermieter.

Im Rahmen der allgemeinen Sicherheitsmaßnahmen nach § 9 BDSG sind in dem Mietverhältnis angemessene Regelungen insbesondere zur Raum- und Infrastruktursicherheit zu treffen.

5.2 Archivierung verschlüsselter Daten ist keine Auftragsdatenverarbeitung

Sind extern archivierte Datenbestände sicher verschlüsselt, gehen wir beim Archivdienstleister nicht mehr von einer Personenbeziehbarkeit der Daten aus.

Bei großen und meist aus handels- und steuerrechtlichen Gründen längerfristig zu archivierenden Datenbeständen mit personenbezogenen Daten, z. B. Buchhaltungsunterlagen, ist für manche Unternehmen die externe Auslagerung an einen spezialisierten Dienstleister zur dortigen Speicherung und Sicherung der Daten ein Thema.

Aus Datenschutz- und Datensicherheitsgründen (Betriebsgeheimnisse) werden manchen Archivdienstleistern die Datenbestände nur in vorher nach dem aktuellen Stand der Technik sicher verschlüsselter Form überlassen.

Es stellt sich dann die Frage, ob bei dem Archivdienstleister noch von einem Umgang mit personenbeziehbaren Daten im Sinne des Datenschutzrechts auszugehen ist.

Nach Ziffer 26 der Erwägungsgründe zur EU-Datenschutzrichtlinie 95/46 sollten bei der Entscheidung, ob eine Person bestimmbar ist, alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden können, um die betreffende Person zu bestimmen.

Das Arbeitspapier WP 136 der EU-Art. 29-Datenschutzgruppe führt dazu auf Seite 17 unten weiter aus, dass die rein hypothetische Möglichkeit zur Bestimmung der Person nicht ausreicht, um die Person als "bestimmbar" anzusehen.

>>> *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf*

Ein Teil der deutschen Datenschutzaufsichtsbehörden hält personenbezogene Daten, die mit einem starken kryptografischen Verfahren nach dem aktuellen Stand der Technik sicher verschlüsselt sind, bei einem Dienstleister für nicht personenbezogen, da er sie nicht zur Kenntnis nehmen könne. Zu dieser Gruppe der Aufsichtsbehörden gehören auch wir.

Erhält also ein externer Dienstleister nur vollständig und sicher verschlüsselte Daten als Archivar zur Aufbewahrung, ist dies dort keine Verarbeitung personenbezogener Daten im Auftrag nach § 11 BDSG.

Der Auftraggeber muss dabei jedoch trotzdem vertraglich ein Mindestmaß an Kontrolle und Weisungsbefugnis über die Verarbeitung der verschlüsselten Daten beim Dienstleister behalten, z. B. dass er ohne weiteres die Daten bzw. Datenträger vollständig zurückfordern kann oder dass ein Subunternehmer-Einsatz ausgeschlossen ist. Die Schutzwirkung einer Verschlüsselung hält bekanntermaßen infolge steigender Rechnerleistungen nicht jahrelang an – insoweit muss der Auftraggeber die technische Entwicklung im Auge behalten.

5.3 Zusatzleistungen von Postunternehmen sind häufig Auftragsdatenverarbeitung

Zusatzdienste von Postunternehmen, die über die Transport- und Zustellleistung hinausgehen, erfüllen häufig den Tatbestand einer nach § 11 BDSG zu regelnden Auftragsdatenverarbeitung.

Postunternehmen bieten als zusätzlichen Service für ihre Kunden neben dem Postzustell-Dienst inzwischen teilweise Zusatzleistungen wie "zentrale Adressverwaltung" oder "Auftragsübersicht" an, die auf Kundenwunsch erbracht werden.

Solche Zusatzdienstleistungen im Kundenauftrag mit einer Verwendung personenbezogener Daten gehen über die eigentliche Postdienstleistung nach dem Postgesetz und der Postdienstleistungsverordnung (Transport-/ Zustellleistung) hinaus und sind datenschutzrechtlich gesondert zu beurteilen.

Die externe Auslagerung z. B. von Kundenadressen an Postunternehmen zur einfacheren Versendungsorganisation, zur Datenpflege und Aktualisierung, oder auch die Auslagerung der Verwaltung und Kontrolle der Versandaufträge sind als weisungsgebundene Datenverarbeitungen im Auftrag nach § 11 BDSG einzuordnen und zu regeln.

5.4 Kontrollmöglichkeit darf nicht ausgeschlossen werden

Unabhängig davon, ob klassische IT-Rechendienstleistungen oder Datenhosting, Prüfung und Wartung von Systemen und Software im Auftrag durchgeführt werden: Der Auftraggeber als nach dem BDSG verantwortliche Stelle darf von Kontrollmöglichkeiten beim Dienstleister nicht ausgeschlossen sein.

Aus der Praxis wird uns immer wieder vorgetragen, dass – meist ausländische – Unternehmen, die zu personenbeziehbaren Daten IT-Rechendienstleistungen oder Datenhosting, Prüfung und Wartung von Systemen und Software im Sinne von § 11 BDSG erbringen, den Auftraggebern möglichst keine eigenständigen Vor-Ort-Auftragskontrollrechte einräumen oder solche Rechte jedenfalls vertraglich abbedingen möchten, etwa, indem der Auftraggeber „darauf verzichtet".

Hierzu vertreten die deutschen Datenschutzbehörden die Auffassung, dass es nicht zulässig ist, die Vor-Ort-Kontrolle durch den Auftraggeber (oder einen vom Auftraggeber ausgewählten geeigneten Dritten) rechtlich/vertraglich auszuschließen. Dies wäre mit der aufgrund von § 11 Abs. 1 Satz 1 BDSG bestehenden umfassenden datenschutzrechtlichen Verantwortlichkeit des Auftraggebers als verantwortliche Stelle auch für die Datenumgänge beim Auftragnehmer und gegebenenfalls bei von dort eingeschalteten Subauftragnehmern nicht zu vereinbaren.

Dies gilt nach § 11 Abs. 5 BDSG auch für Fälle der Prüfung und Wartung von Systemen und Software.

Hinsichtlich der praktischen Durchführung der Auftragskontrolle im Alltag ist nicht allgemein eine Vor-Ort-Kontrolle zwingend. Häufig ist es sachgerecht und ausreichend, dass der Auftragnehmer sein Datensicherheitskonzept

und/oder Datensicherheitszertifikate vorlegt und der Auftraggeber dies auf Schlüssigkeit und Nachvollziehbarkeit hin prüft.

5.5 Einbindung von freien Mitarbeitern

Freie Mitarbeiter können als Auftragsdatenverarbeiter tätig oder vergleichbar den Festangestellten beschäftigt sein.

Das Bedürfnis nach Flexibilität beim Personaleinsatz in Unternehmen führt teilweise auch zum Einsatz von sog. freien Mitarbeitern, die von Unternehmen bei Bedarf außerhalb des klassischen Arbeitsverhältnisses – meist vorübergehend – beschäftigt werden.

Welche datenschutzrechtliche Einordnung von solchen freien Mitarbeitern eines Unternehmens jeweils sachgerecht ist, hängt nach unserer Auffassung im Wesentlichen davon ab,

- ob der Externe/Freie nach den Vorgaben und unter der Aufsicht der verantwortlichen Stelle, vergleichbar den festangestellten Mitarbeitern (z. B. zur Bewältigung von Arbeitsspitzen), tätig wird, oder
- ob der Externe/Freie auf weitgehend eigenständiger Basis seine Dienstleistungen für die verantwortliche Stelle erbringt (z. B. beauftragt mit Programmierung und Wartung von spezieller Software).

Im letzteren Fall wäre eine vertragliche Beauftragung des Externen nach § 11 BDSG das richtige Mittel nach dem BDSG, im ersteren Fall eine Verpflichtung nach § 5 BDSG auf das Datengeheimnis.

5.6 Vertragliche Regelungen zum Datenschutz bei Aufgaben- oder Funktionsauslagerungen

Bei den vertraglichen Gestaltungen der datenschutzrechtlichen Seite einer Aufgabenauslagerung bzw. Funktionsübertragung kommt es nach unserer Auffassung wesentlich darauf an, um welche Art der Auslagerung und um welche Aufgabenübernehmer es sich handelt.

Immer wieder werden wir gefragt, wie die vertraglichen Regelungen zum Datenschutz bei einer Aufgaben- oder Funktionsausgliederung aussehen müssen.

Während der aus datenschutzrechtlicher Sicht notwendige Inhalt von Verträgen zur weisungsgebundenen Auftragsdatenverarbeitung in § 11 Abs. 2 Satz 2 BDSG vom Gesetz her schon detailliert vorgegeben wird, bestehen für die Auslagerung von Aufgaben bzw. Funktionen an Dritte wegen der verschiedenen Art der möglichen Auslagerungen keine solchen konkreten Vorgaben.

Häufig kann für die datenschutzrechtliche Rechtfertigung der Aufgaben- oder Funktionsausgliederung mangels anderer Rechtsgrundlagen nur die Regelung in § 28 Abs. 1 Satz 1 Nr. 2 BDSG als rechtliche Basis herangezogen werden. Bei der in § 28 Abs. 1 Satz 1 Nr. 2 BDSG vorgeschriebenen Abwägung der Interessen der verantwortlichen Stelle mit den schutzwürdigen Interessen der betroffenen Personen für die Bewertung der Zulässigkeit der mit einer Aufgaben- oder Funktionsausgliederung verbundenen Übermittlung personenbezogener Daten ist auch entscheidend, inwieweit die verantwortliche Stelle in dem Vertrag mit dem Übernehmer die Datenschutzbelange sicherstellt. § 28 Abs. 5 Satz 3 BDSG regelt z. B. ausdrücklich, dass die übermittelnde Stelle den Dritten als Datenempfänger auf die Zweckbindung der betreffenden personenbezogenen Daten hinweisen muss.

Bei der Aufgaben- oder Funktionsauslagerung an bereichsspezifisch streng reglementierte Dritte, wie z. B.

- der Auslagerung der Lohnabrechnung, Steuererklärung oder Finanzbuchhaltung an einen Steuerberater oder
- der betriebsärztlichen Betreuung an einen niedergelassenen Arzt,

sind aus unserer Sicht allgemeinere Regelungen zu den durchzuführenden Tätigkeiten, zur Zweckbindung von übermittelten Daten und zur Geheimhaltung ausreichend, weil die dort geltenden berufsrechtlichen Vorschriften (Steuerberatergesetz, Ärztliche Berufsordnung, § 203 Abs. 1 StGB, usw.) schon Grenzen ziehen und eigenverantwortliche Pflichten festlegen. Zudem besteht dort auch noch eine berufsrechtliche Kammeraufsicht, die für die Einhaltung der rechtlichen Pflichten ihrer Kammer-Mitglieder zuständig ist.

Anders ist es beim Fehlen solcher enger bereichsspezifischer Regelungen wie z. B.

- bei einer Auslagerung der Personalverwaltung an eine Schwester- oder die Muttergesellschaft eines Unternehmens oder
- bei der gesamten Auslagerung des Einzugs rückständiger Forderungen an ein Inkassounternehmen.

Hier sind detailliertere Regelungen notwendig, die sich auch an den gesetzlichen Vorgaben von § 11 Abs. 2 Satz 2 BDSG orientieren können.

Als Beispiel kann dazu auch auf den Art. 22 Abs. 4 der mit den Datenschutzaufsichtsbehörden abgestimmten Verhaltensregeln in der Versicherungswirtschaft verwiesen werden.

> > >
http://www.gdv.de/wp-content/uploads/2013/03/GDV_Code-of-Conduct_Datenschutz_2012.pdf

6

Rund um den datenschutzrechtlichen Auskunftsanspruch

6 Rund um den datenschutzrechtlichen Auskunftsanspruch

Beschwerden Betroffener im Zusammenhang mit der Erteilung oder Nichterteilung datenschutzrechtlicher Auskunft nehmen bei uns einen Spitzenplatz ein. In der Praxis gibt es sowohl bei Betroffenen als auch bei den verantwortlichen Stellen immer wieder unzutreffende Vorstellungen darüber, was eigentlich mit Hilfe des datenschutzrechtlichen Auskunftsanspruchs durchgesetzt werden kann und wie weit der Anspruch im Einzelnen reicht. Nachfolgend soll anhand der bei uns eingegangenen Beschwerden zu diesem Themenkomplex auf einige der häufigsten Fehlvorstellungen kurz eingegangen werden.

6.1 Gegenstand des Auskunftsanspruchs: personenbezogene Daten, nicht jedoch Datenträger

Der datenschutzrechtliche Auskunftsanspruch richtet sich auf die Nennung der personenbezogenen Daten, nicht auf die Vorlage oder Herausgabe von Unterlagen, in denen die Daten enthalten sind.

Häufig wandten sich Beschwerdeführer mit der Bitte um Unterstützung an uns, die von einer „verantwortlichen Stelle" (z. B. Unternehmen) nicht lediglich Auskunft über die dort zu ihrer Person gespeicherten Daten erhalten, sondern die Vorlage oder Herausgabe der Unterlagen oder sonstiger Datenträger erwirken wollten, in denen jene Daten enthalten waren. Die Vorlage oder Herausgabe kann jedoch im Wege des datenschutzrechtlichen Auskunftsanspruchs nicht durchgesetzt werden. Denn der Auskunftsanspruch gemäß § 34 BDSG (ggf. in Verbindung mit § 12 Abs. 7 TMG) richtet sich nur auf die Nennung der personenbezogenen Daten, nicht jedoch auf die Vorlage der Unterlagen, Dokumente, Dateien bzw. Datei-Ausdrucke oder sonstiger „Datenträger", in denen diese Daten enthalten sind.

Gemäß § 34 Abs. 1 BDSG kann ein Betroffener Auskunft verlangen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
2. Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und
3. den Zweck der Speicherung.

Die Auskunft ist in aller Regel in Textform zu erteilen (§ 34 Abs. 6 BDSG). Der datenschutzrechtliche Auskunftsanspruch ist somit (nur) auf die Nennung von Daten – in der Regel in Textform – gerichtet, nicht hingegen auf Vorlage oder Herausgabe von Unterlagen oder sonstiger Datenträger. Ein Anspruch auf Vorlage oder Herausgabe von Datenträgern, d. h. von Gegenständen, könnte sich ggf. nur (je nach Fall) aus zivilrechtlichen oder sonstigen Vorschriften außerhalb des Datenschutzrechts ergeben; dies zu beurteilen liegt jedoch außerhalb der Zuständigkeit der Datenschutzaufsichtsbehörde. Die Durchsetzung solcher Ansprüche wäre daher ggf. unter Inanspruchnahme der Gerichte im einschlägigen (z. B. zivilrechtlichen) Rechtsweg zu versuchen. Da es sich hierbei nicht um datenschutzrechtliche Ansprüche handelt, kann die Datenschutzaufsichtsbehörde Betroffene bei der Geltendmachung solcher Vorlage-/Herausgabeansprüche nicht unterstützen.

6.2 Anspruch auf wörtliche Wiedergabe

Die auskunftspflichtige Stelle muss dem Betroffenen seine Daten grundsätzlich im Wortlaut („Klartext") nennen.

Eingabeführer wünschten im Rahmen des datenschutzrechtlichen Auskunftsanspruchs häufig die Mitteilung interner Aufzeichnungen „im Wortlaut". Unstreitig ist, dass der Betroffene Anspruch auf Nennung seiner bei der „verantwortlichen Stelle" gespeicherten personenbezogenen Daten im Klartext – somit letztlich im Wortlaut – hat. Die Nennung der bloßen Da-

tenkategorien genügt nicht, denn das Auskunftsrecht nach § 34 BDSG soll den Betroffenen in die Lage versetzen, einen Überblick über die bei der „verantwortlichen Stelle" zu seiner Person gespeicherten Informationen zu erhalten und ggf. etwaige Änderungs-, Sperrungs- oder Löschverlangen nach § 35 BDSG geltend zu machen. Dies ist nur möglich, wenn dem Betroffenen die Daten im Klartext mitgeteilt werden, z. B. die konkrete gespeicherte Telefonnummer oder Adresse genannt wird anstelle der bloßen Angabe „Wir speichern Ihre Adresse" bzw. „Wir speichern Ihre Telefonnummer". Leider war in der Praxis immer wieder festzustellen, dass Unternehmen zunächst den Betroffenen nur die Datenkategorien und erst auf unsere Hinweise hin Klartext-Daten mitteilten.

6.3 Auskunftsanspruch nur hinsichtlich personenbezogener Daten

Enthält ein Dokument oder eine Datei gewisse „personenbezogene Daten" im rechtlichen Sinn, bedeutet dies nicht zwingend, dass das gesamte Dokument bzw. die gesamte Datei aus „personenbezogenen Daten" des Betroffenen besteht.

Schwierigkeiten bereitete immer wieder die Frage, was eigentlich im Rahmen der datenschutzrechtlichen Auskunft dem Betroffenen mitgeteilt werden muss. Unternehmen und anderen verantwortlichen Stellen ist häufig nicht klar, welche bei ihnen gespeicherten Informationen – im datenschutzrechtlichen Sinne – personenbezogene Daten (zu dem im konkreten Fall jeweiligen Betroffenen) darstellen und daher dem Auskunftsanspruch unterfallen. Betroffene wiederum überschätzen offenbar manchmal den Umfang ihres Auskunftsanspruchs und sind dann bisweilen unzufrieden, wenn Unternehmen im Wege der Auskunft bestimmte Dateien oder Dokumenten nicht komplett, sondern nur in Teilen wiedergeben. Häufig verlangten Betroffene z. B. die Wiedergabe „aller Aufzeichnungen", „aller Informationen" (o. ä.), die bei einem Unternehmen z. B. „zum Kundenkonto" des jeweiligen Betroffenen vorhanden sind. Im Berichtszeitraum beschwerten sich Betroffene bei uns in solchen Fällen häufig mit dem Argument, das Unternehmen habe z. B. nicht den kompletten Inhalt eines Kundenkontos oder nicht alle dort vorliegenden Dokumente aus der Korrespondenz mit dem Betroffenen vollständig zitiert.

Wie weit der Anspruch gemäß § 34 BDSG reicht, muss indessen strikt danach beurteilt werden, ob es sich bei der einzelnen gespeicherten Information um ein personenbezogenes Datum des jeweiligen Betroffenen im gesetzlichen Sinne handelt, d. h. um eine „Einzelangabe über persönliche oder sachliche Verhältnisse" dieser Person (§ 3 Abs. 1 BDSG). Dies ist nicht automatisch bei allen Einzelinformationen und Aufzeichnungen der Fall, die z. B. in einem bestimmten Kundenkonto o. ä. gespeichert oder einem solchen Kundenkonto zugeordnet sind. Denn nicht ein Kundenkonto, eine Datei oder ein Dokument als solches, d. h. in seiner Gesamtheit, stellt ein personenbezogenes Datum im rechtlichen Sinn dar. Vielmehr ist die Frage, ob es sich um ein personenbezogenes Datum handelt, für jede in dem betreffenden Kundenkonto bzw. in der betreffenden Datei oder dem jeweiligen Dokument enthaltene Einzelinformation („Einzelangabe" im Sinne von § 3 Abs. 1 BDSG) jeweils gesondert zu beurteilen. Dass ein Dokument – etwa ein Vertrag, eine Gesprächsnotiz, ein Protokoll, eine Datei usw. – einige Angaben enthält, die unter Zugrundelegung der Definition des Begriffs des „personenbezogenen Datums" (s. o.) als personenbezogene Daten einer bestimmten Person einzustufen sind, bedeutet noch nicht, dass der gesamte Inhalt jenes Dokuments aus personenbezogenen Daten im rechtlichen Sinne bestünde. Es gibt durchaus Inhalte, die keinen Informationsgehalt zu einer bestimmten oder bestimmbaren natürlichen Person haben und die deshalb nicht unter den gesetzlichen Begriff des personenbezogenen Datums fallen: So sagen etwa technische Beschreibungen eines Gegenstandes grundsätzlich lediglich etwas über den Gegenstand als solchen aus, nicht jedoch auch über eine Person (etwa den Eigentümer des Gegenstands), und sind daher für sich gesehen keine „personenbezogenen" Daten. Inhalte, die z. B. lediglich interne Arbeitsprozesse oder Verwaltungsvorgänge der

verantwortlichen Stelle beschreiben, stellen für sich gesehen ebenfalls keine Einzelangaben „über eine natürliche Person" im Sinne des Begriffs des personenbezogenen Datums (§ 3 Abs. 1 BDSG) dar.

Bei der Bearbeitung bei uns eingegangener Beschwerden haben wir den Beschwerdeführern in solchen Fällen daher erläutert, dass der datenschutzrechtliche Auskunftsanspruch auf „personenbezogene Daten" im gesetzlichen Sinne beschränkt ist, und haben versucht, die Reichweite des Anspruchs im konkreten Fall zu erläutern.

Wie weit im konkreten Einzelfall Dokumenten- und Dateiinhalte „personenbezogene Daten" des Auskunftbegehrenden darstellen, kann somit nur unter strikter Anwendung der gesetzlichen Definition des Begriffs der „personenbezogenen Daten" auf die jeweilige Angabe entschieden werden. Die auskunftspflichtige verantwortliche Stelle muss daher prüfen, welche bei ihr gespeicherten Informationen Einzelangaben über den jeweiligen Betroffenen darstellen. Hat die verantwortliche Stelle erst einmal die Angaben „herausdestilliert", die als personenbezogene Daten des Auskunftsersuchenden anzusehen sind, muss sie diese Angaben dem Auskunftsersuchenden allerdings dann grundsätzlich im Wortlaut mitteilen (siehe dazu Kapitel 6.2).

6.4 Auskunftsanspruch hinsichtlich Standorten von Auftragsdatenverarbeitern

Setzt ein Unternehmen, z. B. durch Inanspruchnahme von Cloud-Computing-Diensten, Auftragsdatenverarbeiter in Staaten außerhalb der Europäischen Union ein, muss es Betroffene hierüber im Rahmen der Auskunft informieren.

Bei unserer beratenden Tätigkeit im Berichtszeitraum sind wir immer wieder Fällen begegnet, bei denen Unternehmen uns mitteilten, im Zuge der Einschaltung von Auftragsdatenverarbeitern personenbezogene Daten auch an Auftragsdatenverarbeiter in Staaten außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums (EWR) zu transferieren. Häufiger Fall ist die Inanspruchnahme von Cloud-Computing-Dienstleistungen, aber auch schon das bloße Hosting personenbezogener Daten bei einem Dienstleister in einem Drittstaat zählt dazu. Gleiches gilt auch für Zugriffe auf personenbezogene Daten, die physisch in der EU bzw. im EWR gespeichert sind, durch Dienstleister aus Drittstaaten zu „Support"-Zwecken oder im Rahmen sonstiger Maßnahmen der Prüfung und Wartung von Datenverarbeitungsanlagen (vgl. § 11 Abs. 5 BDSG). In solchen Fällen haben wir die Unternehmen darauf hingewiesen, dass sie im Falle der Beantwortung datenschutzrechtlicher Auskunftsersuchen die Betroffenen auch über den Umstand informieren müssen, dass ihre Daten auch an Dienstleister gegeben werden, die außerhalb der Europäischen Union ansässig sind. Denn gemäß § 34 Abs. 1 Nr. 2 BDSG muss die verantwortliche Stelle Betroffenen im Rahmen der Auskunft auch die „Kategorien von Empfängern" nennen, an die ihre Daten weitergegeben werden. Als „Empfänger" sind hierbei nach weitgehend unstreitiger und auch unserer Auffassung auch Auftragsdatenverarbeiter anzusehen.

Wenn ein Unternehmen Auftragsdatenverarbeiter außerhalb der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraums (EWR) einschaltet, muss es daher diesen Umstand im Rahmen der datenschutzrechtlichen Auskunft mitteilen, da derartige Datenempfänger als eine spezifische „Kategorie von Empfängern" im Sinne von § 34 Abs. 1 Nr. 2 BDSG anzusehen sind. Denn Staaten außerhalb der EU und des EWR besitzen – bis auf wenige durch die Europäische Kommission anerkannte Ausnahmefälle – kein Datenschutzniveau, das demjenigen der EU-/EWR-Staaten vergleichbar wäre. Für die Betroffenen, deren Daten an solche Auftragsverarbeiter transferiert werden, ist dies im Rahmen der datenschutzrechtlichen Auskunft daher transparent zu machen, da es sich hierbei um einen Umstand handelt, die für die Beurteilung der Datenverarbeitung aus Sicht der Betroffenen potentiell von Interesse ist.

Aus diesem Grund muss im Übrigen die verantwortliche Stelle den Betroffenen diesen

Umstand auch bereits bei der Datenerhebung im Zuge der Information nach § 4 Abs. 3 Nr. 3 BDSG mitteilen. Im Rahmen unserer beratenden Tätigkeit haben wir bei Unternehmen, die sich Auftragsdatenverarbeitern in Drittstaaten bedienten, festgestellt, dass auch diese Information – etwa in „Datenschutzerklärungen" auf Unternehmenswebsites – nicht immer gegeben wird; in solchen Fällen haben wir für entsprechende Nachbesserung gesorgt.

6.5 Auskunftsanspruch über Dienstleister als Empfänger von Daten

Anlass zu einer weiteren Beschwerde gab die nicht vollständig erteilte Auskunft einer Versicherung gemäß § 34 Abs. 1 BDSG über die Empfänger personenbezogener Daten im Zusammenhang mit der Einstellung von Daten in eine Kfz-Restwertbörse.

Das Versicherungsunternehmen vertrat die Auffassung, dass ein Hinweis auf die von der Versicherung im Internet veröffentlichte Dienstleisterliste an den Betroffenen genüge, um ein Auskunftsersuchen nach § 34 BDSG zu erfüllen, das sich ausdrücklich auch auf die Empfänger der Daten bezog. Dieser Hinweis war jedoch schon deshalb nicht ausreichend, weil die Dienstleisterliste in dem konkreten Fall lediglich die Stellen enthielt, mit denen die Versicherung unter Verwendung von Gesundheitsdaten und weiterer nach § 203 StGB geschützter Daten zusammenarbeitet. Eine Online-Restwertbörse aus dem Bereich Kfz-Versicherung, an die die Daten im Rahmen einer Auftragsdatenverarbeitung weitergegeben worden waren (siehe dazu auch Kapitel 9.2), war in dieser Liste jedoch nicht enthalten.

6.6 Kein Anspruch einer bewerteten Person gegenüber dem Betreiber einer Internet-Bewertungsplattform auf Auskunft über die Person des Bewertenden

Wird eine Person auf einer Bewertungsplattform (z. B. für Ärzte) bewertet und möchte diese vom Plattformbetreiber Auskunft über die Identität des Bewertenden, ist keine Rechtsgrundlage ersichtlich, die den Plattformbetreiber ermächtigen würde, ohne eine entsprechende Einwilligung des bewertenden Nutzers die gewünschten Auskünfte zu erteilen.

Die Rechtsprechung hat in jüngerer Vergangenheit in Bezug auf Internetportale zur Bewertung von Ärzten mehrfach festgestellt, dass derartige Bewertungsportale aus datenschutzrechtlicher Sicht nicht grundsätzlich unzulässig sind (siehe dazu Kapitel 7.5).

Fühlt sich eine Person durch eine im Portal veröffentlichte Bewertung in ihrem Persönlichkeitsrecht verletzt, besteht häufig das zunächst aus ihrer Sicht nachvollziehbare Interesse, die Identität des Bewertenden in Erfahrung zu bringen. Da den veröffentlichten Bewertungen in diesen Portalen regelmäßig keine personenbezogenen Daten zum Autor einer Bewertung zu entnehmen sind, werden die gewünschten Auskünfte oft von den Plattformbetreibern gefordert. Letztere weigern sich in der Regel, die entsprechende Auskunft zu erteilen. Aus diesem Grund erreichten uns im Berichtszeitraum zahlreiche Anfragen und Beschwerden bewerteter Personen, die die Identität des Bewertenden erfahren wollten. Begründet wurde dies meist damit, dass sich der Bewertete dann direkt an die bewertende Person wenden könne bzw. diese Informationen für die Führung eines Rechtsstreits hilfreich wären. Eine Rechtsgrundlage für einen solchen Anspruch auf Auskunft über die Person des Bewertenden ist jedoch nach dem einschlägigen Telemediengesetz nicht vorhanden.

Dies hat der Bundesgerichtshof (BGH) nunmehr in seinen Entscheidungen vom 01.07.2014 (Az.: VI ZR 345/13) und 23.09.2014 (Az.: VI ZR 358/13) zum Auskunftsanspruch gegen ein Arztbewertungsportal festgestellt. Der BGH vertritt darin die Auffassung, dass die fehlende Möglichkeit des Arztes, sich mit dem Bewertenden direkt auseinanderzusetzen, angesichts der dem Internet immanenten Möglichkeit zur anonymen Nutzung hinzunehmen ist. In Ermangelung einer gesetzlichen Ermächtigungsgrundlage im Sinne des § 12 Abs. 2 TMG ist der Betreiber eines Internetportals grundsätzlich nicht befugt, ohne Einwilligung des Nutzers dessen personenbezogene Daten im Rahmen eines wegen einer behaupteten Persönlichkeitsrechtsverletzung geltend gemachten Auskunftsanspruchs an den bewerteten Arzt zu übermitteln.

Der Bundesgerichtshof führt hierzu in seiner Entscheidung vom 01.07.2014 Folgendes aus:

„Offen bleiben kann, ob § 13 Abs. 6 Satz 1 TMG, wonach ein Diensteanbieter die Nutzung von Telemedien anonym oder unter Pseudonym zu ermöglichen hat, soweit dies technisch möglich und zumutbar ist, einer Auskunftserteilung über Nutzerdaten entgegensteht. (…) Die vom Kläger begehrte Auskunftserteilung scheitert jedenfalls daran, dass die Beklagte gemäß § 12 Abs. 2 TMG nicht zur Herausgabe der zur Bereitstellung des Telemediums erhobenen Anmeldedaten befugt ist. (…) Nach dem Gebot der engen Zweckbindung des § 12 Abs. 2 TMG dürfen für die Bereitstellung von Telemedien erhobene personenbezogene Daten für andere Zwecke nur verwendet werden, soweit eine Rechtsvorschrift dies erlaubt oder der Nutzer – was hier nicht in Rede steht – eingewilligt hat. (…) Eine Erlaubnis durch Rechtsvorschrift kommt außerhalb des Telemediengesetzes nach dem Gesetzeswortlaut lediglich dann in Betracht, wenn sich eine solche Vorschrift ausdrücklich auf Telemedien bezieht. (…) Der aus Treu und Glauben (§ 242 BGB) hergeleitete allgemeine Auskunftsanspruch beinhaltet keine Erlaubnis im Sinne des § 12 Abs. 2 TMG, die sich ausdrücklich auf Telemedien bezieht. (…) Eine Ermächtigung zur Erteilung der begehrten Auskunft ergibt sich auch nicht aus § 14 Abs. 2 TMG. Nach dieser Bestimmung, die nach § 15 Abs. 5 Satz 4 TMG auf Nutzungs- und Abrechnungsdaten entsprechend anwendbar ist, darf zwar der Diensteanbieter auf Anordnung der zuständigen Stellen im Einzelfall Auskunft über Bestandsdaten erteilen, soweit dies für Zwecke der Strafverfolgung, zur Gefahrenabwehr durch die Polizeibehörden der Länder, zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes oder des Bundeskriminalamtes im Rahmen seiner Aufgabe zur Abwehr von Gefahren des internationalen Terrorismus oder zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist. Eine Ermächtigung zur Auskunftserteilung zu Zwecken des Schutzes von Persönlichkeitsrechten ist darin (…) nicht enthalten."

Damit ist der Betreiber einer Bewertungsplattform im Internet mangels einer gesetzlichen Ermächtigungsgrundlage grundsätzlich nicht befugt, ohne Einwilligung des Bewertenden dessen personenbezogene Daten an eine bewertete Person zu übermitteln, die einen Auskunftsanspruch wegen einer Persönlichkeitsrechtsverletzung an ihn herangetragen hat.

7

Datenschutz im Internet

7 Datenschutz im Internet

7.1 „Google"-Urteil des EuGH

Mit Urteil vom 13. Mai 2014 (C-131/12) entschied der Europäische Gerichtshof (EuGH) in einem Vorabentscheidungsverfahren, dass der Suchmaschinenbetreiber „Google" als verantwortliche Stelle Suchergebnisse aus den Ergebnislisten entfernen muss, soweit das berechtigte Interesse der betroffenen Person das Interesse des Suchmaschinenbetreibers und der Öffentlichkeit überwiegt.

Auch wenn sich das EuGH-Urteil speziell auf den Suchmaschinenbetreiber „Google" bezieht, sind die Aussagen des Urteils auch auf die sonstigen Suchmaschinenbetreiber innerhalb und außerhalb der Europäischen Union (EU), wie z. B. Microsoft („Bing") und Yahoo!, anwendbar. Da diese beiden Suchmaschinenbetreiber Niederlassungen in Bayern führen, sind wir für Anfragen und Eingaben zu diesen zuständig. Entgegen der Erwartungen erreichten uns seit dem EuGH-Urteil lediglich eine sehr geringe Anzahl an Anfragen und Eingaben, welche mit wachsendem zeitlichem Abstand zu der Verkündung des Urteils kontinuierlich zurückgingen.

Konkret ging es in dem Verfahren um einen spanischen Bürger, der sich unter anderem über Google Spain und Google Inc. beschwerte, da bei Eingabe seines Namens in der Suchmaschine „Google" Links zu zwei Seiten einer spanischen Tageszeitung aus dem Jahr 1998 aufgefunden werden konnten, die auf eine Anzeige zu einer Versteigerung eines Grundstücks aufgrund einer Pfändung hinwiesen. Die Spanische Aufsichtsbehörde gab der Beschwerde gegen die Google Inc. statt. Hiergegen klagte die Google Inc. vor dem spanischen Gericht, das wiederum dem EuGH einige Fragen zur Vorabentscheidung vorlegte.

Der EuGH entschied, dass es sich bei dem Suchmaschinenbetreiber Google Inc. um eine datenschutzrechtlich verantwortliche Stelle handelt, die personenbezogene Daten verarbeitet. Auch wenn sich der Sitz der Google Inc. in den USA, d. h. außerhalb der EU, befindet, wurde der Anwendungsbereich des jeweils in den Mitgliedstaaten geltenden nationalen Datenschutzrechts – hier des spanischen Datenschutzrechts – als eröffnet angesehen, da eine Datenverarbeitung im Rahmen der Tätigkeiten einer Niederlassung, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet eines Mitgliedstaats besitzt, ausgeführt wird. Eine solche Datenverarbeitung wurde angenommen, da der Suchmaschinenbetreiber die Niederlassung Google Spain in dem Mitgliedstaat Spanien für die Förderung des Verkaufs der Werbeflächen der Suchmaschine und des Verkaufs selbst unterhält und aufgrund der gleichzeitigen Aufblendung von Suchergebnissen und damit verbundenen Werbeanzeigen eine Verarbeitung im Rahmen der Werbetätigkeit der Google Spain erfolgt.

Auf der Basis der dargestellten Bewertungen führte der EuGH weiter aus, dass der Suchmaschinenbetreiber verpflichtet ist, Suchergebnisse, die anhand des Namens einer Person aufgezeigt werden, zu entfernen, soweit das Interesse der betroffenen Person das Interesse der Öffentlichkeit und des Suchmaschinenbetreibers überwiegt. Als Orientierung für die Durchführung der Interessenabwägung hat die Artikel 29 Gruppe inzwischen Richtlinien und einen Kriterienkatalog entwickelt (WP 225 – Guidelines on the implementation of the Court of Justice of the European Union Judgment on „Google Spain and Inc v. Agencia Espanola de Proteccion de datos (AEPD) and Mario Costeja González" C-131/12).

Die Entfernung von Ergebnissen aus der Ergebnisliste einer Suchmaschine bedeutet jedoch nicht, dass der zugrunde liegende Artikel gelöscht wird. Vielmehr ist dieser nach der Entfernung des entsprechenden Links nicht mehr anhand einer Namenssuche über die Suchmaschine auffindbar; allerdings kann der Artikel bei Eingabe sonstiger passender Suchbegriffe weiterhin aufgefunden werden. Dies wird auch ausdrücklich von der 88. Datenschutzkonferenz in ihrer Entschließung „Zum

Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen“ vom 8./9. Oktober 2014 dargestellt.

Betroffene Personen, die eine Entfernung von unter ihrem Namen auffindbaren Links begehren, müssen sich zunächst an den jeweiligen Suchmaschinenbetreiber wenden. Zu diesem Zweck stellen einige Suchmaschinenbetreiber Online-Formulare zur Verfügung:

Google:
https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=de

Microsoft (Suchmaschine “Bing”):
https://www.bing.com/webmaster/tools/eu-privacy-request

Yahoo!:
https://de.hilfe.yahoo.com/kb/search/SLN24378.html?impressions=true

Wird der Antrag auf Entfernung eines Links abgelehnt, ist es dem Betroffenen möglich, sich bei der jeweils zuständigen Datenschutzaufsichtsbehörde zu beschweren. Während wir in Deutschland für Microsoft und Yahoo! zuständig sind, liegt die Zuständigkeit für Google bei dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit.

7.2 International Sweep Day

In den Jahren 2013 und 2014 nahmen wir an dem durch das Global Privacy Network angeregten International Sweep Day teil. Hierbei stellten wir einen erheblichen Mangel an Transparenz bei den überprüften Online-Angeboten fest.

Seit 2013 lädt das Global Privacy Network (GPEN) jährlich weltweit Aufsichtsbehörden dazu ein, sich am International Sweep Day zu beteiligen. Hierbei sollen Online-Angebote im Rahmen einer koordinierten Prüfung hinsichtlich vorab konkret festgelegter internationaler Prüfkriterien überprüft werden. Ziel ist es, zunächst einen Überblick über die jeweiligen Angebote zu erhalten, eine Vergleichbarkeit herzustellen und insbesondere datenschutzrechtliche Mängel festzustellen. Nach Durchführung des „Sweeps“ ist es den Aufsichtsbehörden freigestellt, weitergehende Prüfungen auf Basis des jeweils nationalen Rechts durchzuführen.

In beiden Prüfaktionen des Berichtszeitraumes haben wir uns mobile Applikationen angesehen und diese hinsichtlich der Transparenz überprüft. Hierzu wurden die Apps im App-Store aufgerufen, installiert und gestartet. In jedem dieser Schritte wurde die Transparenz der Datenumgänge überprüft (Prüfung „durch Sichtung“).

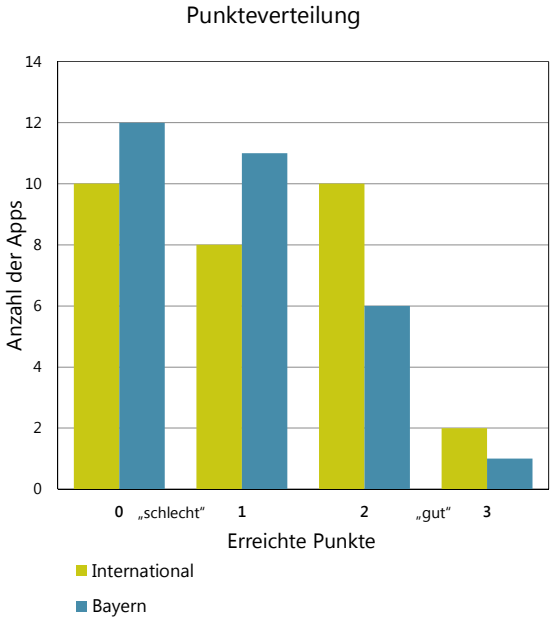
2013 nahmen wir uns die Prüfung von 30 zufällig ausgewählten bayerischen Android- und iOS- Apps vor und mussten feststellen, dass lediglich ca. 25 % der geprüften Apps über eine App-spezifische Datenschutzerklärung verfügten.

Aber auch im Jahr 2014 fanden wir heraus, dass bei der Prüfung von 60 zufällig ausgewählten Android- und iOS-Apps bei einer vorgegebenen Benotungsskala von 0 bis 3 (0 als schlechteste Wertung) lediglich ein Durchschnittsergebnis von 0,98 erreicht werden konnte.

Im Gegensatz zum Vorjahr hatten wir dabei jedoch nicht nur bayerische, sondern auch internationale Apps (jeweils 30) geprüft, um auch die Umsetzung der Transparenzanforderungen außerhalb Bayerns zu erfahren. Allerdings rührte das negative Ergebnis von 0,98 nicht allein von der Intransparenz der internationalen Apps her. Zu unserem Erstaunen schnitten gerade die bayerischen iOS-Apps mit der Durchschnittsnote 0,5 am schlechtesten ab. Die internationalen iOS-Apps konnten zumindest einen Durchschnittswert von 1,2 erreichen.

Ebenfalls die Note 1,2 konnten die bayerischen Android-Apps erreichen, während die internationalen Android-Apps mit der Note 1,1 bewertet wurden (Notenübersicht getrennt nach Android/iOS siehe Kapitel 3.4.6).

Der Punktevergleich zwischen internationalen und bayerischen Apps ist der nachfolgenden Grafik zu entnehmen:



Im Anschluss an den „Sweep“ wurden die bayerischen Apps wiederum im aufsichtlichen Verfahren nach deutschem Datenschutzrecht geprüft. Durch die beiden „Sweeps“ konnten wir innerhalb kurzer Zeit eine große Anzahl von Apps sichten und so eine Vergleichbarkeit herstellen, um konkrete Mängel in der Transparenz erkennen zu können. Dies führte dazu, dass wir Hinweise zu den Anforderungen an Datenschutzerklärungen für bayerische App-Anbieter veröffentlichten und dieser Thematik auch in unserer 2014 erstellten umfangreichen Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter ein besonderes Gewicht beimaßen.

Diese Orientierungshilfe und andere umfassende Informationen zum Thema „Mobile Applikationen“ befinden sich auf unserer Webseite.

> > >
http://www.lda.bayern.de/MobileApplikationen/index.html

7.3 Prüfung des Einsatzes von Adobe Analytics im Internetauftritt bayerischer Unternehmen

Bereits bei der Durchführung der Google-Analytics-Prüfung im vergangenen Berichtszeitraum (vgl. 5. Tätigkeitsbericht 2011/2012, Kapitel 4.1.3) hatten wir angekündigt, den Einsatz eines weiteren Verfahrens zur Reichweitenmessung von Webseiten im Rahmen einer weiteren Online-Prüfung zu prüfen. Im Berichtszeitraum haben wir deshalb das Verfahren zur Reichweitenmessung von Adobe „Adobe Analytics“ (ehemals Omniture SiteCatalyst) geprüft.

Auf Grundlage des Beschlusses des Düsseldorfer Kreises vom 26./27.11.2009 über die beanstandungsfreie Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internetangeboten haben wir uns mit der Firma Adobe darüber verständigt, wie das Produkt Adobe Analytics angepasst werden muss, damit es die bayerischen Webseitenbetreiber beanstandungsfrei einsetzen können. Nach dieser Verständigung überprüften wir 10.238 zufällig ausgewählte Webseiten daraufhin, ob das Analysetool eingesetzt wurde. Diejenigen Webseitenbetreiber, welche Adobe Analytics einsetzten, wurden von uns mit einem Fragebogen angeschrieben.
Mit Hilfe des Fragebogens wurde

- der Abschluss des Vertrages zur Auftragsdatenverarbeitung,
- das Vorhandensein einer angepassten, den Einsatz von Adobe Analytics darstellenden Datenschutzerklärung,
- das Vorhandensein einer wirksamen Widerspruchsmöglichkeit gegen das Setzen von Tracking-Cookies von Adobe,
- die Begrenzung der Cookie-Laufzeit auf maximal 24 Monate,
- das vollständige Ersetzen der IP-Adresse durch eine generische IP-

Adresse durch Vornahme der Einstellung Obfuscate IP –Removed und

- die vollständige Anonymisierung der IP-Adressen vor deren systematischer Verarbeitung (z. B. Geolokalisierung) durch Vornahme der Einstellung: „Before Geo-Lookup: Replace visitor's last IP octet with 0"

abgefragt.

Besonderes Augenmerk hatten wir dabei auf die zweifache Einstellung zur Anonymisierung der IP-Adresse gelegt. Diese ist bei dem Einsatz von Adobe Analytics im Gegensatz zu sonstigen Analyseverfahren notwendig, da zunächst eine Geolokalisierung stattfindet. Das Ergebnis dieser Geolokalisierung wiederum wird zur statistischen Auswertung an das Tracking-Paket, das zunächst die vollständige IP-Adresse enthält, hinzugefügt. Da in beiden Fällen eine Verwendung (Geolokalisierung, Auswertung) der (vollständigen) IP-Adresse vorläge, für welche keine Rechtsgrundlage ersichtlich ist, bedarf es jeweils einer wirksamen Anonymisierung.

Sofern nach Auswertung der eingegangenen Antworten Nachbesserungen erforderlich waren, wurden diese im Rahmen aufsichtlicher Verfahren durchgeführt und dadurch ein beanstandungsfreier Einsatz von Adobe Analytics herbeigeführt.

7.4 Privatfahndung in sozialen Netzwerken

Großes Presseecho erfuhren wir, als wir einem Juwelier von der Veröffentlichung von Aufnahmen seiner Videoüberwachung, welche die Täter eines Raubüberfalls zeigten, abrieten und ihm stattdessen das Setzen eines Links auf die Polizei-Homepage, auf welcher ebenfalls Bilder der Täter veröffentlicht waren, empfahlen. Eine Privatfahndung mittels eines sozialen Netzwerks ist unserer Ansicht nach datenschutzrechtlich nicht ohne Weiteres zulässig.

Im Rahmen einer Presseanfrage wurden wir auf einen Juwelier aufmerksam, der Opfer eines Raubüberfalls geworden war und Bilder und Ausschnitte von Aufnahmen seiner Videoüberwachungsanlage, auf welcher die Täter zu erkennen waren, zu Fahndungszwecken auf seine Facebook-Fanpage gestellt hat. Zeitgleich hatte bereits die Polizei eine Öffentlichkeitsfahndung angestoßen und Fotos und Videos der Täter, die ebenfalls aus der Videoüberwachung des Juweliers stammten, auf ihrer Homepage veröffentlicht. Die Veröffentlichung des Bildmaterials durch den Juwelier sahen wir als nicht ohne Weiteres zulässig an und bewerteten diese als Grenzfall. Auf unser Anraten hin entfernte der Juwelier die Bildaufnahmen von seiner Facebook-Fanpage und verwies stattdessen von seiner Fanpage mittels eines Links auf die Homepage der Polizei, auf der die Fotos der Täter veröffentlicht waren. Anzumerken ist, dass wir – anders als in der Presse zum Teil dargestellt –, zu keinem Zeitpunkt eine datenschutzaufsichtliche Anordnung angedroht oder erlassen haben.

Speziell für die Veröffentlichung von Bildnissen stellt das Kunsturhebergesetz (KUG) strenge Anforderungen. Regelmäßig ist eine Einwilligung der abgebildeten Personen erforderlich. Nur wenn eine der in § 23 Abs. 1 KUG abschließend aufgezählten Ausnahmen gegeben und ein berechtigtes Interesse des Abgebildeten nicht verletzt ist, ist eine Einwilligung der abgebildeten Person nicht erforderlich. Darüber hinaus gibt das KUG in § 24 die zentralen Maßstäbe vor, die die Veröffentlichung von Bildern zu Zwecken der Rechtspflege und der öffentlichen Sicherheit regeln. Diese Vorschrift bietet aber ausdrücklich nur eine Rechtsgrundlage für Behörden und nicht für Privatpersonen. Das bedeutet jedoch nicht, dass es Behörden erlaubt ist, Fahndungsbilder in sozialen Netzwerken zu veröffentlichen. Vielmehr hat der für die bayerische Polizei zuständige Bayerische Landesbeauftragte für den Datenschutz bereits seit längerem Handlungshinweise bereitgestellt, die von der Rechtswidrigkeit der Nutzung von Facebook durch öffentliche Stellen ausgehen. Liegen die Voraussetzungen für eine Öffentlichkeitsfahndung vor, dürfen auch Strafverfolgungsbehörden Abbildungen von Verdächtigen oder Tätern im Internet nur auf Sei-

ten von Anbietern veröffentlichen, die die Vorgaben des deutschen Datenschutzrechts beachten.

Bedenken hatten wir insbesondere aufgrund zahlreicher ungeklärter Rechtsfragen im Zusammenhang mit der Datenverarbeitung durch Facebook und vor dem Hintergrund, dass Veröffentlichungen in sozialen Netzwerken häufig eine Eigendynamik entwickeln, die oftmals nicht mehr gesteuert werden kann. Zudem hatte die Polizei unseres Erachtens in Bezug auf die Veröffentlichung der Fotos alles getan, um ihrer Rolle als Strafverfolgungsbehörde gerecht zu werden. Die Verlinkung auf der privaten Facebook-Fanpage zu der Internetveröffentlichung der Polizei erschien uns als datenschutzrechtlich angemessener Weg. Auf diese Weise konnte der Juwelier weiterhin auf den Raubüberfall aufmerksam machen und um Unterstützung bei der Suche nach den Tätern bitten.

7.5 Portale mit Bewertungsmöglichkeit

Neben reinen Bewertungsportalen reichern immer mehr Telefonbücher, Branchenverzeichnisse, Auskunftsdienste, usw. ihre Online-Angebote um eine Bewertungsfunktion an. Hierbei werden mitunter auch Freiberufler oder auch einzelne Gewerbetreibende bewertet. Wir haben einige Diensteanbieter mit einem umfassenden Fragenkatalog angeschrieben, um Beantwortung desselben gebeten, die Antworten anschließend geprüft und auf eine datenschutzkonforme Ausgestaltung hingewirkt.

Im Berichtszeitraum stellten wir fest, dass immer mehr Auskunftsdienste im Internet dazu übergehen, ihr Angebot mit einer Bewertungsfunktion anzureichern, d. h. Nutzer können über solche Dienste nicht mehr nur Name, Anschrift und Telefonnummer beispielsweise eines gesuchten Freiberuflers oder Gewerbetreibenden ausfindig machen, sondern bekommen gleichzeitig noch angezeigt, wie bisherige Kunden deren Tätigkeit beurteilt haben bzw. wird ihnen die Möglichkeit eröffnet, der Allgemeinheit mitzuteilen, wie die eigene Bewertung seiner beruflichen Tätigkeit ausfällt.

Im Rahmen mehrerer Eingaben, aber auch anlasslos waren wir im Berichtszeitraum mit verschiedenen Portalen befasst und haben deren Angebot auf eine datenschutzkonforme Ausgestaltung hin überprüft bzw. diese bei einer entsprechenden Überarbeitung des Internetauftritts begleitet. Hierzu haben wir uns eines umfangreichen Fragenkatalogs bedient, um von Anfang an einen umfassenden Überblick zu erhalten.

Aus datenschutzrechtlicher Sicht ist der Anwendungsbereich des BDSG nur dann eröffnet, wenn sich die Bewertung auf eine bestimmte oder bestimmbare natürliche Person bezieht. Die Vorschriften des BDSG sind daher zwar anwendbar auf die Bewertung einer Einzelperson (z. B. Arzt, Handwerker, Rechtsanwalt), nicht aber beispielsweise auf die Bewertung eines aus mehreren Personen bestehenden Handwerksbetriebs oder Unternehmens.

Messen lassen muss sich die Bewertungsfunktion am Maßstab des § 29 BDSG, in dessen Anwendung eine Abwägung zwischen dem Schutz des Rechts auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz (GG) und dem Recht auf Kommunikationsfreiheit nach Art. 5 Abs. 1 GG stattzufinden hat (siehe auch Kapitel 4.1.4 unseres Tätigkeitsberichts 2009/2010). Der Bundesgerichtshof (BGH) hat in seinem sogenannten „spickmich"-Urteil vom 23. Juni 2009 (Az.: VI ZR 196/08) entschieden, dass Meinungsäußerungen, die die berufliche Tätigkeit einer Lehrerin betreffen,

> *„nur im Falle schwerwiegender Auswirkungen auf das Persönlichkeitsrecht mit negativen Sanktionen verknüpft werden (dürfen), so etwa dann, wenn eine Stigmatisierung, soziale Ausgrenzung oder Prangerwirkung zu besorgen sind."*

Dass Bewertungsportale aus datenschutzrechtlicher Sicht nicht grundsätzlich unzulässig sind, hat der BGH in einem weiterem Urteil vom 23. September 2014 (Az.: VI ZR 358/13) bestätigt,

in dem er den Anspruch eines Arztes auf Löschung seiner Daten aus einem Ärztebewertungsportal abgelehnt hat:

> *„Zwar wird ein Arzt durch seine Aufnahme in ein Bewertungsportal nicht unerheblich belastet. Abgegebene Bewertungen können neben den Auswirkungen für den sozialen und beruflichen Geltungsanspruch des Arztes die Arztwahl behandlungsbedürftiger Personen beeinflussen, so dass er im Falle negativer Bewertungen wirtschaftliche Nachteile zu gewärtigen hat. Auch besteht eine gewisse Gefahr des Missbrauchs des Portals. Auf der anderen Seite war im Rahmen der Abwägung aber zu berücksichtigen, dass das Interesse der Öffentlichkeit an Informationen über ärztliche Leistungen vor dem Hintergrund der freien Arztwahl ganz erheblich ist und das von der Beklagten betriebene Portal dazu beitragen kann, einem Patienten die aus seiner Sicht erforderlichen Informationen zur Verfügung zu stellen. Zudem berühren die für den Betrieb des Portals erhobenen, gespeicherten und übermittelten Daten den Arzt nur in seiner sogenannten „Sozialsphäre", also in einem Bereich, in dem sich die persönliche Entfaltung von vornherein im Kontakt mit anderen Personen vollzieht. Hier muss sich der Einzelne auf die Beobachtung seines Verhaltens durch eine breitere Öffentlichkeit sowie auf Kritik einstellen. Missbrauchsgefahren ist der betroffene Arzt nicht schutzlos ausgeliefert, da er von der Beklagten die Löschung unwahrer Tatsachenbehauptungen sowie beleidigender oder sonst unzulässiger Bewertungen verlangen kann. Dass Bewertungen anonym abgegeben werden können, führt zu keinem anderen Ergebnis. Denn die Möglichkeit zur anonymen Nutzung ist dem Internet immanent"*

(aus der Pressemitteilung des BGH zu dem angesprochenen Urteil)

Wenngleich das Geschäftsmodell einer Bewertungsfunktion im Internet zur beruflichen Tätigkeit von Einzelpersonen nicht von vornherein unzulässig ist, obliegt es dem jeweiligen Diensteanbieter, durch verschiedene Maßnahmen den Schutz bewerteter Personen im gesetzlichen Rahmen zu gewährleisten. Hierzu zählt beispielsweise, dass Nutzer das Alter der jeweiligen Einzelbewertung erkennen können müssen, Einzelbewertungen nur bis zu einem bestimmten Alter in eine veröffentlichte Gesamtbewertung einfließen dürfen, Maßnahmen zur Vermeidung von Missbrauchs- und Manipulationsmöglichkeiten entwickelt werden und ein transparentes Verfahren zum Umgang mit Beschwerden bewerteter Personen zur Verfügung gestellt wird. Bereits im März 2013 haben die Datenschutzaufsichtsbehörden „datenschutzrechtliche Leitlinien mit Mindestanforderungen für die Ausgestaltung und den Betrieb von Arztbewertungsportalen im Internet" veröffentlicht, die neben den bereits zitierten und weiteren unterinstanzlichen Urteilen als Orientierung für einen datenschutzgerechten Umgang mit personenbezogenen Daten im Rahmen eines Bewertungsportals bzw. einer Bewertungsfunktion herangezogen werden können.

In konstruktiven Gesprächen und bereitwilliger Zusammenarbeit verschiedener Betreiber von Auskunftsdiensten mit Bewertungsfunktion konnten im Berichtszeitraum Änderungen in der Verfahrenspraxis und Überarbeitungen der Internetauftritte erreicht werden, die vor allem auch dem Schutz bewerteter Personen dienen. Dazu zählt nicht zuletzt, dass wir darauf geachtet haben, dass diese Diensteanbieter ihrer Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten (§§ 4f, 4g BDSG) und ihrer Meldepflicht aus § 4d Abs. 4 Nr. 1 BDSG nachgekommen sind.

7.6 Keine schematisierten Datenschutzerklärungen im Internet

„Baukasten-" bzw. schematisierte Datenschutzerklärungen verführen Diensteanbieter häufig dazu, unzureichende oder falsche Datenschutzerklärungen zu erstellen und zu veröffentlichen.

Im Rahmen der Überprüfung von Datenschutzerklärungen stellten wir in zahlreichen Fällen fest, dass die in einem Diensteangebot veröffentlichte Datenschutzerklärung nicht über den konkreten Datenumgang bei der Nutzung des

Dienstes informierte. Eine auf den Dienst bezogene Datenschutzerklärung wird jedoch gem. § 13 Abs. 1 TMG gefordert.

Zur Informationspflicht des Diensteanbieters bestimmt § 13 Abs. 1 Satz 1 TMG, dass er den Nutzer

> "*zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten (…) in allgemein verständlicher Form zu unterrichten*"

hat. Für den Fall, dass der Diensteanbieter beabsichtigt, für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung des Diensteangebotes Nutzungsprofile bei Verwendung von Pseudonymen zu erstellen, ist der Nutzer in der Datenschutzerklärung auf sein diesbezügliches Widerspruchsrecht hinzuweisen (§ 15 Abs. 3 TMG). Gemäß § 13 Abs. 1 Satz 2 TMG hat der Diensteanbieter den Nutzer zudem bei

> *„einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, zu Beginn dieses Verfahrens zu unterrichten"*.

Diese Anforderung stellt insbesondere auf den Einsatz von Cookies ab, gilt jedoch allgemein bei dem Einsatz entsprechender Verfahren. Zusätzlich sind die Informationspflichten des § 4 Abs. 3 BDSG zu beachten.

Ergänzend weisen wir darauf hin, dass sich jeder Diensteanbieter nach § 2 Nr. 1 TMG mit der Thematik einer Datenschutzerklärung im Internetauftritt bzw. in der mobilen (Online-) Applikation zu beschäftigen hat, selbst wenn ein Nutzer nicht aktiv Daten eingeben kann und auch keine Cookies o. ä. Verfahren genutzt werden. Dies hängt damit zusammen, dass die Erhebung und Verwendung der IP-Adresse des Nutzers als technische Steuerungsinformation zur Übertragung von Informationen im Internet zwischen Diensteanbieter und Nutzer erforderlich ist. Da die IP-Adresse von den Aufsichtsbehörden als personenbezogenes Datum angesehen wird, ist eine Information hierzu nicht entbehrlich. Daraus ergibt sich, dass eine Datenschutzerklärung zumindest hierzu selbst dann entsprechende Informationen beinhalten muss, wenn ansonsten bei der Nutzung des Internetauftritts oder der mobilen Online-Applikation kein weiterer Umgang mit personenbezogenen Daten ausgelöst wird.

Nach unserer Erkenntnis sind die abstrakten, fehlerhaften und unvollständigen Datenschutzerklärungen häufig darauf zurückzuführen, dass Diensteanbieter (oder deren Dienstleister) die Datenschutzerklärung – entweder aus Unwissenheit oder Sorglosigkeit – vollständig oder zumindest teilweise aus verschiedensten Mustern im Internet kopiert hatten bzw. zum Teil auch online verfügbare Konfiguratoren zur Erstellung von Standard-Datenschutzerklärungen nutzten. Allzu oft werden dabei sicherheitshalber alle Textbausteine angeklickt oder gar die komplette Muster-Datenschutzerklärung übernommen. Dies führt dazu, dass eine Datenschutzerklärung erstellt und veröffentlicht wird, die über Sachverhalte informiert, die auf den konkreten Dienst nicht zutreffen, oder es werden Textbausteine für bestimmte Sachverhalte nicht gefunden, so dass eine Datenschutzerklärung unvollständig bleibt und gerade nicht über den konkreten Datenumgang informiert.

Da gem. § 16 Abs. 2 Nr. 2 TMG eine Ordnungswidrigkeit begeht, wer entgegen § 13 Abs. 1 Satz 1 oder 2 TMG den Nutzer vorsätzlich oder fahrlässig nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig informiert, ist es ratsam, die Datenschutzerklärung mit der entsprechenden Sorgfalt zu gestalten und bei konkreten Fragestellungen Rat bei fachkundigen Stellen oder der Aufsichtsbehörde einzuholen.

Aus den dargestellten Gründen stellen wir kein Muster für eine Datenschutzerklärung zur Verfügung. Unabhängig davon prüfen wir uns vorgelegte Datenschutzerklärungen, soweit uns dies möglich ist.

7.7 Tracking mit fortgeschrittenen Webtechnologien

Die gezielte Verfolgung von Webnutzern ist ohne Hilfe der allgemein bekannten Cookies möglich, jedoch gestaltet sich ein datenschutzkonformer Einsatz häufig recht schwierig.

Nahezu alle größeren Webseiten setzen mittlerweile mehrere Softwareprodukte zum Tracking der eigenen Webseitenbesucher ein. Bei einem technischen Datenschutzblick auf die Funktionalität dieser Verfahren fällt einem zwangsläufig der klassische Cookie ein, der gerne als "kleine Textdatei" beschrieben und von einer Webseite auf dem Rechner des Nutzers abgelegt wird. Diese Cookies werden technisch als sogenannte HTTP-Cookies benannt und sind Bestandteil des Internetprotokolls. Ein Nutzer kann in der Regel in seinem Browser die abgelegten Cookies ansehen, diese nach Bedarf löschen (auch direkt als Einstellung bei Beenden des Browsers) oder sogenannte Drittanbieter-Cookies, die häufig für (Werbe-)Tracking eingesetzt werden, grundsätzlich ablehnen. Ebenso existiert mittlerweile eine Menge von Browsererweiterungen (Addons), die Drittanbieterinhalte und deren Cookies aus Nutzersicht komfortabel blockieren.

Aus Sicht eines Webseiten- oder Trackingbetreibers ist diese Entwicklung, bei der ein Endanwender vermehrt die Kontrolle über die eigenen Datenflüsse behält und zunehmend auch umsetzt, insofern nachteilig, da die Anzahl der zum Tracking geeigneten Browser bzw. Nutzer und damit die Menge der erhobenen Daten spürbar weniger werden. In den letzten Jahren wurden neuartige Verfahren entwickelt bzw. entdeckt, die das Tracking von Webseitenbesuchern ermöglichen, ohne auf die Hilfe von üblichen Cookies zurück zu greifen:

- Nachverfolgung über sogenannte Flash Cookies (Local Shared Objects) – das sind Dateien mit einer Größe von 100 Kilobytes, in die Flash-Anwendungen beliebige Daten (eben auch Tracking-Daten) ablegen können.
- Verwendung von Long-Storage-Objects wie HTML5-Storage, Java- und Silverlight-Persistierungen zur Speicherung von Tracking-Informationen.
- Einsatz von ETags: Der HTTP-Header If-None-Match, der für die erfolgte Zustellung von Web-Ressourcen konzipiert ist und automatisch wie HTTP-Cookies an Webserver als Bestandteil des HTTP-Requests versendet wird, kann zur Speicherung von eindeutigen Kennungen verwendet werden und so Anwender identifizieren.
- Browser-Fingerprinting: Durch Ausführung von JavaScript-Code im Browser des Webnutzers können plattform- und browserindividuelle Informationen der Webseitenbesucher wie z. B. User-Agent, Plugin-Liste, installierte Schriftarten derart abgerufen werden, dass eine äußerst hohe Wahrscheinlichkeit für die Eindeutigkeit der Browser berechnet werden kann.
- Canvas-Fingerprinting: Durch Aufruf der OpenGL-API des Browsers können bei HTML5 Renderinginformationen ermittelt werden, die eine ähnlich hohe Eindeutigkeit besitzen wie das Browser-Fingerprinting mit JavaScript.

Der Einsatz dieser Trackingmethoden ermöglicht folglich, dass der Browser eines Webseitenbesuchers mit sehr hoher Wahrscheinlichkeit eindeutig bestimmt werden kann. Somit wäre damit technisch eine Alternative für den Einsatz von herkömmlichen Cookies vorhanden, die selbst bei Ablehnen und/oder Löschen von Cookies ein Tracking realisierbar macht.

Aus datenschutzrechtlicher Sicht ist das Erstellen von Nutzungsprofilen unter Pseudonym zu Zwecken der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien in § 15 Abs. 3 TMG geregelt. Das Erstellen eines pseudonymen Nutzungsprofils zu den genannten Zwecken ist jedoch nur erlaubt, wenn ein Nutzer einer solchen Nutzungsprofilbildung nicht widerspricht (§ 15 Abs. 3 Satz 1 TMG). Auf seine Widerspruchsmöglichkeit ist der Nutzer gem. § 15 Abs. 3

Satz 2 TMG im Rahmen der Datenschutzerklärung gem. § 13 Abs. 1 TMG ebenso wie auf das Verfahren an sich hinzuweisen (§ 13 Abs. 1 Satz 2 TMG). Soweit bei den vorher genannten Verfahren z. B. mangels Nutzungsprofilbildung unter Pseudonym oder aufgrund des verfolgten Zwecks § 15 Abs. 3 TMG keine Anwendung findet, bedarf es einer Einwilligung des Nutzers.

Nach unserer Erfahrung gestaltet sich die praktische Umsetzung dieser gesetzlichen Anforderung jedoch oftmals als nicht ausreichend. Zwar ist eine Information theoretisch noch möglich, scheitert jedoch häufig an den Anforderungen einer tatsächlich transparenten und vor allem allgemein verständlichen Darstellung. Darüber hinaus stellt sich aber auch die Frage, wie eine wirksame Widerspruchsmöglichkeit bei den einzelnen Tracking-Technologien überhaupt machbar wäre.

Wir empfehlen daher grundsätzlich, vom Einsatz alternativer Trackingverfahren dieser Art Abstand zu nehmen. Das Risiko eines Bußgeldes wäre hier insofern erhöht, da wir den ordnungswidrigen Einsatz von Verfahren, mit denen die Nutzereinstellungen zum Schutz vor einer Nutzungsprofilbildung gezielt ausgehebelt werden, verstärkt mit Bußgeldern ahnden. Wir weisen darauf hin, dass stattdessen der Einsatz von HTTP-Cookies nach wie vor möglich ist.

7.8 Veröffentlichung von Fotos im Internet

Die Veröffentlichung von Fotos eines minderjährigen Kindes durch die leibliche Mutter ist unzulässig, wenn dieser das Sorgerecht entzogen wurde und keine Einwilligung der gesetzlichen Vertreter vorliegt.

Pflegeeltern haben sich an uns mit dem Hinweis gewandt, dass die leibliche Mutter ihres neunjährigen Pflegekindes Fotos des Kindes in ihrem Facebook-Account veröffentlicht, die von jedem Dritten eingesehen werden können. Hierfür hätten sie keine Einwilligung erteilt und forderten die Löschung dieser Fotos.

Gemäß § 22 Satz 1 Kunsturhebergesetz (KUG) dürfen „Bildnisse (…) nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden." Davon ist im Sinne dieser Vorschrift auszugehen, wenn ein Foto mit einer Person einer nicht begrenzten Öffentlichkeit sichtbar gemacht, z. B. in einem sozialen Netzwerk (Facebook) im dort öffentlich zugänglichen Bereich eingestellt wird. Grundsätzlich muss in solchen Fällen deshalb eine Einwilligung der abgebildeten Person zur Veröffentlichung des Fotos eingeholt werden.

Soweit es sich bei der abgebildeten Person um eine minderjährige Person handelt, kann diese bei vorhandener Einsichtsfähigkeit eine Einwilligung selbst erteilen, ansonsten müssen die gesetzlichen Vertreter einwilligen. Die Einsichtsfähigkeit einer Person ist dann zu bejahen, wenn die abgebildete Person einschätzen kann, was eine Veröffentlichung im Internet bedeutet, wer dieses Foto zur Kenntnis nehmen kann und welche Folgen aus der Veröffentlichung entstehen können. Regelmäßig wird vom Vorliegen der Einsichtsfähigkeit zwischen 13 und 16 Jahren ausgegangen, wobei aber stets auf den konkreten Einzelfall abzustellen ist. Da die abgebildete Person im konkreten Fall erst neun Jahre alt gewesen ist, war eine Einsichtsfähigkeit der Person noch nicht gegeben, so dass es der Einwilligung der gesetzlichen Vertreter bedurfte.

Muss die gesetzliche Vertretung des Kindes einwilligen, sind dies grundsätzlich die Eltern (vgl. § 1626 BGB). Soweit diesen jedoch das Sorgerecht entzogen und ein Vormund bestellt wurde, vertritt dieser gemäß § 1793 BGB das Mündel und kann die Einwilligung zur Veröffentlichung der Bilder erteilen.

Nachdem die leibliche Mutter über die Rechtslage informiert wurde, hat sie auf unsere Aufforderung hin, wenn auch wenig einsichtig und unter Protest, die Bilder ihres Kindes von ihrem Facebook-Account entfernt.

7.9 Einwilligung aus Afrika

Regelmäßig erreichen uns Anfragen zu der Formulierung von Einwilligungen, insbesondere zur Veröffentlichung von Fotos. Ungewöhnlich war der Wunsch nach Unterstützung bei der Formulierung einer Einwilligungserklärung von einer in Afrika tätigen deutschen Hilfsorganisation für die Veröffentlichung von Bildern in Deutschland.

Die Hilfsorganisation wandte sich an uns und sagte, sie wolle über die Verwendung von gesammelten Spenden für ein Hilfsprojekt in Afrika berichten und dabei Bilder von hilfsbedürftigen Kindern sowie alten Menschen, die konkrete Hilfe erfahren haben, auf den Webseiten von Unterstützungsorganisationen in Deutschland durch diese veröffentlichen lassen.

Wohl wissend, dass die von der Veröffentlichung betroffenen Personen in Afrika gewichtigere Sorgen als die Veröffentlichung ihres Fotos auf der Homepage einer deutschen Hilfsorganisation haben, sind wir unserer Beratungspflicht natürlich dennoch gerne nachgekommen und haben folgenden Einwilligungsvorschlag unterbreitet:

„Einwilligung zur Veröffentlichung von Fotos im Internet unter … [bitte URL angeben]

Ich bin damit einverstanden, dass Fotos, welche im Rahmen des Projektes XY [bitte konkretisieren, alternativ: im Rahmen eines Projektes] von Mitarbeitern der A-Organisation gemacht werden und auf denen ich abgebildet bin, an die B-Organisation [bitte Name der Unterstützungsorganisation eintragen] weitergegeben und von dieser im Internet auf ihrer Webseite unter … [bitte URL angeben] für die Dauer von … [soweit der Zeitraum der Veröffentlichung bekannt ist, diesen bitte angeben] veröffentlicht werden. Die Veröffentlichung auf den Webseiten der Unterstützerorganisation erfolgt, um die Tätigkeit und das Engagement der A-Organisation einem größeren Personenkreis bekannt zu machen. Mir ist bekannt, dass im Internet veröffentlichte Fotos weltweit abrufbar sind und eine Weiterverwendung dieser Fotos durch Dritte nicht generell ausgeschlossen werden kann. Die von mir erteilte Einwilligungserklärung kann ich jederzeit mit Wirkung für die Zukunft gegenüber der A-Organisation [bitte Kontaktdaten angeben, an die ein Widerruf gerichtet werden kann] widerrufen.

Ort, Datum

Unterschrift der abgebildeten Person"

Soweit eine Einsichtsfähigkeit der abgebildeten Person nicht anzunehmen ist, schlugen wir folgende Ergänzung für die gesetzliche Vertretung vor:

„Ich / Wir …..[Name und Zuname des/der gesetzlichen Vertreter/s] habe/n den oben aufgeführten Text zur Kenntnis genommen und bin/sind damit einverstanden, dass von meinem/unserem Kind … [Name und Zuname] Fotos, welche im Rahmen des Projektes … [bitte konkretisieren, alternativ: im Rahmen eines Projektes] von Mitarbeitern der A-Organisation gemacht wurden, im Internetauftritt unter … [bitte URL angeben] veröffentlicht werden.

Mir/Uns ist bekannt, dass ich/wir diese Einwilligungserklärung jederzeit mit Wirkung für die Zukunft gegenüber der A-Organisation [bitte Kontaktdaten angeben, an die ein Widerruf gerichtet werden kann] widerrufen kann/können.

Ort, Datum

Unterschrift(en) des/der gesetzlichen Vertreter/s"

Daneben wiesen wir darauf hin, dass bei der Übermittlung von Fotos an andere Unterstützungsorganisationen mit diesen klar vereinbart werden sollte, zu welchem Zweck und für welche Dauer eine Veröffentlichung der Fotos erfolgen soll/kann und dass diese nach der bestimmten Frist gelöscht werden müssen.

Darüber hinaus sollte bei der Einholung der Einwilligungserklärung darauf geachtet werden, dass die Erklärung später einer konkreten Person zugeordnet werden kann – auch bei unleserlicher Unterschrift. Möglich wäre es,

noch eine Zeile einzufügen bzw. den Namen auf der Einwilligungserklärung nochmals zu vermerken. Dies ist insbesondere dann relevant, wenn eine Einwilligung widerrufen wird.

Damit diese Einwilligungserklärungen informiert abgegeben werden können, hatten wir uns ausnahmsweise bereit erklärt, sie in die Amtssprache des afrikanischen Landes, die glücklicherweise Englisch war, zu übersetzen.

7.10 Messe-Registrierungen

Ob und inwieweit die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Besuchern einer Messe zulässig ist, hängt zunächst maßgeblich davon ab, ob es sich um eine Messe handelt, die für jedermann oder nur für ein bestimmtes Fachpublikum zugänglich ist. Unabhängig davon kann die Erhebung und Verarbeitung von Besucherdaten erforderlich sein, wenn Gutscheine von Ausstellern einer Messe eingelöst werden.

Im Berichtszeitraum haben sich auffallend viele Bürger an uns gewandt, die sich über die Erhebung, Verarbeitung und Nutzung ihrer personenbezogenen Daten im Zusammenhang mit einem Messebesuch beschwert haben. Dabei wurde beispielsweise vorgetragen, dass bei der Bestellung von Tickets im Online-Shop des Messeveranstalters – obwohl der Besteller im Besitz eines Gutscheins für ein Tagesticket war – eine Vielzahl von personenbezogenen Daten anzugeben waren oder die Messebesucher vor Ort zum Ausfüllen eines Registrierungsformulars „animiert" worden sind.

Wir haben uns mit der durch die Eingaben wieder aktuell gewordenen Thematik befasst und verschiedenen Messeveranstaltern unsere folgende Auffassung mitgeteilt:

Zunächst ist nach dem Charakter der jeweiligen Messe zu unterscheiden, d. h. ob eine Messe ausschließlich für Fachbesucher geöffnet ist, die für einen Besuch eine bestimmte fachliche Qualifikation vorweisen müssen („geschlossene" Messe), oder sich die Messe an die breite Öffentlichkeit richtet und der Besuch damit jedem Interessenten offen steht („offene" Messe).

Handelt es sich um eine „geschlossene" Messe, ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Messebesuchern aus datenschutzrechtlicher Sicht zulässig, sofern dies zum Zweck der Legitimationsprüfung erforderlich ist (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Anders zu beurteilen ist der Sachverhalt bei einer „offenen" Messe. Hier lässt sich eine (zwangsweise) Besucherregistrierung – sowohl an der Kasse vor Ort, als auch bei einer Ticketbestellung im Online-Shop – grundsätzlich nicht auf die Erlaubnisse des BDSG stützen, denn diese Datenerhebung ist für die Erfüllung und die Zweckbestimmung des Vertragsverhältnisses zwischen dem Messeveranstalter und dem Messebesucher nicht erforderlich. Diesbezüglich weisen wir auf unseren 1. Tätigkeitsbericht 2002/2003 (S. 39 f.) hin.

Allerdings ist es datenschutzrechtlich zulässig, wenn die Gewährung von Vergünstigungen (z. B. Gutschein für eine Eintrittskarte, Vorverkaufsrabatt) im Rahmen der allgemeinen Vertragsfreiheit von Seiten des Messeveranstalters von einer Besucherregistrierung abhängig gemacht wird, sofern der Messebesucher auf die Alternative eines anonymen Messebesuches durch Kauf eines regulären Tickets aufmerksam gemacht wird (z. B. durch einen Hinweis auf dem Gutschein und/oder der Datenschutzerklärung des Online-Shops). Regelmäßig werden die Daten der Besucher, die einen von einem Aussteller zur Verfügung gestellten Eintrittsgutschein einlösen, an diesen weitergeleitet. So kann er nachvollziehen, welche seiner Kunden den Gutschein eingelöst haben und für wie viele Gutscheine er gegenüber der Messe aufkommen muss.

Es ist aus unserer Sicht jeweils entscheidend, dass der Messeveranstalter auf eine ausreichende Transparenz gegenüber dem Messebesucher, sowohl im Internetauftritt (z. B. Ticket-Shop), als auch vor Ort (Registrierungsformular) achtet, um ihm gegenüber beispielsweise deutlich zu machen, dass das Ausfüllen eines Registrierungsformulars bei einer „offenen"

Messe vor Ort auf ausdrücklich freiwilliger Basis erfolgt oder die Möglichkeit des Einlösens eines Gutscheins von einem bestimmten Datenumgang abhängig gemacht wird.

7.11 Ahnenforschung im Internet

Werden im Rahmen einer Ahnenforschung auch lebende Nachkommen benannt, so ist zunächst zu prüfen, inwiefern der familiäre und persönliche Bereich überschritten wird. Wird dies bejaht, ist eine Interessenabwägung zwischen dem Interesse der noch lebenden Nachkommen an der Nicht-Benennung und dem Interesse der veröffentlichenden Stelle an der Bekanntmachung der Nachkommen durchzuführen. In vielen Fällen genügt die Kennzeichnung, dass lebende Nachkommen existieren und ggf. welches Geschlecht diese haben.

Eine Eingabeführerin hat sich an uns gewandt und vorgetragen, sie sei zufällig auf den Internetauftritt einer Familienstiftung gestoßen, die sich mit der (Abstammungs-)Geschichte einer bestimmten Familie beschäftigt. Es seien dort insbesondere auch ein Stammbaum, sowie verschiedene weitere Datensammlungen zur Familie (z. B. Geburten in einem bestimmten Zeitraum) veröffentlicht. In diesen Datensammlungen und dem Stammbaum habe sie Daten zu ihrer eigenen Person und ihren Kindern entdeckt. In eine solche Veröffentlichung personenbezogener Daten im offenen Internet habe sie nicht eingewilligt.

Bei den Ermittlungen zum vorgetragenen Sachverhalt wurde festgestellt, dass in besagtem Internetauftritt zur Person der Eingabeführerin der Anfangsbuchstabe ihres Vornamens sowie ihr Geburtsname, zu ihren Kindern der vollständige Vor- und Familienname samt Geburtsdatum veröffentlicht wurden.

Bei der datenschutzrechtlichen Bewertung von Familienstammbäumen im offenen Internet gehen wir davon aus, dass sich der Anwendungsbereich des BDSG nur auf natürliche, lebende Personen erstreckt (also nicht auf bereits verstorbene Personen) und dann nicht eröffnet ist, wenn die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt (§ 1 Abs. 2 Nr. 3 BDSG).

Ist der Anwendungsbereich des BDSG eröffnet, handelt es sich bei einer Veröffentlichung personenbezogener Daten im Internet um eine Übermittlung personenbezogener Daten, für die es einer Rechtsgrundlage bzw. der ausdrücklichen Einwilligung der von der Veröffentlichung betroffenen Person bedarf. Konfrontiert mit diesen datenschutzrechtlichen Rahmenbedingungen hat die für die Internetveröffentlichung verantwortliche Familienstiftung darauf umgehend reagiert, die Veröffentlichungen aus dem öffentlich zugänglichen Bereich des Internetauftritts beseitigt und auf den „Mitgliederbereich" der Familienstiftung begrenzt, zu dem nur auf Antrag von Familienmitgliedern eine Zugangsberechtigung erteilt wird.

Da der Kreis der potentiell zugangsberechtigten Familienmitglieder aber ca. 1.500 Personen umfasst, haben wir die Auffassung vertreten, dass im konkreten Sachverhalt auch nach der Beschränkung auf den „Mitgliederbereich" nicht mehr von einer „persönlichen oder familiären Tätigkeit" ausgegangen werden kann und sich der Umgang mit den personenbezogenen Daten am Maßstab des BDSG messen lassen muss.

Das Gesetz beinhaltet zwar keine Definition, wann genau von einer persönlichen oder familiären Tätigkeit auszugehen ist. Wir sind der Auffassung, dass dieser Tatbestand restriktiv auszulegen und entscheidend ist, dass der Datenumgang im privaten Aktionskreis stattfindet. Auch wenn das Gesetz nicht verlangt, dass zu allen vom Datenumgang Betroffenen eine persönliche Beziehung besteht, wird angenommen, dass der betroffene Personenkreis meist den persönlichen oder familiären Zweck widerspiegelt.

Bei dem großen Kreis von 1.500 Familienangehörigen sind wir nicht mehr von einer „persönlichen oder familiären Tätigkeit" ausgegangen

und haben die Veröffentlichung nur bei Vorliegen einer Einwilligung der Betroffenen oder einer einschlägigen Rechtsgrundlage für die Übermittlung für datenschutzrechtlich als zulässig erachtet.

Da eine ausdrückliche Einwilligung der Betroffenen in dem uns vorgetragenen Fall nicht vorgelegen hat, kamen als Rechtsgrundlage nach dem BDSG die Vorschriften des § 28 Abs. 1 Satz 1 Nr. 2, 3 BDSG in Betracht. Damit hat eine Abwägung zwischen dem berechtigten Interesse der Familienstiftung einerseits und der von einer Erhebung, Verarbeitung und Nutzung ihrer personenbezogenen Daten betroffenen Person andererseits zu erfolgen. Im vorliegenden Fall konnten uns keine überwiegenden Interessen durch die Familienstiftung dargelegt werden. Die Stiftung ist deshalb durch eine Sperrung der Daten für die Öffentlichkeit und andere Familienmitglieder durch einen schlichten Hinweis im Internetauftritt auf weitere lebende Personen bzw. auf deren Geschlecht dem Widerspruch der Eingabeführerin nachgekommen.

7.12 Anfertigung von Fotos im Kindergarten mit anschließender Online-Bestellmöglichkeit

Bei der Durchführung von Fototerminen in Kindergärten und einer online angebotenen Bestellmöglichkeit für die Eltern ist darauf zu achten, dass diese über die Anfertigung der Fotos und der Nachbestellungsmöglichkeit über ein Online-Portal hinreichend informiert werden. Besteht kein Interesse (mehr) an den Fotos und wird dies von den Eltern kommuniziert, müssen diese aus dem Online-Portal entfernt werden.

Im konkreten Sachverhalt wurde den Eltern nach Erstellung von Aufnahmen durch einen professionellen Fotografen über den Kindergarten eine entsprechende Fotomappe zu ihrem Kind ausgehändigt und zum Kauf angeboten. Dabei war in der Fotomappe ein Hinweis enthalten, wonach die Fotos auch in einem geschlossenen Bereich des Internetauftritts des Fotounternehmens gespeichert sind, von den Eltern durch Eingabe eines Benutzernamens und eines Passwortes dort eingesehen werden und eventuelle Nachbestellungen in Auftrag gegeben werden können.

Da die Eltern in unserem Fall kein Interesse an der Fotomappe hatten, gaben sie diese dem Kindergarten zurück. Bei uns haben sich die Eltern schließlich über den Umstand beschwert, dass die Fotos ihrer Tochter offenbar für die Dauer eines Jahres im geschlossenen Bereich des Internetauftritts des Fotounternehmens gespeichert und für Nachbestellungen vorgehalten werden. Hierfür hätten sie keine Einwilligung erteilt und eine Nachbestellung von Fotos könnten sie bereits zum jetzigen Zeitpunkt definitiv ausschließen.

Der Beschwerde der Eltern konnte dadurch abgeholfen werden, dass sich das Fotounternehmen dazu bereit erklärt hat, eine Löschung der Bilder aus der Datenbank vorzunehmen. Dennoch war dieser Eingabefall Anlass für uns, die allgemeine Verfahrenspraxis des Unternehmens aus datenschutzrechtlicher Sicht näher zu beleuchten.

Der grundsätzliche Ablauf einer Fotoaktion in einem Kindergarten wurde uns stichpunktartig wie folgt dargestellt, wobei wir davon ausgehen, dass sich dieser Ablauf auch bei der Tätigkeit vieler anderer Fotounternehmen wiederfinden lassen dürfte:

- Das Fotounternehmen stimmt mit der Kindergartenleitung die Durchführung einer Fotoaktion ab und legt die konkreten Termine fest.
- Die Kindergartenleitung informiert die Eltern der Kinder über die Durchführung der Fotoaktion durch Aushänge und/oder Verteilung entsprechender Informationszettel, wobei auf die Freiwilligkeit der Teilnahme hingewiesen wird.
- Beim Fototermin werden nur die Kinder der Eltern, die dies wünschen, fotografiert. Das Fotounternehmen erhebt im Rahmen der Erstellung der Fotos keine personenbezogenen Daten zur Person

des fotografierten Kindes bzw. dessen Eltern.

- Über die Kindergartenleitung werden den Eltern die Bilder ihres Kindes durch Aushändigung einer Fotomappe zum Kauf angeboten. Die Fotomappe enthält einen individualisierten Zugangscode und ein Passwort, mit deren Hilfe Eltern zu Nachbestellzwecken auf einen geschlossenen Bereich des Internetauftritts des Fotounternehmens und die dortigen Fotos des einzelnen Kindes zugreifen können. Die Bilder des Kindes bleiben dort für die Dauer eines Kindergartenjahres gespeichert.
- Fotomappen, die nicht gekauft werden, werden dem Kindergarten zurückgegeben, vom Fotounternehmen dort abgeholt und datenschutzgerecht vernichtet. Auf schriftlichen Wunsch der Eltern eines fotografierten Kindes werden die Fotos aus der Bilddatenbank im Internetauftritt des Fotounternehmens gelöscht.

Zu berücksichtigen ist hierbei, dass ein Vertragsschluss über die Abnahme von Fotos zwischen dem Fotounternehmen und den Eltern des fotografierten Kindes zustande kommt. Zwar mag dem Kindergarten eine vermittelnde Rolle dadurch zukommen, dass er die Eltern vorab über eine bevorstehende Fotoaktion informiert und die Aushändigung der Fotomappen übernimmt. Vertragspartner sind aber das Fotounternehmen und die jeweiligen Eltern.

Wird der Umgang mit den personenbezogenen Daten des Kindes (= der Fotos) darauf gestützt, dass dies für die Durchführung „eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich" ist (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG), muss den Eltern der Vertragsinhalt und der damit einhergehende Umgang mit den personenbezogenen Daten des Kindes klar sein. Dies umfasst einerseits die Erstellung von Fotos für Bildermappen, die den Eltern zum Kauf angeboten werden, andererseits aber auch die Aufnahme der erstellten Fotos in eine Bilderdatenbank zu Nachbestellzwecken für den Zeitraum eines Kindergartenjahres.

Während das Fotounternehmen in unserem Fall darauf abgestellt hat, dass die Information der Eltern durch die Kindergartenleitung übernommen wird, haben wir darauf hingewiesen, dass die Informationspflicht dem Fotounternehmen als der im datenschutzrechtlichen Sinn verantwortlichen Stelle obliegt und dieses durch geeignete Maßnahmen sicherzustellen hat, dass den Eltern zu fotografierender Kinder die erforderlichen Informationen zukommen.

Als vertretbare und praxisnahe Lösung haben wir im Ergebnis angesehen, dass in den ausgegebenen Fotomappen neben dem Hinweis auf die Möglichkeit der Bestellung/Nachbestellung künftig auch eine deutliche Information über die Dauer der Speicherung des Bildes zu finden sein wird und den Eltern die Möglichkeit und der Weg einer (vorzeitigen) Löschung des Bildes aus der Bilderdatenbank des Fotounternehmens aufgezeigt wird.

8

Rechtsanwälte

8 Rechtsanwälte

Wir haben in der Vergangenheit sowohl anlassbezogen als auch im Rahmen anlassloser Prüfaktivitäten Rechtsanwaltskanzleien datenschutzrechtlich überprüft. Aus aktuellem Anlass haben wir mit der Bundesrechtsanwaltskammer ein Gespräch über die Reichweite unserer aufsichtlichen Befugnisse geführt und das Thema im Düsseldorfer Kreis erörtert.

Ein Rechtsanwalt, der von uns anlasslos geprüft werden sollte, hat sich unter Berufung auf seine anwaltliche Schweigepflicht nach § 203 Abs. 1 Nr. 3 StGB, § 43a Abs. 2 BRAO und § 2 BORA geweigert, uns die geforderten Auskünfte insbesondere zur Gewährleistung der Datensicherheit zu erteilen und uns Zutritt zur Kanzlei zu gewähren. Zudem hat er seine Bedenken der Bundesrechtsanwaltskammer (BRAK) vorgetragen. Vor diesem Hintergrund haben wir mit Vertretern der BRAK ein Gespräch über die Reichweite unserer aufsichtlichen Befugnisse nach § 38 BDSG gegenüber Rechtsanwälten geführt.

Die Vertreter der BRAK betonten, dass sich die Rechtsanwälte wegen ihrer gebotenen Staatsferne in einer besonderen Situation befänden, die nicht mit der anderer Berufsgeheimnisträger (z. B. Ärzte) vergleichbar sei. Denn die Tatsache, dass der Staat im Prozess häufig als Gegner auftrete (z. B. im Verwaltungs- oder Steuerrecht), mache es erforderlich, die Rechtsanwälte der staatlichen Kontrolle zu entziehen und sie der Aufsicht durch die Rechtsanwaltskammern zu unterstellen. Diesem Umstand werde beispielsweise durch die gesondert eingerichtete Anwaltsgerichtsbarkeit Rechnung getragen. Eine Zuständigkeit der Datenschutzaufsichtsbehörden bestehe daher lediglich dann, wenn Rechtsanwälte unternehmerisch tätig würden oder es um den Beschäftigtendatenschutz von Mitarbeitern gehe. Im Übrigen stünden den Datenschutzaufsichtsbehörden keine Befugnisse gegenüber Rechtsanwälten zu.

Unserer Auffassung nach sind hingegen die Datenschutzaufsichtsbehörden zur Kontrolle von Berufsgeheimnisträgern im Sinn des § 203 Abs. 1 StGB und damit grundsätzlich auch zur Prüfung bei Rechtsanwälten befugt. Denn angesichts der gesetzlich geregelten Aufsichtsbefugnisse in § 38 BDSG liegt bei einer solchen Prüfung grundsätzlich kein unbefugtes Offenbaren von Berufsgeheimnissen vor. Insbesondere im Hinblick auf einen Beschluss des Kammergerichts Berlin vom 20.08.2010 (Az. 1 Ws (B) 51/07) erkennen wir aber eine Beschränkung unserer Aufsichtsbefugnisse an, soweit es um die Einsicht in Daten geht, die sich auf ein konkretes anwaltliches Mandat beziehen; diese Daten unterliegen somit nicht unserer Prüfung. Dies ist insbesondere für diejenigen Fälle relevant, in denen sich Eingabeführer an uns mit der Bitte wenden, gegenüber einem (gegnerischen) Rechtsanwalt einen Auskunftsanspruch nach § 34 Abs. 1 BDSG durchzusetzen, um zu erfahren, über welche Informationen der Rechtsanwalt verfügt und woher er diese erhalten hat. Bei derartigen Eingaben weisen wir die Eingabeführer auf das anwaltliche Berufsgeheimnis und die damit einhergehende Schweigepflicht des Rechtsanwalts hin. Auch wenn solche konkreten mandatsbezogenen Daten nicht unserer Prüfung unterliegen, sind wir der Auffassung, dass insbesondere Fragen der Datensicherheit, die unabhängig vom konkreten Mandat generell dem Schutz der Daten in der Kanzlei dienen, unserer Kontrollkompetenz unterfallen und wir deshalb insbesondere zur Prüfung der Einhaltung der Vorschriften des § 9 BDSG befugt sind.

Bevor wir im Rahmen unserer laufenden Prüfverfahren ggf. eine Anordnung nach § 38 Abs. 5 BDSG erlassen, die zur Klärung durch die Verwaltungsgerichtsbarkeit führen kann, haben wir auf Bitten der BRAK das Thema im Düsseldorfer Kreis erörtert, um eine Abstimmung unter den Aufsichtsbehörden zu erreichen. Eine abschließende Befassung hierzu steht noch aus.

Unabhängig davon haben wir auch andere Rechtsanwaltskanzleien geprüft, die keine Zweifel an unserer Prüfungskompetenz hatten, sich vielmehr dankbar zeigten für die prakti-

schen Hinweise insbesondere zur Verbesserung ihrer technisch organisatorischen Maßnahmen nach § 9 BDSG und der Anlage dazu.

9 Versicherungswirtschaft

9 Versicherungswirtschaft

9.1 Erfahrungen mit der neuen Einwilligungs- und Schweigepflichtentbindungserklärung

Das Bundesverfassungsgericht hat sich 2013 erneut zum zulässigen Umfang einer Einwilligungs- und Schweigepflichtentbindungserklärung einer Versicherung geäußert.

Im letzten Tätigkeitsbericht hatten wir darüber berichtet, dass infolge einer Entscheidung des Bundesverfassungsgerichts (BVerfG) aus dem Jahr 2006 zwischen der Versicherungswirtschaft und den Aufsichtsbehörden eine neue Einwilligungs- und Schweigepflichtentbindungserklärung für den Umgang mit Gesundheitsdaten abgestimmt worden ist. Seitdem gingen bei uns zahlreiche Anfragen von Betroffenen ein, die sich über die Bedeutung und Tragweite der Einwilligungs- und Schweigepflichtentbindungserklärung informieren wollten oder Zweifel an der von ihrer Versicherung verwendeten Erklärung hatten. Bei den meisten von uns überprüften Eingaben konnten wir keine Datenschutzverstöße feststellen. In einzelnen Fällen haben wir darauf hingewirkt, dass seitens der betroffenen Versicherungen Anpassungen in ihren Formularen vorgenommen werden oder der Betroffene ergänzende Auskünfte erhält.

Im Jahr 2013 hat sich das BVerfG erneut mit einer Einwilligungs- und Schweigepflichtentbindungserklärung beschäftigt, die von einer Versicherung für die Erhebung von Gesundheitsdaten verwendet worden war (Beschluss vom 17.07.2013, Az. 1 BvR 3167/08). Zwar liegt der Entscheidung ein Sachverhalt zugrunde, in dem noch nicht die neue Einwilligungs- und Schweigepflichtentbindungserklärung zum Einsatz kam. Die Anforderungen, die das BVerfG dort für den zulässigen Umfang einer Einwilligungs- und Schweigepflichtentbindungserklärung aufgestellt hat, sind aber auch für die nun verwendete Erklärung von Bedeutung. In dem vom BVerfG entschiedenen Fall sollte Ärzten durch die Einwilligungserklärung erlaubt werden, der Versicherung „umfassend" Auskunft über die Gesundheitsverhältnisse der Betroffenen zu erteilen. Das BVerfG stellte hierzu fest, dass es dadurch der Versicherung ermöglicht würde, „auch über das für die Abwicklung des Versicherungsfalls erforderliche Maß hinaus in weitem Umfang sensible Informationen" einzuholen; die Formulierung würde damit auch Informationen umfassen, die für die Abwicklung des Versicherungsfalls bedeutungslos sind. Eine solche Regelung trage dem Recht auf informationelle Selbstbestimmung nicht hinreichend Rechnung.

Diesen Vorgaben des BVerfG wird die neue Erklärung dadurch gerecht, dass der Betroffene nur in die Erhebung, Verarbeitung und Nutzung seiner Gesundheitsdaten einwilligen soll, soweit dies zur Antrags- bzw. Leistungsfallprüfung „erforderlich" ist. Vor diesem Hintergrund ergibt sich unserer Einschätzung nach aus der Entscheidung des BVerfG derzeit kein Änderungsbedarf für die mit der Versicherungswirtschaft abgestimmte Einwilligungs- und Schweigepflichtentbindungserklärung. Die Versicherungen haben aber dafür Sorge zu tragen, dass sich die Erhebung von Gesundheitsdaten tatsächlich auf das erforderliche Maß beschränkt. Dies gilt insbesondere für die Fälle, in denen der Betroffene seine Einwilligung bereits vor Abgabe der Vertragserklärung generell erteilt (vgl. § 213 Abs. 2 des Versicherungsvertragsgesetzes) und deshalb vor einer Datenerhebung von der Versicherung im konkreten Fall informiert werden muss, von wem und zu welchem Zweck die Daten erhoben werden sollen. Diese Unterrichtung muss es dem Betroffenen ermöglichen, die Erforderlichkeit der beabsichtigten Datenerhebung nachzuvollziehen.

9.2 Beauftragung einer Restwertbörse zwecks Ermittlung des Restwerts eines Kfz

Die Fahrzeug-Identifizierungsnummer ist ein personenbezogenes Datum. Verlangt

ein Versicherungsnehmer gegenüber dem Versicherungsunternehmen Auskunft nach § 34 Abs. 1 BDSG, ist ihm daher auch mitzuteilen, welche Dienstleister dieses Datum von der Versicherung erhalten haben.

Um nach Verkehrsunfällen den Wert zu ermitteln, der sich bei einem Verkauf eines beschädigten Fahrzeugs noch erzielen lässt, beauftragen Kfz-Versicherungen sogenannte Online-Restwertbörsen. Zu diesem Zweck erhält das Unternehmen, das die Restwertbörse betreibt, von der Versicherung verschiedene Angaben über das beschädigte Fahrzeug; zwecks eindeutiger Identifizierung des Fahrzeugs zählt zu diesen Angaben auch die sogenannte Fahrzeug-Identifizierungsnummer (FIN). Die Onlinebörse stellt daraufhin die relevanten Informationen in ein Online-Portal ein, ohne dabei jedoch die vollständige FIN anzugeben. Nach Abschluss der Aktion informiert die Restwertbörse die Versicherung über das höchste Angebot, das dort abgegeben wurde, sowie über den Namen und die Kontaktdaten des entsprechenden Händlers. Die Versicherung gibt diese Informationen wiederum an den Versicherungsnehmer weiter, damit dieser sich mit dem Händler in Verbindung setzen kann. Nachdem ein Bürger von seiner Kfz-Versicherung über ein solches Angebot eines Händlers unterrichtet worden war, beschwerte er sich bei uns, dass seine Daten rechtswidrig an die Restwertbörse übermittelt worden seien; zudem enthalte die Auskunft, die er nach § 34 Abs. 1 BDSG von der Versicherung erbeten habe, keine Aussage darüber, ob bzw. welche Daten an die Restwertbörse übermittelt worden seien.

Das Versicherungsunternehmen vertrat die Auffassung, dass die Restwertbörse keine personenbezogenen Daten erhalten habe. Vor diesem Hintergrund sei im Rahmen der Auskunftserteilung nach § 34 Abs. 1 BDSG auch nicht auf die Restwertbörse eingegangen worden. Diese Einschätzung teilen wir nicht. Denn die FIN ermöglicht es auch privaten Stellen, den Halter des Fahrzeugs ohne unverhältnismäßigen Aufwand zu ermitteln. Hierzu genügt eine einfache Registerauskunft nach § 39 Abs. 1 des Straßenverkehrsgesetzes (StVG), wonach die Zulassungsbehörde oder das Kraftfahrt-Bundesamt u. a. den Namen und die Anschrift des Fahrzeughalters übermittelt, wenn der Empfänger unter Angabe der FIN ein berechtigtes Interesse an diesen Daten darlegt. Eine solche Abfrage bereitet weder einen großen Aufwand noch verursacht sie hohe Kosten (vgl. Urteil des AG Coburg vom 07.11.2012, Az. 12 C 179/12 und Urteil des LG Kassel vom 25.02.2014, Az. 1 S 172/13). Für die Einordnung der FIN als personenbezogenes Datum im Sinn des § 3 Abs. 1 BDSG spricht auch die Regelung in § 45 Satz 2 StVG, wonach die FIN ausdrücklich zu den Daten gehört, die einen Bezug zu einer bestimmten oder bestimmbaren Person ermöglichen. Wir haben daher das Versicherungsunternehmen darauf hingewiesen, dass sie der Restwertbörse mit der FIN ein personenbezogenes Datum mitgeteilt hat, deren Übermittlung grundsätzlich der Einwilligung des Betroffenen oder einer Rechtsgrundlage bedarf.

Eine Restwertbörse kann für ein Versicherungsunternehmen jedoch im Rahmen einer Auftragsdatenverarbeitung tätig werden. Wird hierfür ein Vertrag gemäß § 11 BDSG abgeschlossen, stellt der Austausch personenbezogener Daten zwischen Versicherung und Restwertbörse keine Datenübermittlung im Sinn des BDSG dar, sondern wird gesetzlich privilegiert (vgl. § 3 Abs. 8 Satz 3 BDSG). Sind die Voraussetzungen nach § 11 BDSG erfüllt, benötigt die Versicherung weder eine Rechtsgrundlage noch die Einwilligung des Betroffenen, um der Restwertbörse personenbezogene Daten wie die FIN mitzuteilen.

Macht ein Versicherungsnehmer gegenüber seiner Versicherung einen Auskunftsanspruch nach § 34 Abs. 1 BDSG geltend, hat ihn die Versicherung darüber zu informieren, dass die FIN als personenbezogenes Datum an die Restwertbörse weitergegeben wurde. Denn gemäß § 34 Abs. 1 Satz 1 Nr. 2 BDSG hat sich die Auskunft u. a. auf den Empfänger, an den Daten weitergegeben werden, zu beziehen. „Empfänger" ist dabei jede Stelle, die Daten erhält, und umfasst anders als der Begriff des „Dritten" auch Auftragnehmer, die als interne Stelle behandelt werden (vgl. § 3 Abs. 8 BDSG). Das Versicherungsunternehmen war der An-

sicht, dass zur Erfüllung des Auskunftsanspruchs allerdings ein Hinweis auf die von der Versicherung im Internet veröffentlichte Dienstleisterliste genüge. Ein solcher Hinweis war im vorliegenden Fall aber schon deshalb nicht ausreichend, weil die betreffende Dienstleisterliste nur die Stellen enthielt, mit denen die Versicherung unter Verwendung von Gesundheitsdaten und weiterer nach § 203 StGB geschützter Daten zusammenarbeitet. Eine Online-Restwertbörse aus dem Bereich Kfz-Versicherung war nicht in der Liste enthalten. Auf unsere Veranlassung hin erteilte das Versicherungsunternehmen dem Betroffenen eine um die FIN bzw. die Restwertbörse als Datenempfänger ergänzte Auskunft nach § 34 Abs. 1 BDSG (siehe dazu auch Kapitel 6.5).

9.3 Personenverschiedenheit von Versicherungsnehmer und versicherter Person

Sind Versicherungsnehmer und versicherte Person nicht identisch, ist sorgfältig zu prüfen, wem die Versicherung jeweils Daten übermitteln oder Auskunft erteilen darf.

Im Regelfall sind Versicherungsnehmer und versicherte Person identisch. Beim Austausch von versichertenbezogenen Daten zwischen der Versicherung und ihrem Versicherungsnehmer – etwa im Rahmen der Leistungsabrechnung – stellt sich daher grundsätzlich nicht die Frage nach der Zulässigkeit eines solchen Austauschs. Anders verhält es sich, wenn es sich bei dem Versicherungsnehmer und der versicherten Person um zwei verschiedene Personen handelt, beispielsweise wenn der Ehegatte oder Kinder mitversichert sind. Zur Frage, wem in einem solchen Fall Abrechnungsdaten zuzusenden oder sonstige Auskünfte zu erteilen sind, erreichen uns immer wieder Anfragen von Versicherungsnehmern, versicherten Personen und Versicherungen.

9.3.1 Auskunftserteilung bei Angaben mit Doppelbezug

Sind Versicherungsnehmer und versicherte Person nicht identisch, handelt es sich bei den von der Versicherung erhobenen und gespeicherten Daten häufig um Angaben mit Doppelbezug, d. h. um Daten, die sich sowohl auf den Versicherungsnehmer als auch auf die versicherte Person beziehen. Verlangt die versicherte Person in einem solchen Fall Auskunft nach § 34 Abs. 1 BDSG, stellt sich die Frage, ob die Versicherung in Erfüllung des Auskunftsanspruchs an die versicherte Person damit auch Daten, die sich zugleich auf den Versicherungsnehmer beziehen, übermitteln muss bzw. darf.

Eine Pflicht zur Auskunftserteilung besteht gemäß § 34 Abs. 7 i. V. m. § 33 Abs. 2 Satz 1 Nr. 3 BDSG unter anderem dann nicht, wenn die Daten wegen des überwiegenden rechtlichen Interesses eines Dritten geheim gehalten werden müssen. Ob das rechtliche Interesse des Dritten überwiegt, ist durch eine Interessenabwägung im Einzelfall zu klären.

So wandte sich in einem Fall ein Eingabeführer mit dem Vorwurf an uns, seine Versicherung habe seiner geschiedenen Ex-Frau unzulässigerweise Daten über seinen Versicherungsvertrag übermittelt. Denn seine Ex-Frau, im vorliegenden Fall die versicherte Person, hatte von seiner Versicherung die Auskunft erlangt, dass ihm als Versicherungsnehmer die Kosten ihrer Behandlung erstattet worden waren. Da die Information über die Erstattung(sfähigkeit) der Behandlungskosten für die Frage entscheidend war, ob die begonnene medizinische Behandlung fortgesetzt bzw. abgeschlossen werden konnte, überwog das Interesse der Frau an der Auskunftserteilung das Geheimhaltungsinteresse ihres geschiedenen Mannes. Die Versicherung war demnach gemäß § 34 Abs. 1 BDSG zur Auskunftserteilung verpflichtet.

Überwiegt hingegen das Geheimhaltungsinteresse des Versicherungsnehmers, besteht gemäß § 34 Abs. 7 i. V. m. § 33 Abs. 2 Satz 1 Nr. 3 BDSG keine Pflicht zur Auskunftserteilung. Die Versicherung ist in einem solchen Fall dann auch nicht befugt, Auskunft zu erteilen. Dies

ergibt sich zunächst aus dem Wortlaut des § 33 Abs. 2 Satz 1 Nr. 3 BDSG, wonach die Daten im Fall des überwiegenden rechtlichen Interesses des Dritten geheim gehalten werden „müssen". Zudem würde sich die Zulässigkeit einer solchen Datenübermittlung nach § 28 Abs. 2 Nr. 2a BDSG richten und daher wiederum von einer Interessenabwägung abhängen. Vor diesem Hintergrund besteht in den Fällen, in denen das Geheimhaltungsinteresse des Versicherungsnehmers das Interesse der versicherten Person an der Auskunftserteilung überwiegt, weder eine Pflicht noch eine Befugnis der Versicherung zur Auskunftserteilung.

Entsprechendes gilt für den umgekehrten Fall, dass der Versicherungsnehmer Auskunft über Daten verlangt, die sich zugleich auf die versicherte Person beziehen.

9.3.2 Versand von Leistungsabrechnungen bei Versicherung für fremde Rechnung

In einem uns zur Prüfung vorgelegten Fall zahlte ein Versicherungsnehmer zwar weiterhin den Versicherungsbeitrag für seine von ihm getrennt lebende Ehefrau, hatte sie aber schriftlich mittels Vollmacht abweichend als empfangsberechtigte Person für Versicherungsleistungen bestimmt. Dennoch erhielt der Ehemann als Versicherungsnehmer Leistungsabrechnungen, die seine Frau betrafen. Die Versicherung sah darin keinen Verstoß gegen datenschutzrechtliche Vorschriften, da ihrer Auffassung nach der Versicherungsnehmer auch bei abweichender Auszahlungsbestimmung anspruchsberechtigt bleibe und daher die Leistungsabrechnungen an ihn versandt werden könnten.

Diese Einschätzung teilten wir nicht. Denn nach § 194 Abs. 3 Satz 1 des Versicherungsvertragsgesetzes (VVG) kann bei einer Versicherung für fremde Rechnung ausschließlich die versicherte Person die Versicherungsleistung verlangen, wenn der Versicherungsnehmer sie gegenüber der Versicherung in Textform als Empfangsberechtigten der Versicherungsleistung benannt hat. Liegt eine solche schriftliche Erklärung des Versicherungsnehmers vor, darf die Leistungsabrechnung nur der versicherten Person zugesandt werden. Die Zusendung der Leistungsabrechnung an den Ehegatten als Versicherungsnehmer stellte daher im vorliegenden Fall eine unzulässige Datenübermittlung dar.

9.3.3 Auskunftserteilung über medizinische Gutachten

Auch wenn eine Versicherung im Rahmen der Prüfung ihrer Leitungspflicht ein Gutachten über die Notwendigkeit einer medizinischen Behandlung eingeholt hat, stellt sich die Frage, wer Auskunft bzw. Einsicht in das Gutachten verlangen kann. Für diesen Fall hat der Gesetzgeber eine spezielle Regelung im Versicherungsvertragsgesetz getroffen: Gemäß § 202 Satz 1 VVG ist die Versicherung verpflichtet, auf Verlangen des Versicherungsnehmers oder der versicherten Person Auskunft über bzw. Einsicht in das Gutachten zu gewähren, so dass grundsätzlich beide Personen Inhaber eines entsprechenden Anspruchs sein können. Nach § 202 Satz 3 VVG kann der Anspruch allerdings nur von der jeweils betroffenen Person oder ihrem gesetzlichen Vertreter geltend gemacht werden.

10 Banken

10 Banken

10.1 Neues Kirchensteuer-Abzugsverfahren für Zinserträge

Finanzinstitute, insbesondere Banken, informierten ihre Kunden im Jahr 2014 pflichtgemäß darüber, dass die Verfahrensweise zur Begleichung der Kirchensteuer auf Kapitalerträge geändert wurde. Dies führte offensichtlich teilweise zu Irritationen bei Kunden und in der Folge zu Beschwerden bei der Datenschutzaufsicht.

Der Deutsche Bundestag hatte mit Änderung des Einkommensteuergesetzes (EStG) die Verfahrensweise zur Begleichung der Kirchensteuer auf Kapitalerträge neu geregelt.

Zur Einkommensteuer selbst war man es schon gewohnt, dass diese zu Zinserträgen von den Banken pauschal abgeführt bzw. die Zinserträge den Finanzämtern mitgeteilt werden. Nun müssen die Banken (aber ggf. auch Versicherungen) künftig grundsätzlich auch zur Kirchensteuer einen entsprechenden Abgeltungsbetrag einbehalten und an das Finanzamt abführen. Damit die Banken wissen, ob ein Kunde kirchensteuerpflichtig ist und welcher Religionsgemeinschaft die Kirchensteuer eines Kunden zusteht, müssen die Banken nach § 51a EStG beim Bundeszentralamt für Steuern nachfragen und bekommen dann von dort die notwendige Information.

Wer diese Information der Zugehörigkeit (oder Nicht-Zugehörigkeit) zu einer bestimmten Religionsgemeinschaft an seine Bank und die automatische Kirchensteuer-Abgeltung von vorne herein nicht haben, sondern weiterhin seine Kirchensteuer selbst über die jährliche Steuererklärung zahlen möchte, musste dies bis spätestens 30. Juni 2014 dem Bundeszentralamt für Steuern mitteilen und dort einen sogenannten Sperrvermerk beantragen, der dann dem Finanzamt bekanntgegeben wurde.

Die Informationskampagnen der Banken über das neue Kirchensteuer-Abgeltungsverfahren haben auch zu einer Reihe von Eingaben von irritierten Kunden bei uns geführt. Kunden wollten nicht, dass ihre Zugehörigkeit oder Nicht-Zugehörigkeit zu einer Religionsgemeinschaft bei ihrem Finanzinstitut bekannt wird, und sahen nicht ein, dass sie nun einem Handlungszwang zur Eintragung eines Sperrvermerks beim Bundeszentralamt für Steuern unterworfen werden.

Wir konnten die anfragenden Bürgerinnen und Bürger nur auf die neue gesetzliche Regelung und die Möglichkeit des Sperrvermerks hinweisen. Mehr, insbesondere eine vorherige Einwilligung der Bürgerinnen und Bürger, gibt das Gesetz nicht her.

Weitere Informationen dazu und einen Link zum Antrag für die Eintragung eines Sperrvermerks hält das Bundeszentralamt für Steuern auf seiner Homepage vor.

>>>
http://www.bzst.de/DE/Steuern_National/Kirchensteu-er/Info_Buerger/Informationen_fuer_Buerger_node.html

10.2 Bezahlverfahren mittels NFC-Technologie

Die NFC-Technologie für das kontaktlose Bezahlen mit EC-Karten wurde in einen datenschutzrechtlich und datensicherheitsmäßig vertretbaren Rahmen gebracht.

Die deutschen Datenschutzaufsichtsbehörden wurden darüber informiert, dass nun auch Banken für die EC-Karten das von Stadion- oder Veranstaltungskarten bekannte kontaktlose Bezahlverfahren mittels „Near Field Communication"-Technologie (NFC) einführen und haben sich daraufhin mit Fragen des Datenschutzes und der Datensicherheit für diese neue Bezahlungsform befasst.

Die Technik auf den EC-Karten für kontaktlose Geldkartenzahlungen per NFC unterscheidet sich von der bisherigen kontaktbehafteten EC-Geldkarte nur durch die kontaktlose Auslesemöglichkeit. Bei einer Zahlung muss die EC-Karte möglichst direkt an das Lesegerät gehalten werden, funktioniert aber auch noch in einem Abstand von etwa drei bis vier Zentimetern.

Bei den auf dem Geldkartenteil gespeicherten Daten haben sich keine Veränderungen ergeben. Gespeichert sind insbesondere der noch verfügbare Restbetrag, die letzten drei Aufladevorgänge und die letzten fünfzehn Zahlungsvorgänge mit der Terminalnummer des Händlers sowie Datum und Betrag des Kaufs. Ohne aktive Aufladung der NFC-fähigen Geldkarte können aus der Karte neben dem Jugendschutzmerkmal (unter/über 18 Jahre, wegen der Zigarettenautomaten) und dem Kartentyp (kontogebundene Karte) noch die Kartennummern ausgelesen werden.

Nicht lesbar ist die Karte, wenn sie der Kunde in einer Metall- oder Alu-Schutzhülle aufbewahrt. Eine solche geschützte Aufbewahrung der Karte kann wegen der nicht gänzlich auszuschließenden heimlichen Auslesbarkeit im Nahbereich (wenige Zentimeter) dann empfohlen werden, wenn auch momentan theoretisch eingeschätzte Risiken garantiert ausgeschlossen werden sollen.

Die Datenschutzaufsichtsbehörden legten Wert darauf, dass die Kunden von den Banken transparent über die Möglichkeiten und Risiken der NFC-fähigen Geldkarte (entsprechend § 6c BDSG) informiert werden (per Info-Blatt, im Internet, etc.) und so der Betroffene bewusst entscheiden kann, ob er überhaupt Geld auflädt, wann er die Karte mit sich trägt usw. Unter diesen Bedingungen gehen wir hier von ausreichenden Datenschutz- und Datensicherheitsmaßnahmen aus.

Für die Zukunft soll außerdem die Software so verändert werden, dass der Kunde selbst die NFC-Funktion aus- bzw. einschalten kann, so dass dann auch ohne Metallhülle eine Auslesbarkeit vom Kunden verhindert werden kann.

Zwischenzeitlich sind vermehrt auch Smartphones mit NFC-Bezahltechnologie auf dem Markt. Die dadurch entstehenden ergänzenden Sicherheitsrisiken, insbesondere bei Aufnahme von weiteren Angeboten auf die Karten – ggf. sogar von Drittanbieter – werden derzeit noch von den Datenschutzaufsichtsbehörden untersucht.

10.3 Ausweiskopien für Banken

Für die Banken bestehen spezialgesetzliche Regelungen zur Anforderung und Aufbewahrung von Ausweiskopien.

In unserem Tätigkeitsbericht 2011/2012 haben wir unter Kapitel 11.4 allgemein über die Zulässigkeit des Kopierens von Personalausweisen im Geschäftsleben informiert.

Immer wieder erreichen uns Anfragen wegen der Forderung von Banken nach Vorlage einer Ausweiskopie. Für Banken und andere dem Geldwäschegesetz unterliegende Finanzinstitute besteht die Pflicht der Identifizierung ihrer Vertragspartner anhand von Ausweisen und der Aufzeichnung der relevanten Daten.

Zur Erfüllung der Aufzeichnungspflicht nach § 8 des Geldwäschegesetzes ist auch die Anfertigung einer Kopie des Ausweisdokuments gesetzlich möglich. Nach dem Geldwäschegesetz prüfungs- und aufzeichnungspflichtig sind bei natürlichen Personen folgende Daten: Name, Geburtsort, Geburtsdatum, Staatsangehörigkeit, Anschrift sowie Art und Gültigkeit des Ausweises. Zu den übrigen im Ausweis enthaltenen Daten, wie Lichtbild, Größe, Augenfarbe, Ausweisnummer, besteht keine Aufzeichnungspflicht nach dem Geldwäschegesetz, so dass diese Daten mangels Erforderlichkeit von den Banken auch nicht verlangt werden dürfen. Um nur die erforderlichen Daten zu erheben, kann dies bei Kopien dadurch erfolgen, dass entweder per Schablone die nicht erforderlichen Daten abgedeckt oder danach geschwärzt werden.

Weil die gesetzliche Regelung zur Aufzeichnung einer Identitätsprüfung durch Ausweis-

kopien in § 8 Abs. 1 Satz 3 Geldwäschegesetz nicht zwingend ist, sondern daraus nur eine gesetzlich mögliche Verfahrensweise abgeleitet werden kann, genügt es für Banken auch, einen Ausweis durch persönliche Einsichtnahme zu prüfen und die Tatsache der Prüfung sowie die notwendigen Identifikationsdaten in sonstiger Weise festzuhalten (z. B. händisch zu notieren oder softwareseitig zu erfassen). Dies gilt insbesondere dann, wenn die Identität eines Kunden und dessen persönliche Daten bei der Bank aufgrund einer schon bestehenden Geschäftsbeziehung geprüft bzw. bekannt sind.

10.4 Umfang der Datenerhebung zu Geldanlagekonten (Familienstand)

Bei der Eröffnung von Geldanlagekonten ist es nicht erforderlich, dass Banken den Familienstand des Neukunden erheben und speichern.

In Kontoeröffnungsanträgen von Banken werden zur Vertragsdurchführung und aufgrund gesetzlicher Vorgaben, z. B. im Geldwäschegesetz, im Wertpapierhandelsgesetz oder im Kreditwesengesetz, eine Reihe von Daten des neuen Kunden abgefragt und bei der Bank gespeichert.

Ein Betroffener fragte uns, ob und aus welchem Grund er bei der Neueröffnung eines Geldanlagekontos auch seinen Familienstand gegenüber der Bank angeben muss.

Unsere Prüfung hat ergeben, dass hierfür aufgrund der obengenannten gesetzlichen Vorgaben Angaben zum Familienstand nicht erforderlich sind und damit auch nicht als Pflichtfeld in einem solchen Geldanlagekonto-Antrag abgefordert werden dürfen.

Dies kann allenfalls als freiwillige Angabe für eventuelle steuerliche Zwecke mancher Kunden (Steuerfreibeträge von gemeinsam veranlagten Ehegatten etc.) abgefragt werden.

11

Auskunfteien

11 Auskunfteien

11.1 Ausweiskopie bei Eigenauskünften

Auskunfteien können zur Identitätsüberprüfung grundsätzlich teilgeschwärzte Ausweiskopien fordern.

Immer wieder fragen uns betroffene Personen, ob das Verlangen von Auskunfteien nach einer Ausweiskopie zu einem Antrag auf Eigenauskunft über gespeicherte Daten nach § 34 BDSG datenschutzrechtlich zulässig ist.

Die von Auskunfteien teilweise geforderte Ausweiskopie bei der Beantragung von Eigenauskünften soll im Schwerpunkt die Identitätsprüfung bei namensgleichen oder namensähnlichen Personen erleichtern, denn die Eigenauskunft darf nur die richtige Person erhalten.

Des Weiteren geht es bei der Forderung nach einer Ausweiskopie aber auch darum, das Erschleichen von Bonitätsauskünften durch Unberechtigte zu erschweren (im Haushalt, in einer Wohngemeinschaft mitlebende Personen etc.), was leider in der Praxis auch immer wieder vorkommt (aus Neugier, in Trennungsfällen, bei Streitigkeiten usw.) und soweit wie möglich vermieden werden muss. Weil eine Ausweiskopie regelmäßig nur der Ausweisinhaber und damit der Berechtigte für eine Selbstauskunft nach § 34 BDSG vorlegen kann, ergibt sich daraus eine zusätzliche Sicherheit für Wirtschaftsauskunfteien zur Abwehr von Missbrauch.

Für die Identifikation nicht notwendige Daten (wie z. B. Größe, Augenfarbe, Ausweisnummer, Bild, Unterschrift) können in der Ausweiskopie geschwärzt bzw. beim Kopieren abgedeckt werden.

Die Datenschutzaufsichtsbehörden und Auskunfteien haben darüber hinaus in einer Besprechung schon im Februar 2011 Einvernehmen darüber erzielt, dass jedenfalls in folgenden Fallgruppen grundsätzlich auf die Vorlage einer Ausweiskopie verzichtet wird:

- Der Betroffene macht seinen Auskunftsanspruch nach § 34 BDSG in einem zeitlichen Zusammenhang zu einer vorherigen Benachrichtigung nach § 33 BDSG geltend (bis zu vier Wochen nach Benachrichtigung).
- Die Auskunftei hat keine Bonitäts- oder sonstigen Inhaltsdaten (Negativ- oder Positivdaten) zu der betroffenen Person gespeichert.

11.2 Verwendung der Anschrift zur Bildung eines Scorewerts

Das Einbeziehen von Anschriftendaten für eine Scorewert-Berechnung ist gesetzlich nicht verboten.

Während örtliche Unternehmen aufgrund der bisherigen Geschäftsbeziehungen und der örtlichen Kenntnisse meist eine ausreichende eigene Datenbasis für die Bewertung der Bonität eines Verbrauchers haben, liegen bei Online-Unternehmen oft keinerlei Vorinformationen zu Bestellern vor. Online-Unternehmen ziehen deshalb bei finanziellen Ausfallrisiken, z. B. bei Warenlieferung gegen offene Rechnung, bei Vorleistung mittels Energiebelieferung oder Telekommunikationsdienstleistungen, regelmäßig Auskunfteien-Informationen in maßgeblicher Weise zu Rate. Einen sekundenschnellen Überblick im Rahmen eines Onlinekontakts bieten sog. Scorewerte, die von Auskunfteien als Prognosewert für die Wahrscheinlichkeit eines Zahlungsausfalls anhand eines mathematisch-statistischen Verfahrens berechnet werden.

Immer wieder fragen uns von Scorebewertungen der Auskunfteien betroffene Personen, ob und inwieweit auch die aus der Anschrift erschließbare Art der Wohnung und des Wohnumfelds für eine Bonitätsscore-Berechnung herangezogen werden darf.

Das BDSG lässt in § 28b auch die Verwendung von Anschriftendaten für die Berechnung von Scorewerten grundsätzlich zu. Voraussetzung dabei ist, dass dafür nicht ausschließlich Anschriftendaten genutzt und die Verbraucher über eine solche Art der Scoreberechnung unterrichtet werden, z. B. mittels der Geschäftsbedingungen des angestrebten Vertragspartners.

Liegt ein Scorewert einer Auskunftei nach Meinung der betroffenen Person „voll daneben", ist manchmal eine Personenverwechslung bei Namensgleichen am gleichen Wohnort der Hintergrund. In solchen Fällen wurden wir von betroffenen Personen eingeschaltet, um schnellstmöglich für eine Datenberichtigung zu sorgen.

Nicht immer sind solche Verwechslungsfälle mit entsprechender Sorgfalt von vorne herein vermeidbar, z. B. wenn Vater und Sohn den gleichen Vornamen haben und unter gleicher Anschrift wohnen oder wenn sonst Namensgleiche auch noch zufällig das gleiche Geburtsdatum haben.

Führt allerdings im Schwerpunkt das Wohnumfeld schon zu einem schlechteren Scorewert, z. B. nach dem Umzug einer Person, so ist die Geeignetheit des Scoreberechnungsverfahrens grundsätzlich zu hinterfragen.

12

Werbung und Adressenhandel

12 Werbung und Adressenhandel

12.1 Anwendungshinweise Werbung und Adresshandel

Die Anwendungshinweise der Aufsichtsbehörden wurden inzwischen wesentlich erweitert.

Die Ad-hoc-Arbeitsgruppe „Werbung und Adresshandel" der Datenschutzaufsichtsbehörden (siehe dazu unseren 5. Tätigkeitsbericht 2011/2012, Kapitel 10.2) hat sich in weiteren jeweils zweitägigen Sitzungen 2013 und 2014 unter unserer Leitung auch mit Ergänzungen der veröffentlichten Anwendungshinweise zu den Datenschutzvorschriften über den Umgang mit personenbezogenen Daten für werbliche Zwecke befasst, die jetzt mit dem Stand September 2014 veröffentlicht wurden.

> > >
http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/Anwendungshinweise_Werbung.pdf

12.2 Verwendung von aus dem Internet stammenden Kontaktdaten (Homepage-Impressum)

Die öffentliche Zugänglichkeit der Pflichtangaben eines Homepage-Impressums erlaubt nicht automatisch deren Nutzung zu Werbezwecken.

Verbraucher, aber auch Unternehmen und Selbständige, klagen bei uns immer wieder darüber, dass die von ihnen im Homepage-Impressum einzutragenden Pflichtangaben zur postalischen und elektronischen Erreichbarkeit dort abgegriffen und für werbliche Kontaktaufnahmen missbraucht werden.

Für die Verwendung von aus dem Homepage-Impressum erlangten Postadressdaten von Verbrauchern gibt es in der maßgeblichen Spezialvorschrift von § 28 Abs. 3 BDSG keine datenschutzrechtliche Erlaubnis zur Zusendung von Briefwerbung. Für die Postadressen von Unternehmen und Selbstständigen gilt diese Einschränkung wegen deren geschäftlicher Tätigkeit und der dort anderen Positionierung in der Öffentlichkeit nicht.

Für E-Mail-Werbung ist außerhalb von Bestandskundenbeziehungen sowohl bei Verbrauchern wie auch bei Unternehmen und Selbständigen Voraussetzung, dass eine ausdrückliche Einwilligung der betreffenden Person oder des betreffenden Gewerbetreibenden vorliegt. Die öffentliche Zugänglichkeit einer E-Mail-Adresse auf einer Homepage, z. B. bei den Pflichtangaben im Impressum, kann nicht als Einwilligung in eine Zusendung von E-Mail-Werbung gewertet werden (siehe hierzu auch den BGH-Beschluss vom 10.12.2009, Az. I ZR 201/07).

12.3 Politische Wahlwerbung

12.3.1 Unzulässige Wahlwerbung durch Vereine

Vereine müssen der Versuchung widerstehen, die Kontaktdaten ihrer Mitglieder zum Zweck der Versendung politischer Wahlwerbung zu nutzen oder an Außenstehende zu übermitteln.

Im Vorfeld der bayerischen Kommunalwahlen 2014 erreichte uns – wie inzwischen regelmäßig vor politischen Wahlen, insbesondere Kommunalwahlen – eine erhebliche Anzahl von Beschwerden im Zusammenhang mit der Versendung politischer Wahlwerbeschreiben per Post oder per E-Mail. Mehrere Beschwerden richteten sich gegen Vorstandsmitglieder von Vereinen, die sich gleichzeitig im Rahmen der Kommunalwahlen für politische Ämter bewarben. Funktionsträger in Vereinen verfügen häufig aufgrund ihrer spezifischen Vereinsfunktion über Adressdaten von Vereinsmitgliedern. So verschickte ein solcher Funktionsträger, der bei einer Wahl zum Stadtrat kandidierte, ein Wahlwerbeschreiben an zahlreiche Vereinsmitglieder und warb darin für seine Wahl mit dem

Argument, er werde im Stadtrat den Interessen des Vereins Gehör verschaffen. Datenschutzrechtlich stellt dies eine unzulässige zweckändernde Nutzung der Adressdaten der Mitglieder dar. Die Vereinsmitglieder stellen ihre Kontaktdaten dem Verein lediglich zur Erfüllung der (satzungsmäßig festgelegten) Vereinszwecke zur Verfügung. Die schutzwürdigen Interessen der Vereinsmitglieder stehen bei der nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG gebotenen Interessenabwägung einer Nutzung ihrer Daten durch den Verein oder durch einzelne Funktionsträger für Wahlwerbezwecke oder sonstige politische Zwecke entgegen. Dies gilt selbst dann, wenn der Werbende erklärt, er werde sich im Falle eines Wahlerfolgs z. B. im Gemeinderat für die Belange des Vereins einsetzen. Denn die gesetzlich definierten Aufgaben und die damit einhergehenden Entscheidungsbefugnisse kommunaler Mandatsträger reichen über die (satzungsmäßig definierten) Zwecke eines Vereins weit hinaus. Daher stellt die Nutzung der Adressdaten von Vereinsmitgliedern für Wahlwerbezwecke eine Zweckänderung dar, die so erheblich ist, dass sie von den Vereinsmitgliedern nicht hingenommen werden muss.

In den uns bekanntgewordenen Fällen dieser Art haben wir die betreffenden Vereine bzw. Vereinsfunktionäre nachdrücklich auf die Unzulässigkeit einer solchen Nutzung von Daten von Vereinsmitgliedern hingewiesen. Gibt ein Funktionsträger eines Vereins Daten von Vereinsmitgliedern an einen Außenstehenden weiter, läge darin sogar eine unzulässige Übermittlung personenbezogener Daten, die gemäß § 43 Abs. 2 Nr. 1 BDSG mit Geldbuße geahndet werden kann.

12.3.2 Zulässige personalisierte Wahlwerbung durch Parteien und andere Wahlvorschlagsträger

Immer noch nicht durchgängig bekannt ist offenbar die für Parteien und andere Träger von Wahlvorschlägen gesetzlich eröffnete Möglichkeit, sich im Vorfeld politischer Wahlen Adressdaten von Wahlberechtigten aus dem Melderegister zu beschaffen.

Mehrere Beschwerdeführer beschwerten sich auch im Vorfeld der Bayerischen Kommunalwahlen 2014 wieder über persönlich an sie adressierte postalische Wahlwerbung von Parteien oder einzelnen Kandidaten. Offensichtlich sind die einschlägigen gesetzlichen Vorschriften, die Parteien und anderen Wahlvorschlagsträgern ein solches Vorgehen erlauben, noch nicht durchgängig in der Bevölkerung bekannt.

Wir haben die Beschwerdeführer darauf hingewiesen, dass sich gemäß Art. 32 Abs. 1 des Bayerischen Meldegesetzes (BayMeldeG) Parteien, Wählergruppen und andere Träger von Wahlvorschlägen im Zusammenhang mit allgemeinen Wahlen und Abstimmungen auf staatlicher oder kommunaler Ebene in den sechs Monaten vor der Stimmabgabe aus dem Melderegister Namen und postalische Anschriften von Gruppen von Wahlberechtigten beschaffen dürfen, für deren Zusammensetzung das Lebensalter der Betroffenen bestimmend ist (sog. Gruppenauskünfte). Die Parteien und Träger von Wahlvorschlägen machen von dieser gesetzlichen Möglichkeit offenbar regen Gebrauch und verschicken postalische Werbung an die Betroffenen. Die Erhebung, Nutzung und Verarbeitung der Daten in diesem Rahmen stellt daher keinen datenschutzrechtlichen Verstoß dar.

Möchte ein Betroffener keine persönlich adressierte Wahlwerbung, so hat er die Möglichkeit, einen entsprechenden Widerspruch bei der Meldebehörde einzulegen, worauf er von der Meldebehörde bei der Anmeldung hingewiesen werden muss (Art. 32 Abs. 2 Satz 1 und 2 BayMeldeG).

Hierzu haben wir im April 2014 auch eine Presseerklärung auf unserer Webseite veröffentlicht.

> > >
http://www.lda.bayern.de/lda/datenschutzaufsicht/p_archiv/2014/pm006.html

12.3.3 Unzulässige Wahlwerbung gegenüber Unterstützern eines Bürgerbegehrens

Geht aus der Gruppe der Initiatoren eines kommunalen Bürgerbegehrens später eine Gruppierung hervor, die einen Wahlvorschlag (Kandidatenliste) zur Teilnahme an den Kommunalwahlen einreicht, dürfen die Adressdaten der Unterstützer des Bürgerbegehrens nicht dazu verwendet werden, an diese Personen Wahlwerbung für den betreffenden Wahlvorschlag zu verschicken.

Bereits in unserem Tätigkeitsbericht 2006 (dort Kapitel 13.2) hatten wir die Frage behandelt, ob Personen, die ein Bürgerbegehren initiiert haben, die Adressdaten der Unterstützer des Bürgerbegehrens dazu verwenden dürfen, an die Unterstützer Werbung für den Bürgerentscheid zu verschicken, der durch das Bürgerbegehren durchgesetzt worden ist. Wir haben diese Frage bejaht. Denn ein Bürgerbegehren ist gerade darauf gerichtet, über das betreffende Anliegen die Durchführung eines Bürgerentscheids durchzusetzen. Daher wird man bei den Unterstützern des Bürgerbegehrens grundsätzlich annehmen dürfen, dass sie ein Interesse haben, dem mit dem Bürgerbegehren verfolgten Anliegen zur Durchsetzung zu verhelfen; hierzu dient gerade der Bürgerentscheid. Es kann daher davon ausgegangen werden, dass bei diesen Personen keine überwiegenden schutzwürdigen Interessen einer Nutzung ihrer Adressdaten zum Zweck der Werbung für den Bürgerentscheid entgegenstehen, so dass die Nutzung insoweit nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig ist.

Anders lag der Fall nun bei einer Eingabe, die uns im Vorfeld der Kommunalwahlen 2014 erreichte. In diesem Fall hatte es in einer Gemeinde in der Vergangenheit ein Bürgerbegehren gegeben, das seinerzeit von einer Bürgerinitiative initiiert worden war und in einen Bürgerentscheid gemündet hatte. Parallel zu diesem Bürgerentscheid schlossen sich einige der Initiatoren des Bürgerbegehrens im Hinblick auf die anstehenden Kommunalwahlen 2014 zu einer Wählergruppe zusammen, die einen Wahlvorschlag (Kandidatenliste) für die Kommunalwahlen einreichte und auch einen Kandidaten für das Bürgermeisteramt benannte (nach bayerischem Kommunalwahlrecht können Wahlvorschläge von Parteien oder von sog. Wählergruppen eingereicht werden, wobei als Wählergruppen jede Vereinigung oder Gruppe natürlicher Personen in Betracht kommt, deren Ziel es ist, sich an den Kommunalwahlen zu beteiligen).

Der Kandidat für das Bürgermeisteramt war seinerzeit einer der Initiatoren des Bürgerbegehrens gewesen. Die Adressdaten der Unterstützer des Bürgerbegehrens waren bei ihm augenscheinlich noch vorhanden. Der Kandidat für das Bürgermeisteramt griff nun im Vorfeld der Kommunalwahlen auf diese Adressdaten zurück und verschickte an die damaligen Unterstützer des Bürgerbegehrens Wahlwerbung für sich selbst sowie für den Wahlvorschlag (Kandidatenlisteliste), dem er angehörte. Mehrere der so Angeschriebenen beschwerten sich bei uns über diese Nutzung ihrer Daten. Der von uns zur Stellungnahme aufgeforderte Bewerber argumentierte, er und die von ihm angeführte Liste (Wahlvorschlag) seien faktisch aus dem Kreis der Initiatoren des Bürgerbegehrens hervorgegangen. Er und weitere der damaligen Initiatoren hätten sich nunmehr dazu entschieden, sich als „politische Gruppierung" mit einer Kandidatenliste um Sitze im Gemeinderat sowie um das Bürgermeisteramt zu bewerben, um auf diese Weise durch Mitarbeit in den kommunalen Organen gerade auch das ursprüngliche Anliegen des Bürgerbegehrens weiter zu befördern.

Wir haben die Nutzung der Adressdaten als unzulässig bewertet. Auch wenn die Argumentation des Bewerbers auf den ersten Blick eine gewisse Plausibilität zu haben scheint, stehen die schutzwürdigen Interessen der angeschriebenen Unterstützer des Bürgerbegehrens bei der nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG gebotenen Interessenabwägung der Nutzung ihrer Adressdaten zum Zwecke der Wahlwerbung entgegen. Dies gilt auch unter Berücksichtigung der vom Kandidaten für das Bürgermeisteramt vorgetragenen Argumente. Die Tatsache, dass dieser und weitere Personen, die auf der von ihm angeführten Liste bei den Kom-

munalwahlen kandidierten, seinerzeit zu den Initiatoren des Bürgerbegehrens gehört hatten, reicht nicht aus, um die Nutzung der Adressdaten der damaligen Unterstützer des Bürgerbegehrens für Zwecke der Wahlwerbung legitimieren zu können. Denn im Unterschied zu dem sehr engen Sachzusammenhang, der zwischen einem Bürgerbegehren und einem daraus hervorgegangenen anschließenden Bürgerentscheid besteht (s. o.), ist die Verbindung zwischen einem Bürgerbegehren einerseits und den allgemeinen Kommunalwahlen andererseits nicht so eng, dass man unterstellen könnte, dass die Unterstützer des Bürgerbegehrens keine Einwände dagegen hätten, unter Nutzung ihrer Adressdaten gezielt Wahlwerbung für eine bestimmte Kandidatenliste oder einen Bürgermeisterkandidaten zu erhalten. Denn der Gegenstand eines Bürgerbegehrens ist grundsätzlich eine begrenzte einzelne Sachfrage, während bei den Kommunalwahlen die kommunalen Organe gewählt werden, denen anschließend die Entscheidungsbefugnisse über die gesamten kommunalpolitischen Angelegenheiten zukommen. Die Zuständigkeiten und Befugnisse eines Bürgermeisters und eines Gemeinderats gehen mithin über den Gegenstand eines einzelnen Bürgerbegehrens weit hinaus. Bei dieser Sachlage kann und darf nicht einfach unterstellt werden, dass diejenigen Personen, die ein Bürgerbegehren unterstützt haben, die „kommunalpolitische Agenda" als Ganzes derjenigen Personen unterstützen, die seinerzeit jenes Bürgerbegehren initiiert hatten, und daher grundsätzlich mit dem Erhalt persönlich adressierter Wahlwerbung für diese Kandidaten einverstanden wären. Der Umstand, dass sich mehrere der Unterstützer des Bürgerbegehrens gegen das Vorgehen des Bürgermeisterkandidaten bei uns beschwerten, ist letztlich ein Beleg für diese Interessenlage.

Gerade aus diesem Grund hatten wir bereits in unserem Tätigkeitsbericht 2006 (dort Kapitel 13.2) darauf hingewiesen, dass die Adressdaten der Unterstützer eines Bürgerbegehrens zwar noch zum Zwecke der Werbung für einen sich anschließenden Bürgerentscheid genutzt werden dürfen, nicht jedoch für andere Zwecke, und im Übrigen gelöscht werden müssen.

Unter Erläuterung dieser Argumente haben wir dem Kandidaten unsere datenschutzrechtliche Bewertung verdeutlichen können. Er hat zugesagt, die Daten der Unterstützer des Bürgerbegehrens für keine weitere Wahl- oder sonstige politische Werbung zu verwenden, sondern umgehend zu löschen.

13

Handel und Dienstleistung

13 Handel und Dienstleistung

13.1 Offener E-Mail-Verteiler

Die Versendung einer E-Mail mit einem für jeden offen einsehbaren Verteiler stellt in der Regel eine unzulässige Übermittlung personenbezogener Daten dar.

Insbesondere seit Veröffentlichung unserer Pressemitteilung vom 28.06.2013 über eine von uns verhängte Geldbuße wegen Verwendung eines offenen E-Mail-Verteilers erreichten uns immer wieder Beschwerden mit Hinweisen auf die Verwendung offener E-Mail-Verteiler durch Unternehmen und andere verantwortliche Stellen.

> > >
http://www.lda.bayern.de/lda/datenschutzaufsicht/p_archiv/2013/pm004.html

Meist handelte es sich um Gruppen-E-Mails, mit denen Unternehmen gleichgelagerte Kurzinformationen an einen mehr oder minder großen Kreis von Kunden versandten, in einem Fall beispielsweise eine Eingangsbestätigung, in einem anderen Fall Weihnachtsgrüße.

Sofern die E-Mail-Adresse personenbezogen ist, stellt auch der Inhalt der E-Mail – d. h. die Mitteilung als solche – häufig ein personenbezogenes Datum dar. Durch die Versendung von E-Mails mit offen einsehbarem Verteiler werden die Adressen aller Empfänger allen anderen Empfängern bekannt gegeben, womit – wie aus den bei uns eingegangenen Eingaben ersichtlich ist – nicht jeder einverstanden ist. Die Versendung einer Sammel-E-Mail an einen offenen E-Mail-Verteiler stellt in diesen Fällen eine unzulässige Übermittlung personenbezogener Daten im Sinne des BDSG an jeweils alle anderen Empfänger dar.

Ein solcher Verstoß kann grundsätzlich mit einer Geldbuße geahndet werden (§ 43 Abs. 2 Nr. 1 BDSG – unbefugte Verarbeitung personenbezogener Daten, die nicht allgemein zugänglich sind). Wir haben inzwischen in mehreren Fällen dieser Art Geldbußen verhängt. Hierbei ist zu beachten, dass Geldbußen grundsätzlich – sofern (zumindest) fahrlässig gehandelt wurde – gegen die Person zu verhängen sind, die in eigener Person den Verstoß begangen hat, d. h. selbst die E-Mail versandt hat. Jedoch sind gemäß den Maßgaben des Ordnungswidrigkeitenrechts auch Geldbußen gegen die betreffenden Unternehmen möglich, sofern festgestellt wird, dass mangelhafte innerbetriebliche organisatorische Vorkehrungen maßgeblich dazu beigetragen haben, dass es zu der Versendung mit offenem Verteiler gekommen ist.

13.2 Herausgabe von Gesellschafterlisten mit Kontaktdaten von Anlegern (oft auf Grund gerichtlicher Entscheidung)

Sofern keine Anhaltspunkte für eine unzulässige Rechtsausübung (§ 242 BGB) oder Schikane (§ 226 BGB) vorliegen, sind Kontaktdaten von Gesellschaftern einer Personengesellschaft grundsätzlich an Mitgesellschafter herauszugeben.

Mitgesellschafter meist von größeren Publikumskommanditgesellschaften haben sich an uns mit der Bitte gewandt, sie dabei zu unterstützen, dass ihre Gesellschafterstellung gegenüber anderen Gesellschaftern bzw. deren Rechtsanwälten nicht bekannt gegeben wird.

Wir orientieren uns dabei an der Rechtsprechung des Bundesgerichtshofs (BGH), der in zwei Urteilen vom 05.02.2013 (Az. II ZR 134/11 und II ZR 136/11) ausgeführt hat, dass jeder Gesellschafter einer Publikumsgesellschaft grundsätzlich Anspruch darauf hat, von der Gesellschaft die Namen und Adressdaten seiner Mitgesellschafter zu erhalten, und zwar sowohl die Daten der unmittelbaren Gesellschafter als auch von etwaigen Treugebern, die lediglich mittelbar – über einen Treuhänder – an der Gesellschaft beteiligt sind. Das bedeutet, dass die Gesellschaft verpflichtet ist, Namen und (postalische) Adressen von Mitgesellschaftern in solchen Fällen herauszugeben.

Der BGH hat in den vorgenannten Urteilen zur Begründung ausgeführt, dass bei einem Gesellschaftsvertrag einer Personengesellschaft bzw. Personenhandelsgesellschaft das Recht, seine Vertragspartner zu kennen, ein grundlegendes Recht darstellt. Dieses folgt als unentziehbares mitgliedschaftliches Recht aus dem durch den Gesellschaftsvertrag zwischen den Gesellschaftern begründeten Vertragsverhältnis als solchem. Der BGH hat ein schützenswertes Geheimhaltungsinteresse der Mitgesellschafter untereinander im Hinblick auf ihre jeweilige Identität und ihre Beteiligungsverhältnisse grundsätzlich verneint. Das Auskunftsbegehren eines Gesellschafters auf Mitteilung der Namen und Anschriften der Mitgesellschafter ist nur durch das Verbot der unzulässigen Rechtsausübung nach § 242 BGB und das Schikaneverbot gemäß § 226 BGB begrenzt.

Im Berichtszeitraum erreichten uns mehrere Anfragen von Publikums-KGs, die von einzelnen Gesellschaftern zur Nennung von Namen und Adressdaten aller Mitgesellschafter aufgefordert worden waren. Angesichts der o. g. Rechtsprechung teilten wir in solchen Fällen regelmäßig mit, dass die Herausgabe dieser Daten an den einzelnen Gesellschafter grundsätzlich keinen datenschutzrechtlichen Verstoß darstellt.

13.3 Datenschutz rund um den Personalausweis

Zahlreiche an uns gerichtete Eingaben betrafen datenschutzrechtliche Fragen zum Personalausweis. Dabei ging es meist um das Kopieren des Personalausweises, doch gab es auch andere Fragestellungen.

13.3.1 Kopieren des Personalausweises häufig unzulässig

Das Personalausweisgesetz schränkt die Zwecke zulässiger Verwendungen des Personalausweises ein: Gemäß § 20 Abs. 1 PAuswG darf der Inhaber den Personalausweis gegenüber nicht-öffentlichen Stellen nur zur Legitimation und zur Identitätsfeststellung verwenden. Das in der Praxis immer wieder zu beobachtende Kopieren des Personalausweises durch Unternehmen ist bei näherer Betrachtung jedenfalls häufig unzulässig.

Ein datenschutzrechtlicher „Dauerbrenner" ist das Kopieren von Personalausweisen. Aus mehreren Branchen erreichten uns Beschwerden darüber, dass Unternehmen von Kunden eine Kopie des Personalausweises forderten oder selbst anfertigten. In einem Fall informierte uns ein Hotelgast, dass das Hotel eine Kopie seines Personalausweises anfertigen wollte. In einem anderen Fall wurden wir darüber verständigt, dass ein Autohaus, das auch Fahrzeuge vermietet, offenbar Personalausweise von Fahrzeugmietern kopierte.

Bei genauer Betrachtung dieser oder anderer Situationen, in denen es in der Praxis offenbar immer wieder zum Kopieren von Personalausweisen kommt, zeigt sich, dass das Kopieren jedenfalls in vielen dieser Fälle datenschutzrechtlich unzulässig ist.

Das Personalausweisgesetz begrenzt die Zwecke zulässiger Verwendungen des Personalausweises: Gemäß § 20 Abs. 1 PAuswG darf der Inhaber den Personalausweis gegenüber nichtöffentlichen Stellen nur zur Legitimation und zur Identitätsfeststellung verwenden. Mit Blick darauf kann festgehalten werden: Wenn der Ausweisinhaber bei der Stelle, die die Identifizierung durchführen möchte, persönlich vorspricht und somit den Personalausweis zur Identifizierung vorlegen kann, ist das Kopieren des Ausweises zum Zwecke der Identifizierung oder der Legitimation nicht erforderlich und daher unzulässig. Ausnahmen gelten nur in den Fällen, in denen eine spezialgesetzliche Vorschrift ausdrücklich das Kopieren des Personalausweises zulässt, etwa gemäß dem Geldwäschegesetz (zu diesen Spezialfällen siehe unten 13.3.2).

Hat ein Unternehmen oder eine andere „verantwortliche Stelle" einen rechtlich tragfähigen Grund und damit eine Rechtsgrundlage, um Identitätsdaten des Betroffenen noch über den Identifizierungsvorgang hinaus zu speichern

(z. B. weil die Daten zur Durchführung eines Vertragsverhältnisses mit dem Betroffenen benötigt werden und die Speicherung daher nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG zulässig ist), so rechtfertigt auch dieser Umstand nicht das Kopieren des Personalausweises des Betroffenen. Denn das Unternehmen könnte auch in diesen Fällen – sofern der Ausweisinhaber anwesend ist und den Ausweis vorzeigt – die benötigten Daten aus dem vorgezeigten Ausweis notieren, so dass auch insoweit kein Bedarf an einer Ausweiskopie als solcher besteht.

Daher ist das Kopieren des Personalausweises oder das Verlangen einer solchen Kopie zwecks Identifizierung grundsätzlich nur in solchen Fällen datenschutzrechtlich zulässig, in denen der Ausweisinhaber nicht persönlich anwesend ist (zu den wenigen Ausnahmen, etwa nach dem Geldwäschegesetz, siehe unten in Kapitel 13.3.2.). Der Ausweisinhaber ist in solchen Fällen von der verantwortlichen Stelle allerdings darauf hinzuweisen, dass er die Daten, die nicht zur Identitätsprüfung benötigt werden (z. B. Seriennummer, Zugangsnummer), auf der Kopie schwärzen kann; denn solche Daten sind zur Identitätsprüfung gerade nicht „erforderlich" im Sinne von § 28 Abs. 1 Satz 1 Nr. 1 oder Nr. 2 BDSG. Zur Identitätsprüfung genügen regelmäßig der Vor- und Nachname, das Geburtsdatum und die postalische Adresse.

Sofern eine Personalausweiskopie nach dem oben Gesagten überhaupt angefordert bzw. erstellt werden darf – d. h. im Wesentlichen (nur) soweit der Ausweisinhaber nicht persönlich anwesend ist –, ist sie nach durchgeführter Identifizierung zu vernichten. Die häufig zu beobachtende Praxis, die Kopie aufzubewahren, um die Durchführung der Identifizierung nachzuweisen („zu dokumentieren"), ist, soweit keine gesetzlichen Ausnahmevorschriften dies ausnahmsweise erlauben, unzulässig. Um die Identifizierung zu dokumentieren, genügt stattdessen in aller Regel die Anfertigung eines Vermerks, wonach die Identifizierung unter Vorlage des Personalausweises oder einer Ausweiskopie durchgeführt worden ist. Darf die verantwortliche Stelle bestimmte Daten des Ausweisinhabers über den Identifizierungsvorgang hinaus speichern (z. B. nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG, s.o.), kann sie diese Daten aus der erhaltenen Ausweiskopie notieren und die Kopie selbst anschließend vernichten. Das Behalten der Kopie als solcher ist jedenfalls dann unzulässig, wenn in der Kopie außer denjenigen Daten des Inhabers, die die verantwortliche Stelle über den Identifizierungsvorgang hinaus noch (z. B. gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG) speichern darf, weitere Daten (ungeschwärzt) enthalten sind, was in der Praxis häufig der Fall sein wird.

Diese Grundsätze haben wir bei Bearbeitung der bei uns eingegangenen Beschwerden angewendet. Dem eingangs erwähnten Autohaus, das Fahrzeuge vermietete, haben wir etwa mitgeteilt, dass sie Personalausweise von persönlich anwesenden Fahrzeugmietern nicht kopieren darf.

13.3.2 Kopieren des Personalausweises zur Erfüllung von Anforderungen nach dem Geldwäschegesetz

Einige gesetzliche Spezialvorschriften erlauben für bestimmte Zwecke ausdrücklich das Kopieren des Personalausweises, darunter die Vorschriften des Geldwäschegesetzes (GwG). Lehnt der Ausweisinhaber das Kopieren ab, muss der Verpflichtete jedoch die nach dem GwG zu erhebenden und zu dokumentierenden Daten auf andere Weise speichern.

Mehrere Immobilienmakler wandten sich mit der Frage an uns, ob es datenschutzrechtlich zulässig sei, zur Erfüllung von Anforderungen nach dem Geldwäschegesetz die Personalausweise von Interessenten zu kopieren.

Einige (wenige) gesetzliche Spezialvorschriften erlauben für bestimmte Lebenssachverhalte ausdrücklich die Anfertigung einer Personalausweiskopie durch nicht-öffentliche Stellen. Hierzu gehört – mit einer beachtlichen Praxisrelevanz – § 8 Abs. 1 Satz 3 GwG. Nach § 3 Abs. 2 Satz 1 Nr. 1 GwG sind u. a. Immobilienmakler, die meisten Kredit- und Finanzdienstleistungsinstitute, Lebensversicherungen und eine Reihe weiterer Stellen verpflichtet, ihre Vertrags-

partner (u. a.) bei Begründung einer Geschäftsbeziehung zu identifizieren. Für bayerische Immobilienmakler gilt diese Verpflichtung gemäß einem Auslegungshinweis des Bayerischen Staatsministeriums des Innern für Bau und Verkehr (IC2 1116.31.18, Stand Februar) beim An- und Verkauf von Immobilien. Der Auslegungshinweis ist auf der nachfolgend genannten Webseite abrufbar.

> > >
http://www.stmi.bayern.de/sus/inneresicherheit/sicherheitundordnung/geldwaeschegesetz/index.php

Ist der Vertragspartner eine natürliche Person, muss der Verpflichtete zur Erfüllung der Identifizierungspflicht Name, Geburtsort, Geburtsdatum, Staatsangehörigkeit und Anschrift seines Vertragspartners erheben (§ 4 Abs. 3 Nr. 1 GwG) und aufzeichnen (§ 8 Abs. 1 Satz 1 GwG). Das Gesetz erlaubt ausdrücklich, diese Aufzeichnung durch Anfertigung einer Kopie des Ausweises vorzunehmen (§ 8 Abs. 1 Satz 3 GwG). Die Aufzeichnungen – d. h. ggf. die Ausweiskopie – dürfen ausdrücklich auch auf einem Bildträger oder sonstigen Datenträger gespeichert werden (§ 8 Abs. 2 Satz 1 GwG).

Somit eröffnet § 8 Abs. 1 Satz 3 GwG die Möglichkeit, den Personalausweis zu Zwecken der Dokumentation der Erfüllung der Pflichten nach dem GwG zu kopieren und die Kopie aufzubewahren. Da die Aufzeichnung der o. g. Daten jedoch nach dem Gesetzeswortlaut auch in anderer Form als durch Anfertigung einer Ausweiskopie – z. B. durch Notieren der Daten – möglich ist, enthält die Vorschrift andererseits keine Pflicht, den Ausweis als solchen zu kopieren. Dies teilten wir auch den Immobilienmaklern mit, die sich an uns gewandt hatten. Die Verpflichtung zur Erhebung und Dokumentierung bezieht sich auf die in § 4 Abs. 3 Nr. 1 GwG genannten Daten, nicht auf eine Ausweiskopie als solche.

Daher muss der Verpflichtete z. B. für den Fall, dass der Ausweisinhaber das Kopieren seines Personalausweises ablehnt, die o. g. Daten aus dem (vorgezeigten) Ausweis einzeln erheben und notieren, um seiner gesetzlichen Verpflichtung zur Aufzeichnung der Daten nachzukommen.

13.3.3 Erheben der Seriennummer des Personalausweises durch Hotels

Hotels dürfen keine Seriennummern aus deutschen Personalausweisen oder Reisepässen erheben und speichern.

Einige Hotelgäste monierten, dass Hotels die Seriennummern ihres Personalausweises notiert hätten. Dies ist unzulässig. Das Bayerische Gesetz über das Meldewesen (BayMeldeG) gibt in den Artikeln 23 und 24 abschließend die personenbezogenen Daten vor, die Beherbergungsbetriebe (z. B. Hotels) von ihren Gästen erheben müssen. Die Hotelgäste müssen die entsprechenden Daten handschriftlich in einen Meldeschein eintragen. Andere als die im Gesetz genannten Daten dürfen vom Beherbergungsbetrieb nicht erhoben werden.

Zu den Daten, die der Beherbergungsbetrieb erheben muss, gehören Tag der Ankunft und der voraussichtlichen Abreise, Familienname, gebräuchlicher Vorname (Rufname), Tag der Geburt, Anschrift sowie Staatsangehörigkeit. Diese Daten sind vom Gast in den Meldeschein handschriftlich einzutragen (Art. 23 Abs. 2 Satz 1, Art. 24 Abs. 2 Satz 1 BayMeldeG). Die Seriennummer ist im Gesetz nicht genannt und darf daher vom Beherbergungsbetrieb nicht aufgeschrieben oder anderweitig erhoben werden.

Eine allgemeine Verpflichtung zur Vorlage eines Identitätsdokuments gegenüber dem Hotel gibt es im bayerischen Melderecht im Übrigen nicht; lediglich für Ausländer gilt eine solche Vorlagepflicht (Art. 23 Abs. 3 BayMeldeG). Das Hotel hat in diesen Fällen die im Meldeschein gemachten Angaben mit denjenigen im Identitätsdokument zu vergleichen und etwaige Abweichungen auf dem Meldeschein zu vermerken.

Das Kopieren von Personalausweisen oder sonstiger Ausweisdokumente von Hotelgästen durch Hotels ist im Gesetz weder bei In- noch bei Ausländern vorgesehen und daher unzuläs-

sig. Im Berichtszeitraum gingen dennoch bei uns einige Beschwerden ein, aus denen sich ergab, dass hiergegen in der Praxis offenbar zumindest gelegentlich verstoßen wird. Den entsprechenden Fällen sind wir nachgegangen und haben dafür gesorgt, dass die betreffenden Hotels künftig keine Personalausweiskopien mehr anfertigen.

13.3.4 Hinterlegung des Personalausweises als Pfand

Der Personalausweis darf nicht – grundsätzlich auch nicht „freiwillig" – als Pfand hinterlegt werden.

Gelegentlich erreichten uns Beschwerden über Unternehmen, die von Kunden das Hinterlegen des Personalausweises als Pfand verlangt hatten, so etwa im Falle einer Diskothek. Dies ist nach dem ausdrücklichen Gesetzeswortlaut unzulässig: Gemäß § 1 Abs. 1 Satz 3 PAuswG darf vom Inhaber nicht verlangt werden, den Personalausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam daran aufzugeben. In der Gesetzesbegründung (BT-Drs. 16/10489, S. 32) findet sich dazu die Aussage, dass auch eine freiwillige Abgabe des Ausweises an Dritte nicht erfolgen „sollte".

Im Ergebnis ist jedenfalls auch das (mehr oder minder) „freiwillige" Aus-der-Hand-Geben des Personalausweises zu Pfandzwecken unzulässig. Hierfür spricht auch der Wortlaut von § 20 Abs. 1 PAuswG, wonach der Inhaber den Personalausweis lediglich als Identitätsnachweis oder Legitimationspapier verwenden darf; die Verwendung als Pfand gehört ersichtlich nicht zu diesen Zwecken. Vor dem Hintergrund, dass gerade der „neue" Personalausweis missbräuchlich durch Dritte verwendet werden könnte, sollte dieses Verbot ernst genommen werden. Denn der neue Personalausweis beinhaltet eine kontaktlose Schnittstelle, die für Authentifizierungs- und Signaturzwecke verwendet werden kann. Hat ein Unbefugter Gewahrsam am Personalausweis, besteht die Gefahr eines Missbrauchs dieser Funktionen.

13.4 Versendung von Kontodaten mit unverschlüsselter E-Mail bei Information zur Umstellung auf SEPA-Verfahren

Bankverbindungsdaten von Kunden dürfen aus Sicherheitsgründen nicht per unverschlüsselter E-Mail versandt werden.

Im Berichtszeitraum erhielten wir eine Reihe von Beschwerden über Unternehmen aus unterschiedlichsten Branchen im Zusammenhang mit der Versendung von Kontoverbindungsdaten per unverschlüsselter E-Mail. Anfang des Jahres 2014 anlässlich der endgültigen Umstellung auf das sog. SEPA-Verfahren im unbaren Zahlungsverkehr häuften sich solche Vorfälle, sei es, dass ein Hausverwalter einer Wohnungseigentümergemeinschaft eine E-Mail mit den Bankverbindungsdaten von Wohnungseigentümern zur Überprüfung der Daten und Rückmeldung versandte, oder dass ein Onlineshop oder ein Internet-Domainbetreiber seine jeweiligen Kunden per E-Mail über die SEPA-Umstellung informieren wollte und dabei die Bankverbindungsdaten im Klartext zur Überprüfung versandte.

Nach § 9 BDSG einschließlich Anlage hat eine Stelle, die selbst oder im Auftrag personenbezogene Daten erhebt, verarbeitet oder nutzt, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG und insbesondere der in der Anlage zu § 9 BDSG dazu genannten Anforderungen zu gewährleisten. Dazu gehört u. a., personenbezogene Daten so weit wie möglich vor unberechtigten Zugriffen Dritter zu schützen (vgl. Satz 2 Nr. 4 der Anlage zu § 9 BDSG). Bei der Übertragung von personenbezogenen Daten per unverschlüsselter E-Mail handelt es sich um ein unsicheres Verfahren, da an jedem an der Internetkommunikation beteiligten Knotenpunkt die Inhalte einer E-Mail gelesen werden können. Zudem werden E-Mails sowohl beim E-Mail-Provider des Absenders als auch des Empfängers im Klartext gespeichert. Damit können sämtliche Daten, welche auf diesem Weg versendet werden, von potentiell Unbefugten gelesen werden.

Nach § 9 Satz 2 BDSG sind technische und organisatorische Maßnahmen nur erforderlich, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Es kommt also auch immer darauf an, welche personenbezogenen Daten in der E-Mail enthalten sind. Da es sich gerade bei Bankdaten um missbrauchsanfällige und daher eher sensible Daten handelt, müssen diese entweder per verschlüsselter E-Mail (Inhaltsverschlüsselung zum Beispiel mit PGP oder S/MIME) oder aber per Post im verschlossenen Umschlag zugesandt werden, um einen angemessenen Schutz zu gewährleisten. Darauf haben wir die betreffenden Unternehmen nachdrücklich hingewiesen.

13.5 Fahrzeugvermietung übermittelt Name und Adresse des Mieters zwecks Einzugs norwegischer Mautforderungen

Das Interesse des Fahrzeugvermieters, nicht auf Mautforderungen „sitzen zu bleiben", überwiegt gegenüber dem Anonymitätsinteresse des Fahrzeugmieters.

Eine Fahrzeugvermietung übermittelte Name und Adresse eines Fahrzeugmieters an eine (britische) Dienstleistungsgesellschaft, die mit dem Einzug von norwegischen Mautgebührenforderungen betraut ist. Der Mieter monierte, dass die Übermittlung nicht erforderlich gewesen sei; er argumentierte, dass die Mietwagenfirma stattdessen die Möglichkeit gehabt hätte, ihm – dem Mieter – die Rechnung des Dienstleisters zur Begleichung zukommen zu lassen.

Nach unserer Bewertung konnte die Übermittlung mit „berechtigten Interessen" der Mietwagenfirma gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG begründet werden. Unstreitig ist, dass der Mieter nicht erwarten kann, dass das Mietwagenunternehmen die Mautgebühren trägt. So war denn auch in den Allgemeinen Geschäftsbedingungen des Mietwagenunternehmens klargestellt, dass Mautgebühren vom Mieter zu tragen sind. Die AGB enthielten aber keine näheren Angaben über das Verfahren zum Umgang mit solchen Mautrechnungen. Nach unserer Auffassung hat der Fahrzeugmieter jedenfalls keinen Anspruch darauf, dass die Mietwagenfirma (z. B. norwegische) Mautrechnungen so bearbeitet, dass sie die Rechnung an den Mieter mit dem Ersuchen um Begleichung weiterleitet; dies wäre für das Unternehmen, wie von diesem nachvollziehbar dargestellt wurde, mit einem deutlichen Mehraufwand verbunden, da das Unternehmen dann im Nachgang u. a. kontrollieren müsste, ob der Mieter die Rechnung beglichen hat. Daher war das Vorgehen dergestalt, dass das Mietwagenunternehmen dem Mautdienstleister Name und Adresse des Mieters nennt, datenschutzrechtlich vertretbar. Das Interesse des Mieters, gegenüber dem Mautdienstleister anonym zu bleiben, wiegt demgegenüber nicht so schwer, dass er von der Mietwagenfirma ein Vorgehen verlangen könnte, bei dem seine zum Forderungseinzug benötigten Daten nicht an den Mautdienstleister übermittelt werden.

Wir haben allerdings vom Mietwagenunternehmen verlangt, die Kunden in seinen AGB gemäß § 4 Abs. 3 Satz 1 Nr. 3 BDSG („Information über Kategorien von Datenempfängern") transparent darüber zu informieren, dass in solchen Fällen Name und Adresse des Fahrzeugmieters zum Zweck der Durchsetzung von Mautforderungen übermittelt werden. Fahrzeugmieter dürfen über die Übermittlung ihrer Daten anlässlich der Bearbeitung solcher Mautforderungen nicht im Dunkeln gelassen werden. Eine entsprechende Information fehlte in den AGB des Unternehmens. Sie wurde seitens des Unternehmens inzwischen dort ergänzt.

13.6 Veraltete Eigentümerdaten bei Energieversorgungsunternehmen

Die gesetzlich geforderte rechtliche Trennung von Vertrieb und Netz bei Energieversorgungsunternehmen führte zu einer Trennung der Datenbestände bei den betroffenen Unternehmen. Hierbei kann es für den Kunden bei Vertragskündigun-

gen durchaus noch zu kuriosen Situationen kommen.

Ein Eingabeführer beschwerte sich bei uns darüber, dass er seit 2009 immer wieder von einem Energieversorgungsunternehmen Schreiben (Begrüßungsschreiben, Abrechnungen, Beendigungsmitteilungen und weitere Korrespondenz) erhalte, er aber dort niemals Kunde gewesen sei. Trotz mehrmaligen Kontakts per Telefon und E-Mail habe sich die Situation nicht geändert. Seine Aufforderungen, seine persönlichen Daten aus der Datenbank zu löschen, seien erfolglos geblieben.

Im Zuge unserer Sachverhaltsaufklärung stellte sich die Situation wie folgt dar:

Der Eingabeführer war als Eigentümer eines Hauses früher Kunde eines Energieversorgers gewesen und hatte daher mit diesem seinerzeit einen Belieferungsvertrag über Gas abgeschlossen. Dann verkaufte er das Haus und meldete sich bei dem Gasversorger ab. Der neue Eigentümer wählte einen anderen Versorger. Die im Rahmen des Vertragsverhältnisses hinterlegten Daten des alten Eigentümers wurden im Datenbestand gesperrt.

Aufgrund der vom Gesetzgeber durch das Energiewirtschaftsgesetz 2005 vorgegebenen rechtlichen Trennung von Vertrieb und Netz bei Energieversorgungsunternehmen wurde der Eigentümerwechsel nicht gesellschaftsübergreifend und damit nicht automatisch (auch) im Datenbestand des Netzbetreiber-Unternehmens umgesetzt. Die Trennung in Netzbetreiberunternehmen und Vertriebsunternehmen führte zu getrennten Datenbeständen. Der Eingabeführer hatte sich bei Verkauf des Hauses zwar bei seinem Versorgungsunternehmen (Vertriebsunternehmen) abgemeldet, nicht jedoch auch beim Netzbetreiber. Deshalb blieben seine Daten – als (in Wirklichkeit nicht mehr aktueller) Eigentümer des Objekts – beim Netzbetreiber gespeichert.

Kündigt ein Kunde seinen Liefervertrag, meldet der Altlieferant (Vertriebsunternehmen) dem Netzbetreiberunternehmen über einen von der Bundesnetzagentur festgeschriebenen und in der GeLi-Gas (Geschäftsprozesse Lieferantenwechsel – Gas) beschriebenen Prozess automatisiert eine Lieferabmeldung. Liegt für die Abnahmestelle kein anderweitiger neuer Liefervertrag vor, meldet der Netzbetreiber dem örtlichen Grundversorger im Rahmen des Ersatz- und Grundversorgungsprozesses („EoG-Prozess“) automatisiert die bei ihm zu der Verbrauchsstelle vorliegenden Daten, insbesondere den vermerkten Eigentümer. Der örtliche Grundversorger bestätigt gegenüber dem Netzbetreiber dann die Aufnahme der Belieferung im Rahmen der sog. Ersatz- bzw. Grundversorgung und stößt die vertrieblichen Folgeprozesse an, u. a. die Begrüßung des Kunden in der Grund- bzw. Ersatzversorgung.

Im vorliegenden Fall hatte sich der neue Eigentümer bei seinem Versorgungsunternehmen abgemeldet. Offenbar wurde für das Objekt kein anderweitiger Liefervertrag abgeschlossen, so dass der EoG-Prozess angestoßen wurde, d. h. die beim Netzbetreiber hinterlegten (nicht mehr den aktuellen Eigentumsverhältnissen entsprechenden) Daten des Eingabeführers wurden an den örtlichen Grundversorger zum Zwecke der Ersatzversorgung angemeldet. Infolgedessen erhielt der Eingabeführer ein Begrüßungsschreiben vom örtlichen Grundversorger. Da sich der Eingabeführer daraufhin beim Grundversorger beschwerte – da er nicht Eigentümer des Objekts sei –, wurde dort diese Anmeldung storniert. Mangels Kenntnis des beim Netzbetreiber noch vorhandenen divergierenden Datenbestandes wurde der Eingabeführer jedoch beim nächsten „Lauf“ des EoG-Prozesses erneut in die Grundversorgung angemeldet, weshalb es zu einem weiteren Begrüßungsschreiben kam.

Im Rahmen unseres Tätigwerdens konnte der beschriebene Datenschiefstand zwischen Vertrieb und Netzbetreiber bereinigt werden. Der Datenbestand auf Seiten des Netzbetreibers wurde berichtigt.

Ein datenschutzrechtlicher Verstoß war den beteiligten Unternehmen bei dieser Sachlage nicht vorzuwerfen. Ein gesellschaftsübergreifender Datenabgleich zwischen Vertriebsunternehmen und Netzbetreiber durfte nicht durchgeführt werden. Letztlich hätte sich der Eingabeführer bei Veräußerung seines Hauses auch

beim Netzbetreiber abmelden müssen. Der Eingabeführer wusste jedoch offenbar nichts davon, dass aus einer Gesellschaft inzwischen zwei geworden waren (Netzbetreiber und Versorger).

13.7 Übermittlung von Beratungsprotokollen von freien Finanzberatern an Finanzinstitute

Die Übermittlung des Beratungsprotokolls an Emittenten durch einen – freiberuflichen, also nicht in die Organisation des Emittenten direkt eingebundenen – Finanzanlagevermittler ist nur mit Einwilligung des Kunden zulässig.

Ein Finanzanlagevermittler ist an uns herangetreten und hat uns geschildert, dass Finanzanlagevermittler nach § 16 der Verordnung über die Finanzanlagenvermittlung (FinVermV) umfangreiche Informationen über ihre Kunden einholen müssten, anhand derer sie die Geeignetheit von Produkten für den jeweiligen Kunden einschätzen müssten. Nach § 18 FinVermV muss der Vermittler ein Beratungsprotokoll anfertigen, das die eingeholten Informationen des Kunden als Basis für die Anlageempfehlung enthält und die Arbeit des Beraters dokumentiert. Eine Abschrift des Protokolls ist dem Anleger zur Verfügung zu stellen.

Der Vermittler schilderte, dass einige Emittenten Anträge nur noch unter der Bedingung annehmen, dass ein firmeneigenes Protokoll, unterschrieben vom Kunden (entgegen § 18 Abs. 1 FinVermV), beim Emittenten eingereicht wird. Damit würden jedoch Kundendaten vom Vermittler an den Emittenten weitergegeben, die – jedenfalls in diesem Umfang – für den Vertragsabschluss mit dem Emittenten nicht erforderlich sind. Durch Zuleitung des Protokolls an den Emittenten erfährt dieser nicht nur das komplette Risikoprofil des Anlegers, sondern auch dessen detaillierte Vermögensaufstellung – unabhängig von der Höhe der im konkreten Einzelfall getätigten Investition.

Nach unserem Verständnis dient das Beratungsprotokoll den Finanzanlagevermittlern als Nachweis, dass sie den Anleger entsprechend seiner Anlageziele und seiner finanziellen Verhältnisse beraten haben. Das Protokoll muss daher beim Finanzanlagevermittler bleiben und eine Kopie dem Anleger ausgehändigt werden. Da im Protokoll viele Kundendaten enthalten sind, die nicht zum Vertragsschluss mit dem Emittenten erforderlich sind, wäre eine Übermittlung des Protokolls an den Emittenten grundsätzlich nur zulässig, wenn der Kunde darin eingewilligt hat. Die Einwilligung müsste der Formvorschrift nach § 4a BDSG genügen, erforderlich ist somit eine sog. informierte Einwilligung; der Kunde müsste daher über die Tatsache der Übermittlung an den jeweiligen Emittenten informiert werden und in diese Übermittlung durch eine Unterschrift einwilligen. Diese Einwilligung kann auf den Beratungsprotokollen selbst oder alternativ auf einem gesonderten Blatt eingeholt werden.

14

Internationaler Datenverkehr

14 Internationaler Datenverkehr

14.1 Binding Corporate Rules (BCR)

Abschluss dreier EU-weiter Verfahren zur Prüfung von konzernweiten Datenschutzregelungen zur konzerninternen Übermittlung personenbezogener Daten in Drittstaaten (Binding Corporate Rules) unter Federführung des BayLDA.

In den Jahren 2013 und 2014 waren wir erstmalig federführende Datenschutzbehörde in mehreren EU-weiten Verfahren zur Prüfung so genannter verbindlicher Unternehmensrichtlinien (Binding Corporate Rules - BCR). Diese sind ein datenschutzrechtliches Instrument, das international tätige Unternehmensgruppen immer häufiger verwenden, um das gesetzlich geforderte „angemessene Datenschutzniveau" bzw. „ausreichende Datenschutzgarantien" (§§ 4b, 4c BDSG) beim Transfer personenbezogener Daten innerhalb des Konzerns aus der EU in Drittstaaten ohne angemessenes Datenschutzniveau zu erbringen. Innerhalb international tätiger Konzerne sind grenzüberschreitende Datenübermittlungen, insbesondere von Mitarbeiterdaten, z. T. aber auch von personenbezogenen Kunden- oder Lieferantendaten, praktisch Alltag. Gerade unter konzernangehörigen Gesellschaften findet eine Vielzahl derartiger Übermittlungen statt, etwa weil Konzerne versuchen, bestimmte Aufgaben innerhalb des Konzerns bei einzelnen Gesellschaften zu zentralisieren und so Synergieeffekte zu erzielen. Für Übermittlungen personenbezogener Daten innerhalb eines Konzerns aus der EU bzw. dem EWR an konzernangehörige Gesellschaften mit Sitz in Drittstaaten ohne angemessenes Datenschutzniveau bieten BCR ein sehr interessantes Instrument zur Erfüllung der Anforderungen nach §§ 4b, 4c BDSG. Gesellschaften eines Konzerns, der BCR implementiert hat, müssen für Übermittlungen personenbezogener Daten an Konzerngesellschaften mit Sitz außerhalb des EWR dann nicht mehr z. B. sog. EU-Standardverträge abschließen. Daher führen BCR dazu, dass sich die in der EU ansässigen Unternehmen eines Konzerns für Transfers personenbezogener Daten an Konzernmitglieder in Drittstaaten den Abschluss einer u. U. ganz erheblichen Anzahl (andernfalls erforderlicher) Einzel-Übermittlungsverträge – etwa von EU-Standardverträgen – „sparen". Dies erklärt die massiv ansteigende Attraktivität des Instruments BCR für international tätige Konzerne angesichts der sich stetig verstärkenden Globalisierung in der Wirtschaft.

Vor diesem Hintergrund ist es verständlich, dass sich der Trend zu BCR im Berichtszeitraum sowohl für Konzerne mit deutscher Konzernmuttergesellschaft als auch für andere international tätige Konzerne deutlich verstärkt hat. Auf der Informationswebsite der Europäischen Kommission, auf der die bislang abgeschlossenen BCR-Anerkennungsverfahren aufgeführt sind, finden sich dementsprechend mittlerweile die Namen von über 60 Konzernen und Unternehmensgruppen. Diese Entwicklung stellt die Datenschutzbehörden in den Mitgliedstaaten vor erhebliche Herausforderungen.

> > >
http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm

Der Trend zu BCR hat dementsprechend im Berichtszeitraum zu einem deutlich erhöhten Arbeitsanfall in diesem Bereich bei den Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten und gerade auch beim BayLDA geführt. Es ist zu erwarten, dass sich diese Entwicklung ähnlich fortsetzen und ggf. noch verstärken wird. Durch die Einführung eines Verfahrens der sog. „Gegenseitigen Anerkennung" (mutual recognition; Näheres dazu auf der Homepage der EU-Kommission) haben die Datenschutzbehörden der meisten Mitgliedstaaten bereits vor einigen Jahren einen maßgeblichen Beitrag für eine Beschleunigung der Prüfung von BCR-Unterlagen geleistet.

> > >
http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/mutual_recognition/index_en.htm

Die Datenschutzbehörden der Mitgliedstaaten haben in den nächsten Jahren mit weiteren zahlreichen BCR-Anträgen zu rechnen und müssen daher durch entsprechende Spezialisierung ihrer Mitarbeiter die für diese Verfahren notwendigen Kenntnisse bereitstellen, darunter auch Sprachkenntnisse. Die Abstimmung unter den Datenschutzbehörden der betroffenen Mitgliedstaaten im Rahmen der Prüfung von BCR wird in aller Regel auf Englisch geführt. Die BCR-Unterlagen müssen den Datenschutzbehörden aus diesem Grund jedenfalls auch in englischer Sprache vorgelegt werden; daher erfolgt in der Praxis üblicherweise bereits die Prüfung der BCR-Unterlagen seitens der jeweiligen federführenden Behörde (jedenfalls auch) anhand der englischen Sprachfassung.

Die Federführung in den Verfahren zu Prüfung von BCR richtet sich grundsätzlich danach, in welchem Mitgliedstaat die Muttergesellschaft des Konzerns ihren Sitz hat. Sofern die Muttergesellschaft ihren Sitz außerhalb der EU hat, kommt es darauf an, in welchem Mitgliedstaat die „Europa-Zentrale" des Konzerns ansässig ist (vgl. WP 107 der Artikel-29-Gruppe). Da in Bayern die Muttergesellschaften oder „Europa-Zentralen" zahlreicher international tätiger Konzerne ihren Sitz haben, ist damit zu rechnen, dass auf uns auch in den Folgejahren die Federführung in weiteren EU-weiten BCR-Prüfungen zukommen wird.

Umfassende Informationen zu BCR finden sich auf der Homepage der EU-Kommission:

> > >
http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm.

Konzernen, die an der Einführung von BCR interessiert sind, ist die Lektüre dieser Informationen nachdrücklich zu empfehlen. Darunter finden sich auch mehrere Arbeitspapiere (Working Papers/WP), in denen die Artikel-29-Gruppe die Anforderungen an BCR zusammengefasst hat, um den interessierten Unternehmensgruppen praktische Hilfe bei der Formulierung der BCR zukommen zu lassen.

Im Berichtszeitraum wurden drei EU-weite BCR-Prüfverfahren unter unserer Federführung erfolgreich abgeschlossen. Es handelt sich um die BCR folgender Unternehmensgruppen:

- Siemens
- BMW
- OSRAM

Damit haben wir im bundesweiten Vergleich die größte Anzahl von EU-weiten BCR-Anerkennungsverfahren als federführende Behörde geleitet. Weitere Verfahren, bei denen wir federführend agieren, sind anhängig. Daneben waren wir in mehreren Fällen als sog. Co-Prüfer (bei Federführung von Datenschutzbehörden anderer Mitgliedstaaten) tätig.

Bei Redaktionsschluss für den vorliegenden Tätigkeitsbericht befanden sich – über die drei bereits abgeschlossenen BCR hinaus – zwei weitere BCR in der EU-weiten koordinierten Prüfung unter unserer Federführung. Daneben haben zwei weitere Unternehmensgruppen die Absicht zur Erstellung und Vorlage von BCR bekundet, für deren Prüfung wir ebenfalls EU-weit federführend zuständig wären. Diese Unternehmensgruppen arbeiten nach unserem Kenntnisstand bereits intensiv an entsprechenden Textentwürfen. Mit der förmlichen Antragstellung in diesen beiden Fällen ist in Kürze zu rechnen.

Neben den unter unserer Federführung geführten BCR-Prüfungen waren und sind wir als sog. Co-Prüfer an der koordinierten Prüfung der BCR weiterer Unternehmensgruppen in Fällen beteiligt, die der Federführung der Datenschutzbehörden anderer EU-Mitgliedstaaten oblagen bzw. obliegen.

Bei den drei o. g. unter unserer Federführung bereits abgeschlossenen Verfahren standen u. a. die folgenden Fragestellungen in besonderer Weise im Fokus:

- Möglichkeiten zur Herstellung rechtlicher Verbindlichkeit der BCR und ihrer Durchsetzbarkeit durch begünstigte Dritte
- Konzerninterne Zuweisung der Zuständigkeit zur Führung von BCR-Audits

(„Welche Einheit innerhalb eines Konzerns kann die BCR-Audits durchführen?")

- Erfordernis der Einholung zusätzlicher behördlicher Genehmigungen für Datenexporte in Drittstaaten auf der Basis von BCR
- Formulierung des Anwendungsbereichs der BCR vor dem Hintergrund, dass die BCR für alle personenbezogenen Daten anwendbar sein müssen, die „aus der EU stammen"

Im Rahmen der BCR-Anerkennungsverfahren, an denen wir beteiligt waren, haben wir im Austausch mit den Datenschutzbehörden anderer Mitgliedstaaten zu diesen Fragen folgende Ergebnisse erarbeitet:

Abschluss eines mehrseitigen Vertrags unter allen Konzerngesellschaften, die an BCR gebunden sein sollen, häufig erforderlich

BCR müssen u. a. sog. externe Verbindlichkeit besitzen. Hierunter versteht man, dass die Betroffenen (z. B. Beschäftigte) die Möglichkeit haben müssen, die ihnen in den BCR verliehenen subjektiven datenschutzrechtlichen Ansprüche (z. B. auf Auskunft, Berichtigung, Löschung, Sperrung von Daten sowie auf Schadensersatz) rechtlich durchzusetzen, insbesondere durch Anrufung von Datenschutzaufsichtsbehörden und Gerichten in der EU. Sofern konkrete BCR – was seitens der Aufsichtsbehörden unter bestimmten Voraussetzungen akzeptiert wird (vgl. WP 155 der Artikel-29-Gruppe, Nr. 3) – ein Haftungsregime enthalten, das demjenigen der EU-Standardverträge entspricht, so dass grundsätzlich der jeweilige Datenexporteur (oder ggf. sogar der jeweilige Datenimporteur) für Verstöße haftet, muss zweifelsfrei sein, dass alle teilnehmenden und somit bei diesem Haftungsregime potentiell haftenden Gesellschaften rechtsverbindlich an die BCR gebunden sind. Dies ist grundsätzlich nur dann gewährleistet, wenn alle teilnehmenden Konzerngesellschaften sich vertraglich – durch einen mehrseitigen Vertrag (intra-group agreement) – auf die Verbindlichkeit der BCR verpflichten. Denn nur Verträge erzeugen zweifelsfrei nach allen Rechtsordnungen der Mitgliedstaaten eine Drittbegünstigungswirkung (vgl. WP 74, Nr. 3.3.2). Im Falle der Wahl eines Haftungsmodells entsprechend den EU-Standardvertragsklauseln genügt es daher nicht, wenn die betreffenden BCR (ohne Abschluss eines mehrseitigen Vertrags unter den Konzerngesellschaften) „lediglich" als Konzernrichtlinie in Kraft gesetzt werden; denn in diesem Fall ist es zumindest nicht zweifelsfrei, ob insoweit von einem hinreichend nachgewiesenen Willen aller potentiell haftenden Gesellschaften zur Einhaltung der BCR einschließlich Übernahme der Haftung für Verstöße gegen drittbegünstigende Inhalte ausgegangen werden kann. Wählt hingegen ein Konzern ein Haftungsmodell, bei dem allein z. B. die (im EWR ansässige) Muttergesellschaft für BCR-Verstöße durch die außerhalb des EWR ansässigen konzernangehörigen Gesellschaften haftet, wäre ein Vertragsschluss durch alle Konzerngesellschaften wohl nicht zwingend erforderlich; vielmehr würde es dann u. U. genügen, wenn die haftende (Mutter-)Gesellschaft gegenüber allen Betroffenen (d. h. Begünstigten) etwa eine Garantieerklärung zur Einhaltung der BCR abgibt; dies wäre jedenfalls dann ausreichend, wenn auf diese Garantieerklärung deutsches Zivilrecht Anwendung findet. Denn man könnte bei Geltung deutschen Zivilrechts wohl davon ausgehen, dass auf diese Weise ein Garantievertrag mit den Betroffenen zustande kommt. Um aber Zweifel im Hinblick auf die Durchsetzbarkeit der BCR durch die Begünstigten so weit wie möglich zu vermeiden, empfehlen wir auch bei diesem Haftungsregime dennoch grundsätzlich den Abschluss eines mehrseitigen Vertrags unter allen beteiligten Konzerngesellschaften.

Getrennte konzerninterne Zuständigkeiten für BCR-Compliance „im Alltag" und für BCR-Audit

BCR müssen unter anderem zwingend Festlegungen zur laufenden Auditierung der BCR-Regelungen innerhalb des Konzerns beinhalten. Durch das Audit soll der Konzern die tatsächliche Umsetzung der BCR bei allen beteiligten Konzerngesellschaften regelmäßig überprüfen. Nach Aussagen der einschlägigen Arbeitspapiere der Artikel-29-Gruppe kann das Audit grundsätzlich sowohl durch externe als auch durch interne Auditoren durchgeführt werden. Anlässlich einiger von unserer Behörde

federführend geführten BCR-Anerkennungsverfahren gab es intensive Diskussionen mit Datenschutzbehörden anderer Mitgliedstaaten darüber, ob das BCR-Audit auch durch solche Funktionsträger innerhalb des Konzerns durchgeführt werden kann, die Datenschutzbeauftragte im Sinne des deutschen Datenschutzrechts (§ 4f BDSG) sind. Für deutsche Unternehmen mag das naheliegend erscheinen. Im Ergebnis scheidet jedoch diese Lösung in den meisten Fällen aus. Dies liegt daran, dass in BCR klar getrennt werden muss zwischen dem Hinwirken auf die Umsetzung der BCR „im Alltag" einerseits und dem BCR-Audit andererseits. Für die Umsetzung der BCR „im Alltag" muss ein gesonderter Mitarbeiterstab gebildet werden, der die Einhaltung der BCR-Vorschriften überwacht und gewährleistet (dies ist der „Mitarbeiterstab", von dem in WP 154 unter Nr. 15 oder in WP 153 unter Nr. 2.4 die Rede ist).

Die beiden Aufgaben (Audit; Überprüfung der BCR-Compliance „im Alltag") dürfen nicht bei derselben Funktionseinheit angesiedelt sein, da eine solche Lösung das Audit zu einer Art Selbstkontrolle durch den „zu Kontrollierenden selbst" machen würde, was naturgemäß nicht akzeptabel ist.

Da es sehr naheliegt, dass bei Konzernen mit deutscher Muttergesellschaft, die BCR einführen möchten, die Datenschutzbeauftragten im Sinne von § 4f BDSG die Zuständigkeit erhalten, auf die Umsetzung der BCR (wie auch des gesetzlichen Datenschutzrechts) „im Alltag" hinzuwirken, können diese nicht gleichzeitig zu BCR-Auditoren bestimmt werden. Diese Trennung der Zuständigkeiten muss aus dem Text der BCR klar hervorgehen. Dies mag aus deutscher Sicht etwas überraschend und unbefriedigend erscheinen, liegt jedoch in der Systematik der BCR begründet und wurde auch von den Datenschutzbehörden der anderen Mitgliedstaaten nachdrücklich bekräftigt.

Die Zuständigkeit für das BCR-Audit muss daher anderen Funktionsträgern überantwortet werden als denjenigen, die auf die BCR-Compliance im Alltag hinwirken sollen. Denkbar ist es z. B., die BCR-Audits einer Abteilung im Konzern zu überantworten, die auch Audits bzw. „Compliance-Prüfungen" zu anderen Themen durchführt. Je nach Organisationsstruktur des Konzerns sind aber auch andere Lösungen denkbar. Sofern es z. B. eine zentrale „Datenschutzabteilung" o. ä. im Konzern gibt, könnte das Audit dieser Abteilung zugewiesen werden, sofern die entsprechenden Personen nicht gleichzeitig Funktionen als Datenschutzbeauftragte für Konzernunternehmen innehaben und in dieser Eigenschaft (wie dann in der Praxis meist der Fall) ausweislich den Festlegungen im Text der BCR auch die Zuständigkeit für die „BCR-Compliance im Alltag" (als „Mitarbeiterstab" im Sinne von WP 154, Nr. 15 und von WP 153, Nr. 2.4) zugewiesen erhalten.

Anwendungsbereich von BCR

Schwierigkeiten bereitete bei einigen BCR die Formulierung ihres Geltungsbereichs. Die Artikel-29-Gruppe hat darauf hingewiesen, dass BCR zwingend jedenfalls auf die Verarbeitung der personenbezogenen Daten anwendbar sein müssen, die „aus der EU" übermittelt werden (vgl. WP 154, Nr. 1). Dies ist angesichts der Funktion von BCR als Mittel zur Herstellung eines „angemessenes Datenschutzniveaus" bzw. als „ausreichende Datenschutzgarantien" (§§ 4b, 4c BDSG) bei Datenübermittlungen aus der EU bzw. dem EWR selbstverständlich. Einige Unternehmen unterschätzen aber die Reichweite der BCR in der Praxis. Im Rahmen der von uns geführten BCR-Prüfverfahren haben wir die Unternehmen daher darauf hingewiesen, dass die BCR häufig auch für solche Daten anwendbar sind, die ursprünglich zwar nicht aus der EU stammen (also nicht in der EU erstmalig erhoben worden sind), jedoch einmal an ein konzernangehöriges Unternehmen in die EU übermittelt worden sind und dort dann Gegenstand einer Verarbeitung oder Nutzung waren. Denn auf diese Daten findet gemäß Art. 4 Abs. 1 Buchst. c der EG-Datenschutzrichtlinie das Datenschutzrecht des Mitgliedstaates Anwendung, in dem die Verarbeitung oder Nutzung unter Rückgriff auf dortige Mittel stattfindet. Wenn somit z. B. eine konzernangehörige brasilianische Gesellschaft Daten ihrer Mitarbeiter an eine Gesellschaft (z. B. die Muttergesellschaft) nach Deutschland übermittelt, ist auf Verarbeitungen und Nutzungen dieser Daten in Deutschland (und folglich auch für anschließende Weiter-Übermittlungen dieser

Daten aus Deutschland an andere Konzerngesellschaften in Drittstaaten) grundsätzlich das deutsche Datenschutzrecht anwendbar. Wenn solche Daten somit aus Deutschland an andere konzernangehörige Gesellschaften in Drittstaaten (z. B. Indien, USA) übermittelt werden, müssen die BCR grundsätzlich auch hierauf und folglich dann auch auf die Weiterverarbeitung dieser Daten beim konzernangehörigen Empfänger z. B. in Indien, USA etc. Anwendung finden. Dies muss aus der Formulierung des Anwendungsbereichs in den BCR hinreichend deutlich hervorgehen. Missverständliche oder unklare Formulierungen wurden in den von uns geführten BCR-Verfahren daher moniert und von den Unternehmen entsprechend nachgebessert. Aus der verwendeten Formulierung muss hervorgehen, dass die BCR auf die Verarbeitungen solcher Daten in Drittstaaten Anwendung finden, die vorher dem Datenschutzrecht von EU-Mitgliedstaaten unterfallen sind. Eine Formulierung, wonach die BCR auf Daten anwendbar sind, die „aus der EU stammen", ist nach unserer Auffassung nicht hinreichend eindeutig und müsste daher im o.g. Sinne zumindest klarstellend ergänzt werden.

Zum Teil Erfordernis behördlicher Genehmigungen für Datenexporte auf der Grundlage von BCR

Wir weisen Konzerne, die BCR einführen wollen, sowohl im Rahmen von BCR-Prüfverfahren als auch im Rahmen der Erteilung allgemeiner Informationen stets darauf hin, dass nach erfolgreichem Abschluss des Anerkennungsverfahrens in einigen Bundesländern bzw. EU-Mitgliedstaaten noch ein weiterer Schritt erforderlich ist, bevor die konzernangehörigen Unternehmen auf der Basis von BCR mit dem Export personenbezogener Daten aus der EU an die konzernangehörigen Gesellschaften mit Sitz in unsicheren Drittstaaten beginnen können: So ist in zahlreichen Mitgliedstaaten sowie, was Deutschland betrifft, jedenfalls in einer Reihe von Bundesländern vor dem Export personenbezogener Daten auf der Grundlage von BCR durch eine einzelne Gesellschaft – zusätzlich zum Vorliegen von aufsichtsbehördlich bereits geprüften und als hinreichend anerkannten BCR – noch eine gesonderte Datenexportgenehmigung nach § 4c Abs. 2 Satz 1 BDSG zu beantragen. Dies muss die jeweilige datenexportierende Gesellschaft bei der für sie örtlich zuständigen Datenschutzbehörde tun. Diejenigen Behörden, die Datenexporte auf der Basis von BCR für nicht genehmigungsbedürftig halten – darunter unsere Behörde – begründen ihre Auffassung damit, dass BCR bereits im Rahmen der Bewertung der Angemessenheit des Datenschutzniveaus beim Datenempfänger im Sinne von § 4b Abs. 2 Satz 2 und Abs. 3 BDSG berücksichtigt werden können. Besitzt ein Konzern BCR, die von den Datenschutzbehörden in einem „BCR-Prüfverfahren" als hinreichend akzeptiert worden sind, kann nach Auffassung dieser Datenschutzbehörden grundsätzlich angenommen werden, dass die daran gebundenen konzernangehörigen Gesellschaften ein „angemessenes Schutzniveau" im Sinne von § 4b Abs. 2 Satz 2 und Abs. 3 BDSG haben; Datenexporte nach § 4b Abs. 2 Satz 2 BDSG bedürfen (anders als nach § 4c Abs. 2 Satz 1 BDSG) nicht der vorherigen Genehmigung.

Auf einer Website der EU-Kommission findet sich eine Übersicht dazu, in welchen Mitgliedstaaten (bzw. Bundesländern) dieses zusätzliche Erfordernis gilt (dort unter dem Link „Table of national administrative requirements"):

> > >
http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/tools/index_en.htm

Die Datenschutzbehörden der Mitgliedstaaten bemühen sich derzeit, diese Übersicht zu aktualisieren. Künftig soll darin u. a. eine gesonderte Rubrik für „BCR für Auftragsdatenverarbeiter" aufgenommen werden.

Dauer von BCR-Prüfverfahren

Was die Dauer der BCR-Prüfverfahren betrifft, bemühen sich die Datenschutzbehörden der Mitgliedstaaten um weitere Beschleunigung. Aufgrund der stetig steigenden Anzahl eingehender Anträge auf BCR-Anerkennung stellt dies die Behörden jedoch vor erhebliche Herausforderungen. Zwar kann ein Zeitraum von (in Einzelfällen ggf. auch deutlich) unter einem Jahr durchaus realistisch sein; die Dauer hängt jedoch maßgeblich ab von der Qualität der eingereichten Unterlagen und auch der Schnel-

ligkeit, mit der der Konzern die Anmerkungen und Hinweise der federführenden Datenschutzbehörde sowie der Co-Prüfer-Behörden umsetzt.

14.2 BCR für Auftragsdatenverarbeiter – ein neues Instrument

Im Berichtszeitraum erreichte uns eine Vielzahl von Fragen zum neuen Instrument der „BCR für Auftragsdatenverarbeiter". Mehrere Konzerne haben derartige BCR angekündigt, deren EU-weite Prüfung unter unserer Federführung erfolgen wird. In einem Verfahren dieser Art haben wir bereits als Co-Prüfer mitgewirkt.

BCR standen zunächst nur als Instrument für den Export personenbezogener Daten durch „verantwortliche Stellen" (die alle ein und demselben Konzern angehören müssen) an konzernangehörige Empfänger in Drittstaaten zur Verfügung. Die Artikel-29-Gruppe hat mit Wirkung zum 1.1.2013 erklärt, dass BCR auch als Instrument in Betracht kommen, mit dessen Hilfe Konzerne, deren Geschäftsgegenstand die Auftragsdatenverarbeitung für konzernfremde Stellen ist, Daten an Konzerngesellschaften mit Sitz in Drittstaaten transferieren können. Die Artikel-29-Gruppe hat für diese Fälle eine neue Variante von BCR ins Leben gerufen, die sog. BCR für Auftragsdatenverarbeiter (BCR for Processors / BCR-P); im Unterschied dazu werden die unter dem vorangegangenen Gliederungspunkt dargestellten „herkömmlichen" BCR nunmehr zur Unterscheidung häufig als „BCR für verantwortliche Stellen" (BCR for Controllers/BCR-C) bezeichnet.

Inzwischen haben die Datenschutzbehörden einiger EU-Mitgliedstaaten die BCR-P mehrerer Unternehmensgruppen abschließend geprüft und gemessen an den von der Artikel-29-Gruppe aufgezeigten Erfordernissen als hinreichend anerkannt. Wir haben bei einem dieser Verfahren – den BCR-P der Atos-Gruppe – als sog. Co-Prüfer mitgewirkt; die Federführung für diesen Fall oblag der französischen Datenschutzaufsichtsbehörde.

Den Hintergrund für die Einführung von BCR-P als neues Instrument bilden die stetig zunehmenden Outsourcing-Entwicklungen im Bereich der Datenverarbeitung. Eine Reihe spezialisierter Konzerne bieten am Markt spezifische datenverarbeitende Dienstleistungen an, die als Auftragsdatenverarbeitung einzustufen sind. Dazu gehören, jedenfalls in der Regel, verschiedene Formen von Cloud Computing. Zu derartigen Unternehmensgruppen gehört häufig eine Vielzahl einzelner konzernangehöriger Gesellschaften, von denen nicht selten einige ihren Sitz in Drittstaaten ohne angemessenes Datenschutzniveau haben. In solchen Fällen werden die Auftragsdatenverarbeitungsdienste somit auf mehrere einzelne Unternehmen desselben Konzerns aufgeteilt. Als Folgen hiervon sind dann zahlreiche Transfers der (im Auftrag verarbeiteten) Daten unter den konzernangehörigen Gesellschaften derartiger „Auftragsdatenverarbeitungskonzerne" („ADV-Konzerne") vorgesehen, darunter auch an Konzerngesellschaften in Drittstaaten. Dies kann bereits der Fall sein, wenn „Support"-Dienste oder andere Dienstleistungen der Wartung und Pflege von Datenverarbeitungssystemen erbracht werden und hierbei unterschiedliche Gesellschaften einer Unternehmensgruppe, die diese Leistungen anbietet, involviert sind.

Für solche „ADV-Konzerne" können BCR-P ein praxistaugliches Instrument sein. Werden nämlich in dieser Weise zahlreiche einzelne Gesellschaften des „ADV-Konzerns" in die Verarbeitung involviert, müsste der jeweilige potentielle Auftraggeber an sich grundsätzlich mit jeder einzelnen dieser Gesellschaften einen schriftlichen Auftrag nach § 11 BDSG und – sofern die Verarbeitung in einem unsicheren Drittstaat erfolgen soll – einen EU-Standardvertrag zur Auftragsdatenverarbeitung gemäß Kommissionsbeschluss 2010/87/EU abschließen, was zu einem häufig sehr hohen vertragsabschlusstechnischen Aufwand führen würde. BCR-P ermöglichen eine deutliche Reduzierung dieses Aufwands: Der Auftraggeber schließt mit einem (einzigen) der konzernangehörigen Unternehmen aus dem „ADV-Konzern" einen Auftrag nach § 11 BDSG; die Weitergabe der Daten von

diesem Konzernunternehmen an die anderen in die Auftragsverarbeitung involvierten konzernangehörigen Unternehmen, auch in unsichere Drittstaaten, kann anschließend auf der Basis der BCR-P erfolgen. Es ist dann für den Auftraggeber nicht (mehr) erforderlich, mit jedem einzelnen dieser Unternehmen einen jeweils gesonderten schriftlichen Auftrag nach § 11 BDSG abzuschließen (vgl. WP 204, Nr. 2.2.1 am Ende).

Betont werden muss, dass die Gesellschaften des „ADV-Konzerns", der BCR-P besitzt, nicht „Datenexporteure" im Sinne des deutschen Datenschutzrechts (d. h. im Sinne von § 4b BDSG oder § 4c BDSG) sind, da Auftrags- und Unterauftragsdatenverarbeiter selbst nicht „verantwortliche Stellen" im datenschutzrechtlichen Sinne sind. „Datenexporteur" im Sinne von §§ 4b, 4c BDSG kann nur eine „verantwortliche Stelle" sein, nicht jedoch ein Auftrags- oder Unterauftragsdatenverarbeiter. Datenexporteure sind mithin alle Unternehmen, die „verantwortliche Stellen" sind und sich als Auftraggeber für Zwecke der Auftragsverarbeitung eines „ADV-Konzerns" bedienen möchten, der BCR-P anwendet. Diese Auftraggeber müssen daher selbst die entsprechende Datenexportgenehmigung bei den für sie örtlich zuständigen Datenschutzbehörden beantragen, jedenfalls soweit die örtlich zuständige Behörde für Datenexporte in unsichere Drittstaaten auf der Basis von BCR-P von einer Genehmigungsbedürftigkeit ausgeht. Hierbei ist (wie für Datenexporte auf der Basis von BCR-C) auch für Exporte auf Grundlage von BCR-P anzumerken, dass ein Teil der Datenschutzbehörden diese als genehmigungsbedürftig erachtet, während der andere Teil der Behörden von Genehmigungsfreiheit ausgeht. Die Artikel-29-Gruppe wird auf der Homepage der Kommission in der bereits erwähnten veröffentlichten Tabelle in Kürze auch Angaben zu BCR-P aufnehmen; dort soll künftig auch bezüglich BCR-P für den Zuständigkeitsbereich aller Datenschutzbehörden in der EU angegeben werden, ob die jeweiligen Datenexporte genehmigungsfrei oder aber genehmigungsbedürftig sind.

>>> *http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/tools/index_en.htm*

14.3 Cloud Computing und Unterauftragserteilung

Uns erreichten zahlreiche Anfragen bayerischer Unternehmen, die eine Auslagerung bestimmter Datenverarbeitungen „in die Cloud" erwägen, jedoch die ihnen von den Cloud-Anbietern vorgelegten datenschutzrechtlichen Vertragsklauseln kritisch bewerteten und uns daher um eine Bewertung baten.

Der „Mega-Trend" zum Cloud Computing hat sich im Berichtszeitraum deutlich verstärkt, auch wenn durchaus festzustellen ist, dass bayerische Unternehmen gerade bei Fragen des Datenschutzrechts begrüßenswerterweise auch kritische Fragen in diesem Zusammenhang aufwerfen. Gerade große US-amerikanische Cloud-Anbieter bieten Dienste zur Verarbeitung personenbezogener Daten im Wege von Cloud-Modellen massiv auf dem Weltmarkt an. Vor diesem Hintergrund erreichte uns im Berichtszeitraum eine Vielzahl von Fragen bayerischer Unternehmen zu Cloud-Computing-Diensten. Die meisten dieser Fragen wurden von Datenschutzbeauftragten von (häufig mittelständischen) Unternehmen gestellt, deren Geschäftsleitungen auf der Suche nach Kostenoptimierungsmöglichkeiten die vielfältigen am Markt angebotenen Dienste zur Auslagerung der Speicherung oder sonstiger Verarbeitungen personenbezogener Daten „in die Cloud" prüfen.

Mehrere bayerische Unternehmen legten uns die ihnen von (häufig großen US-amerikanischen) Cloud-Computing-Dienstleistern vorgeschlagenen Datenschutzverträge vor, weil sie Zweifel an der Vereinbarkeit bestimmter Klauseln mit dem deutschen Datenschutzrecht hatten. Die von uns daraufhin geprüften Verträge zeigten, dass solche Zweifel häufig berechtigt waren.

Häufige Probleme bereiten gerade die Cloud-Verträge von Anbietern aus Drittstaaten. Beispielhaft seien einige der konkreten Fragestellungen dargestellt:

Unzureichende Einräumung von Auftragskontrollrechten für den Auftraggeber

Als besonders häufiger Schwachpunkt datenschutzrechtlicher Verträge für Cloud-Dienste erwies sich die unzureichende Einräumung von Auftragskontrollrechten für den Auftraggeber, insbesondere bei Einschaltung von Unterauftragnehmern. Auf diese Problematik haben wir bereits in unserem 5. Tätigkeitsbericht 2011/2012 hingewiesen. Unsere damalige Beobachtung, dass gerade Cloud-Computing-Verträge diesbezüglich häufig unzureichend sind, hat sich im Berichtszeitraum 2013/2014 fortgesetzt.

Bei der Vergabe von Unteraufträgen zur Datenverarbeitung, auch im Rahmen von Cloud Computing, ist daran zu erinnern, dass die Verantwortlichkeit zur Einhaltung der datenschutzrechtlichen Vorschriften stets beim Auftraggeber („Kunden"; „Cloud-Anwender") verbleibt, während der Cloud-Anbieter in aller Regel Auftragsdatenverarbeiter ist. Dem Auftraggeber müssen – auch gegenüber allen etwaigen Unterauftragnehmern – Auftragskontrollmöglichkeiten gemäß § 11 Abs. 2 Satz 4 BDSG ausdrücklich vorbehalten bleiben.

Bei mehreren von uns gesichteten Verträgen räumte der Cloud-Anbieter (= Auftragsverarbeiter) dem „Kunden" (= Auftraggeber) keine Auftragskontrollrechte ein oder wollte eine Auftragskontrolle ausschließlich in der Form der Vorlage von Datensicherheitszertifikaten an den Auftraggeber akzeptieren. Dies ist nach deutschem Datenschutzrecht nicht akzeptabel, da es nicht vereinbar mit der Verantwortlichkeit des Auftraggebers gemäß § 11 Abs. 1 BDSG wäre, eigene Kontrollmöglichkeiten des Auftraggebers vertraglich schlechthin auszuschließen. Zwar besteht Einigkeit dahingehend, dass der Auftraggeber die Auftragskontrolle nicht zwingend „vor Ort" durchführen muss, sondern insoweit grundsätzlich auch die Vorlage geeigneter Zertifikate in Betracht kommt, die das Vorhandensein ausreichender technischer und organisatorischer Maßnahmen beim Auftragsdatenverarbeiter belegen. Das vollständige vertragliche Ausschließen jeglicher Vor-Ort-Kontrollmöglichkeit, indem vertraglich festgelegt wird, dass die Auftragskontrolle ausschließlich durch die Vorlage von Zertifikaten an den Auftraggeber ausgeübt wird, kann jedoch nicht hingenommen werden. So sieht auch der Standardvertrag zur Auftragsverarbeitung gemäß Kommissionsbeschluss 2010/87/EU, der als Modell für die Anforderungen an grenzüberschreitende Auftragsdatenverarbeitung angesehen werden kann und muss, zwingend ein eigenes Kontrollrecht des Auftraggebers vor (Klausel 5f). Wenn wir im Rahmen unserer Tätigkeit derartige unzureichende Klauseln festgestellt haben, haben wir die betreffenden Unternehmen (Cloud-Anbieter bzw. potentielle Auftraggeber) darauf hingewiesen, dass die Datenexporte unter diesen Umständen den Anforderungen an eine hinreichende Auftragskontrolle gemäß § 11 Abs. 2 Satz 4 BDSG nicht genügen und daher bei Bedarf durch aufsichtsbehördliche Anordnungen gemäß § 38 Abs. 5 BDSG unterbunden werden könnten.

Einschaltung von Unterauftragnehmern: mindestens vorherige Widerspruchsmöglichkeit für den Auftraggeber

Die Einschaltung von Unterauftragnehmern ist in jedem Einzelfall nur mit vorheriger Zustimmung des Auftraggebers zulässig; „Blankoermächtigungen" des Auftraggebers an den Auftragsverarbeiter zur Einschaltung vorher nicht namentlich benannter (z. B. mehr oder minder beliebig „rollierender") Unterauftragsverarbeiter genügen dieser Anforderung nicht. Mehrere Verträge von Cloud-Anbietern, die uns durch potentielle Auftraggeber-Unternehmen mit der Bitte um Beurteilung vorgelegt wurden, wiesen in dieser Frage offensichtliche Mängel auf.

Die uns vorgelegten Texte von Datenschutzverträgen von Cloud-Anbietern sahen häufig vor, dass der Cloud-Anbieter (d. h. der Auftragsverarbeiter) die Möglichkeit haben soll, Unterauftragnehmer in die Verarbeitung einzubinden, über deren Identität der Auftraggeber erst informiert wird, nachdem die Daten an den entsprechenden Unterauftragnehmer bereits geflossen sind. Hierfür mögen aus Sicht des Cloud-Anbieters Praktikabilitätsgründe spre-

chen, zumal jedenfalls für bestimmte Varianten des Cloud-Computing gerade der Umstand „typisch" sein soll, dass die Verarbeitung auf eine Vielzahl einzelner, unter Umständen „rollierender" Unternehmen verteilt wird. Mit der umfassenden Verantwortlichkeit des Auftraggebers gemäß europäischem und deutschem Datenschutzrecht (§ 11 Abs. 1 BDSG) ist ein solches Vorgehen jedoch nicht vereinbar. Die Datenschutzbehörden der EU-Mitgliedstaaten haben darauf hingewiesen (vgl. WP 196, Nr. 3.3.2), dass der Auftraggeber vor jeder Unterauftragserteilung über die Identität des jeweiligen Unterauftragnehmers informiert und ihm vertraglich ausdrücklich ein (zeitlich ausreichend bemessenes) Recht zum Widerspruch oder zur Vertragsbeendigung eingeräumt werden muss. Soweit uns im Rahmen unserer Tätigkeit Vertragsklauseln bekannt geworden sind, die diesen Anforderungen nicht genügten, haben wir die beteiligten Unternehmen darauf hingewiesen, dass Datenübermittlungen an Unterauftragnehmer, die den genannten Anforderungen nicht genügen, unzulässig sind. Sollten konkrete derartige Fälle bekannt werden, werden wir daher geeignete Reaktionen bis hin zur Anordnung der Aussetzung derartiger Übermittlungen nach § 38 Abs. 5 BDSG prüfen.

Vertragsgestaltung bei der Erteilung von Unteraufträgen

Bei Cloud-Computing-Dienstleistungen ist oft gewollt, dass auf Seiten des Cloud-Anbieters außer derjenigen rechtlichen Einheit (Gesellschaft, „entity"), die den Auftragsverarbeitungsvertrag mit dem Auftraggeber abschließt, weitere Unternehmen desselben „Cloud-Konzerns" und ggf. auch konzernfremde Unternehmen in die Erbringung der Cloud-Leistungen eingebunden werden sollen. Datenschutzrechtlich wären solche Gesellschaften grundsätzlich als (Unter-)Auftragnehmer einzustufen. In den Texten der datenschutzrechtlichen Verträge von Cloud-Anbietern wird dieser Sachverhalt jedoch offenbar nicht immer ordnungsgemäß umgesetzt. Uns wurden z. B. Vertragstexte bekannt, in denen auf solche (Unter-)Auftragnehmer die gesetzlich zwingenden Pflichten eines (Unter-)Auftragnehmers vertraglich nicht eindeutig übertragen wurden. In manchen Auftragsverarbeitungsverträgen wurden derartige weitere in die Verarbeitung eingebundene Gesellschaften zwar (z. B. in einem Anhang) genannt, ohne jedoch eindeutig zu regeln, dass für sie dieselben Pflichten gelten, die gemäß dem zwischen Auftraggeber und (Haupt-)Auftragsverarbeiter abgeschlossenen schriftlichen Auftrag nach § 11 BDSG für den Haupt-Auftragsverarbeiter gelten. Vermutlich steckt hinter diesem Fehler bisweilen die Vorstellung, dass jedenfalls Gesellschaften desselben Konzerns eine Art „Einheit" bilden würden und daher die explizite Übertragung der Auftragnehmerpflichten auf jede einzelne Konzerngesellschaft, die als (Unter-) Auftragnehmer an der Verarbeitung beteiligt sein soll, nicht erforderlich sei. Datenschutzrechtlich ist diese Vorstellung unzutreffend. Richtigerweise muss jede einzelne Gesellschaft, die in die Auftragsdatenverarbeitung eingebunden sein soll, in vertraglich eindeutiger Weise als Auftragnehmer oder Unterauftragnehmer ausgewiesen und an die entsprechenden datenschutzrechtlichen Pflichten gebunden werden, indem ihr (hinsichtlich der von ihr verarbeiteten Daten und erbrachten Verarbeitungsschritte) dieselben Pflichten auferlegt werden, die für den Hauptauftragnehmer gelten. Zwar kommt u.U. auch eine Erteilung des Unterauftrags durch den „ersten" Auftragnehmer (anstelle des Auftraggebers) in Betracht, etwa wenn zwischen Auftraggeber und „erstem" Auftragnehmer der Standardvertrag 2010/87/EU abgeschlossen wurde, denn gemäß Klausel 11 dieses Standardvertrags kann der Auftragnehmer Unteraufträge auch im eigenen Namen vergeben (freilich nur mit vorheriger Zustimmung des Auftraggebers, s. o.; vgl. WP 196). Jedoch muss dafür gesorgt werden, dass auch in solchen Unteraufträgen Auftragskontrollrechte des Auftraggebers gegenüber dem Unterauftragnehmer ausdrücklich vorgesehen werden, und dass den Unterauftragnehmer dieselben Pflichten treffen, wie sie für den „ersten" Auftragnehmer gelten. Andernfalls würde sich die datenschutzrechtliche Verantwortlichkeit des Auftraggebers jedenfalls für die bei den Unterauftragnehmern erfolgenden Datenverarbeitungsschritte „verflüchtigen", was mit § 11 Abs. 1 BDSG nicht vereinbar wäre.

Neues Verfahren zur EU-weit koordinierten Prüfung von Vertragsklauseln zur internationalen Auftragsdatenverarbeitung

Wie im vorangegangenen Gliederungspunkt erläutert, haben uns im Berichtszeitraum mehrere Unternehmen, die die Auslagerung von Datenverarbeitungen an Cloud-Computing-Anbieter oder Anbieter sonstiger Auftragsdatenverarbeitungsdienste erwogen, um Bewertung der datenschutzrechtlichen Vertragsklauseln gebeten, die ihnen hierbei durch (häufig US-amerikanische) Cloud- oder ADV-Anbieter unterbreitet wurden. Wie uns aus dem Kontakt mit Datenschutzbehörden anderer Mitgliedstaaten bekannt ist, erhalten auch andere Datenschutzbehörden in der EU häufig ähnliche Bitten um Bewertung vorformulierter Vertragsklauseln, die Anbieter von Cloud- bzw. Auftragsverarbeitungsdiensten ihren potentiellen Kunden (Auftraggebern) zum Abschluss vorlegen. Häufig bieten die Anbieter von Cloud- und ADV-Diensten dieselben datenschutzrechtlichen Vertragsklauseln für potentielle Kunden weltweit und somit auch in den verschiedenen EU-Mitgliedstaaten an.

Wir haben daher im Rahmen unserer Mitwirkung in der Unterarbeitsgruppe „International Transfers" der Artikel-29-Gruppe darauf hingewiesen, dass es sinnvoll wäre, die Texte solcher EU-weit angebotenen datenschutzrechtlichen Vertragsklauseln durch die Datenschutzbehörden der EU-Mitgliedstaaten koordiniert zu bewerten, vergleichbar etwa dem bewährten EU-weiten koordinierten Verfahren zur Prüfung von Binding Corporate Rules (vgl. dazu Kapitel 14.1.).

Nachdem unser Vorschlag auch von den Behörden anderer Mitgliedstaaten geteilt wurde, hat die Artikel-29-Gruppe in ihrem WP 226 kürzlich erklärt, dass Unternehmensgruppen, die ihre Dienste der Auftragsdatenverarbeitung in mehreren Mitgliedstaaten anbieten, die Möglichkeit haben, die von ihnen für diese Dienste den potentiellen Auftraggebern („Kunden") angebotenen Datenschutzvertragsklauseln koordiniert von den Datenschutzbehörden der Mitgliedstaaten bewerten zu lassen.

>>> *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp226_en.pdf*

Eine wichtige Einschränkung besteht jedoch darin, dass die Datenschutzbehörden die koordinierte Prüfung nur unter der Voraussetzung anzubieten bereit sind, dass der angebotene Vertragstext weitgehend auf dem EU-Standardvertrag zur Auftragsdatenverarbeitung gemäß Kommissionsbeschluss 2010/87/EU beruht (auch wenn er gegebenenfalls gewisse Zusatzklauseln enthält). Denn nur in diesem Fall steht mit dem EU-Standardvertrag ein hinreichend eindeutiger Maßstab zur Verfügung, anhand dessen eine koordinierte Prüfung unter Berücksichtigung des damit verbundenen Aufwands leistbar ist. Durch diese Einschränkung soll zudem Cloud-Anbietern ein Anreiz geboten werden, ihren Kunden datenschutzrechtliche Vertragsklauseln anzubieten, die dem EU-Standardvertrag möglichst entsprechen und damit ein hohes Datenschutzniveau gewährleisten.

Die koordinierte Prüfung solcher Vertragsklauseln durch die Datenschutzbehörden wird auf die Frage beschränkt sein, ob der angebotene Vertrag, auch wenn er ggf. gewisse Zusatzklauseln enthält, letztlich keine nachteiligen Abweichungen im Vergleich zum o. g. EU-Standardvertrag beinhaltet (vgl. WP 226, Nr. II.A und Nr. II.B.3). Eine darüber hinausgehende „Komplettprüfung" des angebotenen Datenschutzvertrages durch die Datenschutzbehörden, etwa im Hinblick auf die technisch-organisatorischen Maßnahmen, ist hierbei nicht beabsichtigt; sie ist im geltenden Datenschutzrecht nicht vorgesehen und wäre im Übrigen mit Blick auf die Kapazitäten der Datenschutzbehörden und die Vielzahl der am Markt angebotenen grenzüberschreitenden Cloud- und sonstigen ADV-Dienste auch kaum leistbar.

Es wird interessant sein zu beobachten, inwieweit international tätige Anbieter von Cloud Computing und anderer Dienste der Auftragsdatenverarbeitung von dem Angebot der koordinierten Prüfung ihrer datenschutzrechtlichen Vertragsklauseln durch die Datenschutz-

behörden der Mitgliedstaaten Gebrauch machen werden.

Orientierungshilfe Cloud Computing Version 2.0

Aufgrund der zahlreichen komplexen datenschutzrechtlichen Anforderungen an Cloud-Computing haben die Datenschutzkonferenz und der „Düsseldorfer Kreis" ihre im Jahr 2011 erstmals veröffentlichte „Orientierungshilfe Cloud Computing" aktualisiert. Sie ist auf unserer Webseite in der aktuellen Fassung abrufbar.

> > >
http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/Orientierungshilfe%20CloudComputing_Stand2014.pdf

14.4 Problematik des Exports personenbezogener Daten vor dem Hintergrund der Darstellungen von Edward Snowden

Die Berichte von Edward Snowden über Datenzugriffe massiven Umfangs durch US-Sicherheitsbehörden haben zu zahlreichen Anfragen von Unternehmen geführt, die personenbezogene Daten in die USA transferieren. Die Berichte werfen auch für die Datenschutzbehörden schwerwiegende Fragen auf.

Beginnend mit dem Frühsommer 2013 veröffentlichte der ehemalige US-Geheimdienstmitarbeiter Edward Snowden umfangreiche Informationen und zahlreiche Dokumente über die Praxis der Informationsgewinnung durch US-Nachrichtendienste, aber auch von Nachrichtendiensten weiterer – mit den US-Diensten zusammenarbeitender – Staaten. Das von diesen Darstellungen berichtete Ausmaß der Informationsgewinnung und möglicher Zugriffe auf personenbezogene Daten durch Nachrichtendienste hat in der Öffentlichkeit zu intensiven Debatten geführt. Jenseits der politischen Dimension der Materie haben die Berichte selbstverständlich auch weitreichende Fragen für die Arbeit und die Aufgaben der Datenschutzbehörden in Deutschland und anderen EU-Mitgliedstaaten aufgeworfen. Nicht zuletzt haben die Darstellungen von Snowden aber vielfach auch bei Unternehmen – also den unserer Aufsicht unterliegenden Stellen – offenbar Anlass zu einer intensiveren Auseinandersetzungen mit Fragen des Datenschutzes geliefert. Diese intensivere Auseinandersetzung machte sich im Berichtszeitraum für unsere tägliche Tätigkeit zum einen bemerkbar in verstärkten Beratungsanfragen von Unternehmen mit stark international ausgerichteter Aktivität. Ein zweiter Bereich, in dem wir aus diesem Anlass verstärkte Anfragen erhielten, betraf die Nutzung von Cloud-Computing-Diensten insbesondere US-amerikanischer Anbieter. Dieser zweite Bereich hängt damit zusammen, dass der „Weg in die Cloud" in den letzten Jahren eine rasante Entwicklung genommen hat und gerade US-amerikanische Anbieter vielfach den Markt für Cloud-Dienste dominieren. Cloud-Anbieter bieten eine Fülle unterschiedlicher Dienste zur Verarbeitung personenbezogener Daten an – angefangen von der bloßen Speicherung von Daten auf Servern des Anbieters (häufig auch außerhalb des EU-Raumes) bis hin etwa zu komplexen Customer-Relationship-Management-Komplettsystemen. Viele dieser Dienste sind gerade auch für kleine und mittelständische Unternehmen interessant, so dass ihr Einsatz für Unternehmen beinahe jeder Branche und jeder Größenordnung eine Option sein kann.

Diese Entwicklung hat zur Folge, dass auch kleine und mittlere Unternehmen sehr schnell von den überaus komplexen datenschutzrechtlichen Fragen des grenzüberschreitenden Datenverkehrs und damit auch von der durch Snowden aufgezeigten Problemlage betroffen sein können. Es ist daher nicht verwunderlich, dass die Zahl der bei uns eingegangenen Beratungsanfragen zu Cloud-Angeboten insbesondere von US-Unternehmen im Berichtszeitraum deutlich angewachsen ist. Meist waren es dabei Datenschutzbeauftragte bayerischer Unternehmen, die uns fragten, welche datenschutzrechtlichen Konsequenzen die Problematik von Datenzugriffen durch US-Behörden im Hinblick auf Übermittlungen personenbezogener Daten in die USA oder allgemein an US-Unternehmen haben. Häufig wurde gezielt gefragt, wie die deutschen Datenschutzbehörden derartige Übermittlungen vor dem genannten Hinter-

grund aktuell bewerten und ob ggf. aufsichtsbehördlich gegen solche Datenübermittlungen eingeschritten werde.

Diese – vor allem von Unternehmen gestellten – Anfragen konzentrierten sich letztlich auf die Frage, inwieweit die europäischen Datenschutzbehörden Übermittlungen personenbezogener Daten in die USA vor dem Hintergrund der Berichte über den Umfang an Datenzugriffen dortiger Nachrichtendienste untersagen und wie sich datenexportierende deutsche Unternehmen verhalten sollten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Pressemitteilung vom 24.07.2013 erklärt, dass die deutschen Datenschutzbehörden vor dem Hintergrund der Darstellungen über Datenzugriffe US-amerikanischer Nachrichtendienste prüfen müssen, ob Datenübermittlungen in Drittstaaten – namentlich in die USA – auszusetzen sind. Vor allem diese Pressemitteilung war Anlass für zahlreiche bei uns eingegangene Anfragen bayerischer Unternehmen.

Den anfragenden Unternehmen erläuterten wir unsere gegenwärtige datenschutzrechtliche Bewertung wie folgt:

Personenbezogene Daten dürfen aus dem Inland in einen Drittstaat nur übermittelt werden, wenn dort ein (von der EU-Kommission förmlich gemäß Art. 25 Abs. 6 der EG-Datenschutzrichtlinie/RL 95/46/EG anerkanntes) sog. angemessenes Datenschutzniveau besteht (§ 4b Abs. 2, Abs. 3 BDSG) oder wenn anderweitig ausreichende Garantien für den Schutz der Daten beim Datenempfänger erbracht werden, wobei im letztgenannten Fall die Übermittlung grundsätzlich der vorherigen Genehmigung der Datenschutzbehörde bedarf (§ 4c Abs. 2 Satz 1 BDSG). Die USA besitzen zwar nicht als Ganzes ein „angemessenes Datenschutzniveau" im vorgenannten Sinne; allerdings hat die Europäische Kommission in ihrer Entscheidung 2000/520/EG vom 26.07.2000 festgelegt, dass für US-Unternehmen, die sich den sog. Safe-Harbor-Datenschutzgrundsätzen unterwerfen, von einem „angemessenen Datenschutzniveau" im Sinne von Art. 25. Abs. 6 RL 95/46/EG auszugehen ist. Diese Entscheidung der Kommission ist gegenwärtig nach wie vor in Kraft und für die Datenschutzbehörden der Mitgliedstaaten bindend (Art. 25 Abs. 6 Satz 2 RL 95/46/EG). Auch wenn gerade die deutschen Datenschutzbehörden bereits mehrfach Kritik an der praktischen Umsetzung des Safe-Harbor-Systems geäußert haben, ist die Safe-Harbor-Kommissionsentscheidung auch für sie bindend. Damit ist nach wie vor davon auszugehen, dass US-Unternehmen, die eine aktuelle gültige Safe-Harbor-Zertifizierung besitzen, jedenfalls grundsätzlich ein „angemessenes Datenschutzniveau" im Sinne von § 4b BDSG aufweisen. In der praktischen Konsequenz bedeutet dies, dass – sofern auch die übrigen Voraussetzungen an Datenübermittlungen erfüllt sind (d. h. die Übermittlung gemäß § 4 Abs. 1 BDSG aufgrund Einwilligung oder einer Rechtsvorschrift zulässig ist) – personenbezogene Daten aus dem Inland an US-Unternehmen mit gültiger Safe-Harbor-Zertifizierung grundsätzlich übermittelt werden dürfen.

Als Alternative zu einer Safe-Harbor-Zertifizierung des datenempfangenden US-Unternehmens kommt für Übermittlungen personenbezogener Daten in die USA freilich auch der Abschluss eines der sog. EU-Standardverträge zwischen dem datenexportierenden Unternehmen und dem US-Datenempfänger in Betracht. Durch den Abschluss eines dieser Standardverträge werden „angemessene Datenschutzgarantien" im Sinne von § 4c Abs. 2 Satz 1 BDSG für den Datenexport in einen Drittstaat erbracht. Sofern die Klauseln eines der Standardverträge unverändert verwendet werden, wird der Datenexport durch die deutschen Datenschutzbehörden als genehmigungsfrei angesehen.

Mithin ist festzuhalten, dass der o. g. „Safe-Harbor-Beschluss" der Kommission vom 26.07.2000 nach wie vor in Kraft und somit für die Datenschutzbehörden verbindlich zu beachten ist. Nicht zuletzt unter dem Eindruck der Snowden-Berichte erkennt allerdings inzwischen auch die Europäische Kommission erheblichen Nachbesserungsbedarf hinsichtlich des durch die Safe-Harbor-Grundsätze geschaffenen Schutzniveaus. Zwar hat die Kom-

mission den Beschluss nicht aufgehoben; in einer Mitteilung vom 27.11.2013 hat sie jedoch an die US-Seite dreizehn Empfehlungen zur Überarbeitung der Safe-Harbor-Grundsätze gerichtet und ist mit der amerikanischen Regierung in Verhandlungen eingetreten, um auf eine entsprechende Anhebung des Schutzstandards in den Safe-Harbor-Grundsätzen hinzuwirken. Diese Verhandlungen dauern derzeit noch an. Der Abschluss wurde wiederholt verschoben; derzeit wird er seitens der Kommission wohl für den Frühsommer 2015 angestrebt.

Allerdings bieten sowohl die Safe-Harbor-Entscheidung der Kommission als auch die drei derzeit zur Verfügung stehenden EU-Standardverträge für die Datenschutzbehörden der EU-Mitgliedstaaten für bestimmte Ausnahmefälle die Möglichkeit, Datenübermittlungen auszusetzen. Nach dem Wortlaut von Art. 3 Abs. 1 Satz 1 Buchstabe b der Safe-Harbor-Entscheidung können die Datenschutzbehörden der EU-Mitgliedstaaten Datenübermittlungen an Safe-Harbor-zertifizierte US-Unternehmen u. a. aussetzen, wenn „eine hohe Wahrscheinlichkeit besteht, dass die (Safe-Harbor-Datenschutz-)Grundsätze verletzt werden" oder „wenn die fortgesetzte Datenübermittlung für die betroffenen Personen das unmittelbar bevorstehende Risiko eines schweren Schadens schaffen würde, und wenn die zuständigen Behörden in den Mitgliedstaaten die Organisation (Anm.: hiermit ist das datenempfangende US-Unternehmen gemeint) unter den gegebenen Umständen in angemessener Weise unterrichten und ihr Gelegenheit zur Stellungnahme geben." In etwa ähnliche Regelungen enthalten auch alle EU-Standardverträge.

Damit ist festzuhalten, dass sowohl der Safe-Harbor-Beschluss als auch die EU-Standardvertragsklauseln den Datenschutzbehörden der EU-Mitgliedstaaten jedenfalls für bestimmte extreme Fälle grundsätzlich die Möglichkeit eröffnen, Datenexporte in die USA bzw. generell in einen Drittstaat zu unterbinden, ungeachtet des Umstands, dass der Datenempfänger eine gültige Safe-Harbor-Zertifizierung besitzt oder mit ihm ein EU-Standardvertrag abgeschlossen wurde. Wir sind daher – wie auch die anderen Datenschutzbehörden in der EU – aufgerufen, die datenschutzrechtlichen Risiken für die von solchen Datenübermittlungen betroffenen Personen zu bewerten. Zu kritisieren ist insoweit allerdings, dass dem Safe-Harbor-Beschluss und auch den Standardverträgen kaum handhabbare, nähere Anhaltspunkte dazu zu entnehmen sind, für welche praktischen Fallgestaltungen die dort vorgesehenen behördlichen Befugnisse zur Aussetzung von Datenübermittlungen zum Tragen kommen sollen. Namentlich sind weder dem Safe-Harbor-Beschluss noch den Standardvertragsklauseln klare Aussagen dazu zu entnehmen, wie in diesem Zusammenhang mit Datenzugriffen ausländischer Nachrichtendienste oder anderer ausländischer Behörden umzugehen ist. Eine weitere Präzisierung könnte allerdings nur die EU-Kommission in Kenntnis der Auffassung der amerikanischen Seite durch Fortschreibung ihres Safe-Harbor-Beschlusses bzw. durch Überarbeitung der Standardvertragsklauseln vornehmen.

Auf der Grundlage der derzeitigen Erkenntnislage haben wir bislang keine Maßnahmen zur Aussetzung von Transfers personenbezogener Daten durch Unternehmen aus Bayern in die USA auf Grundlage von Art. 3 Abs. 1 Satz 1 Buchstabe b des Safe-Harbor-Entscheidung oder auf Grundlage ähnlicher Befugnisse aus den EU-Standardvertragsklauseln eingeleitet. Auch sind, jedenfalls auf Grund des gegenwärtigen Erkenntnisstandes, von hiesiger Seite derzeit keine entsprechenden Maßnahmen vorgesehen. Jedoch müssen und werden wir die weiteren Entwicklungen und insbesondere die aktuellen Verhandlungen der Kommission mit der US-Seite über eine Verbesserung des Safe-Harbor-Schutzstandards sorgfältig beobachten. Zudem stimmen wir uns in der Bewertung der Problematik eng mit den anderen Datenschutzbehörden in Deutschland und der EU ab. Anfragende Unternehmen weisen wir jedoch darauf hin, dass andere Datenschutzaufsichtsbehörden in Deutschland diese Frage anders als wir beurteilen könnten, auch wenn uns bisher noch keine Anordnungen anderer deutscher Datenschutzbehörden bekannt geworden sind, mit der eine Datenübermittlung in einen Drittstaat auf der Grundlage des Safe-Harbor-Abkommens oder von Standardver-

tragsklauseln aus Anlass der in Rede stehenden Problematik als datenschutzrechtlich unzulässig untersagt worden wäre.

Aus unserer Sicht können die von den Berichten über massive Datenzugriffe von US-Nachrichtendiensten aufgeworfenen schwerwiegenden datenschutzrechtlichen Fragen ihrer Art nach letztlich nur „systemisch" gelöst werden, nicht jedoch durch behördliche Einzelmaßnahmen, die nur einzelne Unternehmen betreffen würden. Denn letztlich geht es hierbei nicht primär um Datenschutzrisiken, die spezifisch bei einzelnen (US-)Unternehmen bestünden, sondern vielmehr um die vom US-amerikanischen Recht den dortigen Behörden generell eröffneten Befugnisse und deren Umsetzung in der dortigen Verwaltungspraxis. Eine derartige systemische, aus der Rechtsordnung und Verwaltungspraxis eines Drittstaates (USA) insgesamt erwachsende Problemlage kann unseres Erachtens kaum sinnvoll durch Einzelmaßnahmen von Datenschutzaufsichtsbehörden einzelner EU-Mitgliedstaaten begegnet werden; die nach Artikel 3 Abs. 1 Satz 1 Buchstabe b der Safe-Harbor-Entscheidung den Datenschutzbehörden der Mitgliedstaaten eröffneten Befugnisse sind nach unserer Auffassung nicht auf den Umgang mit solchen Datenschutzrisiken zugeschnitten, die einen Drittstaat als Ganzes betreffen, sondern auf spezifische Risiken, die für Datenexporte an ein bestimmtes Unternehmen aufgrund der spezifischen Gegebenheiten bei diesem Unternehmen bestehen.

Aus hiesiger Sicht ist daher ein genereller Ansatz erforderlich, bei dem den durch die Snowden-Berichten gewonnenen neuen Erkenntnissen bereits im Rahmen der Rechtsetzung auf EU-Ebene (insbesondere im Rahmen der kommenden EU-Datenschutzgrundverordnung) Rechnung getragen werden muss. Als weiterer Schritt sollten diese Erkenntnisse zur Überarbeitung aller datenschutzrechtlichen Instrumente führen, die für den Export personenbezogener Daten in Drittstaaten zur Verfügung gestellt werden, d. h. insbesondere der EU-Standardvertragsklauseln sowie der Safe-Harbor-Entscheidung. Namentlich sollte in diesen Instrumenten wesentlich stärker geklärt werden, welche Bedeutung der Frage von Datenzugriffen ausländischer Behörden bei der Beurteilung des Datenschutzniveaus im konkreten Fall zukommt. Die dringende Aufgabe der Klärung dieser Grundsatzfrage kommt letztlich der Europäischen Kommission zu, denn die Zuständigkeit im Hinblick auf die Anerkennung des Safe-Harbor-Regimes als „angemessenes Datenschutzniveau" liegt gemäß der EG-Datenschutzrichtlinie bei der Europäischen Kommission; gleiches gilt im Hinblick auf die Zurverfügungstellung von Standardvertragsklauseln.

Was Datenübermittlungen in die USA auf der Basis von „Safe Harbor" angeht, ist daher primär die Europäische Kommission aufgerufen, den von ihr unterbreiteten dreizehn Empfehlungen zur Verbesserung der Safe-Harbor-Grundsätze in den aktuellen Verhandlungen mit der US-Seite Nachdruck zu verleihen. Von besonderer Wichtigkeit sind hier vor allem die Empfehlungen zur Frage der Zugriffe von US-Behörden auf personenbezogene Daten, die aus der EU stammen. Die Kommission hatte insoweit betont, dass Zugriffe von US-Behörden für Zwecke der nationalen Sicherheit auf personenbezogene Daten, die aus der EU übermittelt worden sind, in einem künftigen Safe-Harbor-Regelwerk wesentlich klarer als bislang den Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit unterworfen werden müssen. Dieser Aspekt wird auch aus der Sicht der Artikel-29-Gruppe entscheidende Bedeutung besitzen für die Beurteilung der Ergebnisse der derzeitigen Verhandlungen zu „Safe Harbor" (vgl. dazu das Schreiben der Artikel-29-Gruppe an die Europäische Kommission vom 10.04.2014).

> > >
http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf

Ferner hat die Artikel-29-Gruppe unter anderem vorgeschlagen, dass die Kommission durch die US-Regierung künftig über alle US-amerikanischen Rechtsvorschriften informiert werden sollte, die für Safe-Harbor-zertifizierte US-Unternehmen dazu führen könnten, dass diese ihre durch die Safe-Harbor-Zertifizierung

eingegangenen Verpflichtungen nicht vollumfänglich erfüllen können.

Ungeachtet dessen ist darauf hinzuweisen, dass beim Europäischen Gerichtshof (EuGH) derzeit ein Verfahren anhängig ist, bei dem der EuGH aus Grundlage einer Vorlage des obersten irischen Gerichts (Irish High Court) vom 18.06.2014 über die Verbindlichkeit des Safe-Harbor-Beschlusses der Kommission vom 26.07.2000 zu entscheiden hat. Anlass hierfür war eine Klage, mit der der österreichische Jurist Max Schrems die irische Datenschutzaufsichtsbehörde vor dem Hintergrund von Darstellungen Edward Snowdens verpflichten wollte, gegen Datenübermittlungen von Facebook Ireland Ltd. an Facebook Inc. in den USA einzuschreiten. Facebook beruft sich bei diesen Übermittlungen auf seine Safe-Harbor-Zertifizierung. Der Irish High Court hatte die Auffassung vertreten, dass die irische Datenschutzbehörde an den Safe-Harbor-Kommissionsbeschluss gebunden sei und danach keine Maßnahmen einleiten könne; jedoch sah der Irish High Court Anlass, den Fall dem EuGH zur Klärung der Frage vorzulegen, ob die Safe-Harbor-Entscheidung im Lichte der Entwicklungen, die seit seinem Inkrafttreten stattgefunden haben, sowie im Lichte der Artikel 7 und 8 der Europäischen Grundrechtecharta, die das Recht auf Achtung der Privatsphäre und der Kommunikation sowie auf Schutz personenbezogener Daten beinhalten, noch als bindend angesehen werden könne.

Es ist zu hoffen, dass die Entscheidung des EuGH einen Beitrag zur weiteren Klärung der Frage leisten wird, welche Rolle den Datenschutzaufsichtsbehörden der Mitgliedstaaten – jedenfalls unter dem Safe-Harbor-Regime – im Zusammenhang mit der Frage von Datenzugriffen staatlicher US-Stellen zukommt. Für die praktische Arbeit der Datenschutzbehörden wäre eine weitere Klärung von großer Bedeutung.

15

Beschäftigtendatenschutz

15 Beschäftigtendatenschutz

15.1 Speicherdauer für krankheitsbedingte Fehlzeiten

Ein Arbeitgeber darf die krankheitsbedingten Fehlzeiten seiner Mitarbeiter grundsätzlich ein Jahr vorhalten, falls in einem Jahr die Fehlzeiten allerdings mehr als sechs Wochen betrugen, vier Jahre.

Wir erhielten eine Anfrage, ob der Arbeitgeber berechtigt ist, über einen Zeitraum von zehn Jahren eine Liste mit den Krankheitstagen des Arbeitnehmers in der Personalakte zu führen.

Das Vorhalten der krankheitsbedingen Fehlzeiten der Mitarbeiter in der Personalakte ist zulässig, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. Für den Arbeitgeber können die Fehlzeiten im Hinblick auf etwaige krankheitsbedingte Kündigungen oder im Hinblick auf seine Verpflichtung, ein betriebliches Eingliederungsmanagement nach § 84 Abs. 2 SGB IX anzubieten von Bedeutung sein. Nach der arbeitsgerichtlichen Rechtsprechung kann zur Begründung einer krankheitsbedingten Kündigung auf Fehlzeiten für einen Zeitraum von bis zu vier Jahren zurückgegriffen werden. Übersteigen in einem Jahr die Fehlzeiten sechs Wochen, dürfen die Fehlzeiten wegen einer potentiellen Kündigungsmöglichkeit vier Jahre vorgehalten werden, liegen sie darunter, so ist nur eine Dauer von einem Jahr zulässig. Datenschutzrechtlich ist die oben angesprochene Erforderlichkeit für die Durchführung oder Beendigung des Beschäftigungsverhältnisses nur gegeben, wenn der genannte zeitliche Rahmen eingehalten wird. Das Vorhalten der Krankheitstage über den vom Fragesteller genannten Zeitraum von zehn Jahren ist somit unzulässig.

15.2 Zweckwidrige Nutzung von Gehaltslisten zur Feststellung, ob Gewerkschaftsbeitrag bezahlt wird

Wenn ein Betriebsrat, der zugleich auch Gewerkschaftsmitglied ist, seine Zugriffsmöglichkeit auf die Gehaltsdaten zur Überprüfung nutzt, ob die Mitarbeiter, die ebenfalls Mitglied in der betreffenden Gewerkschaft sind, ihren Mitgliedsbeitrag entrichtet haben, ist dies unzulässig.

Wir wurden gefragt, ob es datenschutzrechtlich zu beanstanden wäre, wenn ein Betriebsrat, der zugleich Mitglied in einer DGB-Gewerkschaft ist, die Gehaltsdaten der Mitarbeiter, die ebenfalls Mitglied in der betreffenden Gewerkschaft sind, zur Überprüfung verwendet, inwieweit diese ihren satzungsmäßigen Gewerkschaftsbeitrag (1% vom Bruttolohn) zahlen.

Der Arbeitgeber gewährt dem Betriebsrat und damit auch dem betreffenden Betriebsratsmitglied den Zugriff auf die Gehaltsdaten der Mitarbeiter zulässigerweise, soweit dies zur Erfüllung der Aufgaben des Betriebsrats erforderlich ist. Der Betriebsrat benötigt diese, um im Rahmen der Mitbestimmung bei Eingruppierungen oder Gewährung sonstiger Gehaltsbestandteile Stellung nehmen zu können.

Da der Betriebsrat insoweit Teil der verantwortlichen Stelle ist, handelt es sich dabei um eine Datennutzung, die nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG gerechtfertigt ist.

Nutzt der Betriebsrat diese Gehaltsdaten zur Überprüfung, ob ein bestimmter Mitarbeiter seinen Gewerkschaftsbeitrag entrichtet hat, ist dies nicht mehr von dem gerechtfertigten Zweck umfasst und damit datenschutzrechtlich unzulässig.

15.3 Erfassung von Telefondaten durch Arbeitgeber

Wenn ein Arbeitgeber seinen Mitarbeitern Diensthandys zur Verfügung stellt und die Privatnutzung verbietet, kann er Einblick in die Einzelverbindungsnachweise nehmen, um die ihm diesbezüglich zustehenden Kontrollbefugnisse wahrnehmen zu können.

Ein Unternehmen hat seinen Mitarbeitern Diensthandys zur Verfügung gestellt und die private Nutzung dieser Handys verboten. Der Datenschutzbeauftragte fragte an, ob es zulässig sei, wenn der Arbeitgeber Einsicht in die Einzelverbindungsnachweise nehmen möchte, um z. B. das Verbot der Privattelefonie zu überwachen.

Der Arbeitgeber darf mit Mitarbeiterdaten umgehen, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. Zunächst ist zu berücksichtigen, dass hier die Privatnutzung verboten war, somit das Fernmeldegeheimnis nicht galt bzw. eine erhöhte Schutzbedürftigkeit der Mitarbeiter nicht gegeben war. Da der Arbeitgeber kraft seiner Stellung gewisse Kontrollbefugnisse hat, besteht für ihn auch eine Berechtigung, die von jedem Mitarbeiter dienstlich veranlassten Kosten aufgeschlüsselt nach Zeitpunkt und Dauer festzuhalten. Auch eine Kontrolle, ob unerlaubt Privatgespräche geführt wurden, kann in diesem Zusammenhang vorgenommen werden. Der Arbeitgeber hat gegenüber der Telefongesellschaft allerdings schriftlich zu erklären, dass er die Mitarbeiter diesbezüglich informiert hat und künftige Mitarbeiter informieren wird und dass der Betriebsrat beteiligt worden ist oder eine solche Beteiligung nicht erforderlich war (§ 99 TKG).

Fraglich ist, ob die Speicherung der kompletten Zielnummer zulässig ist. Zwischen Arbeitgeber und externen Gesprächspartnern der Mitarbeiter fehlt ein Vertragsverhältnis, das die Telefondatenerfassung rechtfertigen könnte. Auch von einer stillschweigenden Einwilligung kann nicht ausgegangen werden. Es ist folglich eine Abwägung der widerstreitenden Interessen von Arbeitgeber und Gesprächsteilnehmer nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG durchzuführen. Um insoweit Probleme zu vermeiden, empfiehlt es sich, nur die Vorwahl und einen Teil der Rufnummer des Gesprächspartners zu speichern, da dies für eine stichprobenartige Kontrolle – unter Rückfrage des Beschäftigten – regelmäßig ausreicht.

15.4 Nachweis der Betriebszugehörigkeit für Erhalt von Nachlässen bei Geschäften

Wenn ein Arbeitgeber seinen Mitarbeitern vergünstigte Einkaufsmöglichkeiten bei Geschäften in der Region verschafft, handelt sich um eine freiwillige Leistung. Mitarbeiter, die diese Vergünstigung in Anspruch nehmen wollen, können deshalb verpflichtet werden, ihren Firmenausweis (ohne Lichtbild) und Personalausweis in den Geschäften vorzulegen, um Missbrauch durch Überlassen des Firmenausweises an Unberechtigte zu verhindern.

Ein Unternehmen handelte bei diversen Geschäften in der Region für seine Mitarbeiter einen Sonderrabatt aus, wenn sie dort einkaufen. Die Mitarbeiter erhielten dazu einen Ausweis (ohne Lichtbild), auf dem sich ihr Name und die Bestätigung, dass sie bei dem betreffenden Unternehmen beschäftigt sind, befanden. Bei Vorlage des Ausweises sollten die Mitarbeiter dann den Rabatt erhalten. Ein bestimmtes Geschäft forderte allerdings vom Unternehmen eine Liste mit den Namen der Mitarbeiter, um einen Abgleich vornehmen und etwaigen Missbrauch verhindern zu können. Das Unternehmen fragte an, ob dies datenschutzrechtlich in Ordnung sei.

Da der Ausweis des Unternehmens kein Lichtbild enthält, bestand die Gefahr des Missbrauchs, indem ein Mitarbeiter seinen Ausweis einem unberechtigten Dritten gibt, der diesen dann beim Einkauf vorlegen und so in den Genuss des Rabatts kommen könnte. Unabhängig davon, dass wir keine Rechtsgrundlage

dafür gesehen haben, eine Mitarbeiterliste an die Partnergeschäfte zu übermitteln, könnte ein Missbrauch auch durch einen Abgleich von Firmen-Ausweis und Mitarbeiterliste nicht verhindert werden. Wir schlugen vor, dass ein Mitarbeiter neben den vom Unternehmen ausgestellten Firmenausweis noch seinen Personalausweis vorzuzeigen hätte. Dadurch wären eine Identifizierung der Person und eine Feststellung der Berechtigung eindeutig möglich.

Es handelt sich um eine freiwillige Angelegenheit des Arbeitgebers, wenn er seinen Mitarbeitern die Möglichkeit eines vergünstigten Einkaufs bei verschiedenen Geschäften bietet, so dass hier eine Einwilligungslösung möglich ist. Der Arbeitgeber kann die o. g. Identifizierungsbedingungen vorgeben, zu denen diese Vergünstigung zur Verfügung gestellt wird. Ist ein Mitarbeiter mit den Bedingungen nicht einverstanden, kann er die Vergünstigung nicht in Anspruch nehmen.

15.5 Kopie des Führerscheins durch Arbeitgeber

Ein Arbeitgeber darf die Führerscheine von Mitarbeitern kopieren, die Dienstfahrzeuge bei der Ausübung ihrer beruflichen Tätigkeit benutzen.

Ein Unternehmen fragte an, ob es berechtigt ist, die Führerscheine der Mitarbeiter, die mit dem Führen von Firmenfahrzeugen beauftragt sind oder denen ein Firmenfahrzeug für die Ausübung ihrer beruflichen Tätigkeit zur Verfügung gestellt wird, zum Zweck der Kontrolle zu kopieren.

Der Arbeitgeber darf Daten seiner Mitarbeiter erheben, verarbeiten oder nutzen, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist (§ 32 Abs. 1 Satz 1 BDSG). Den Arbeitgeber trifft die Pflicht, in gewissen Abständen zu prüfen, ob die Mitarbeiter, die mit Firmenfahrzeugen fahren, über einen gültigen Führerschein verfügen. Es sind Situationen denkbar, bei denen der Arbeitgeber nachweisen können muss, dass er sich vom Vorhandensein eines gültigen Führerscheins eines bestimmten Mitarbeiters überzeugt hat. Dabei kann es hilfreich sein, wenn er eine Kopie des Führerscheins zur Verfügung hat. Da zudem im Führerschein nur Daten enthalten sein dürften, die dem Arbeitgeber ohnehin schon bekannt sind bzw. die eher banal sind (z. B. Führerscheinklasse), halten wir es für vertretbar, wenn der Arbeitgeber den Führerschein kopiert.

15.6 Mithören von Telefongesprächen durch Arbeitgeber bei Markt- und Meinungsforschungsunternehmen

Der Arbeitgeber darf Telefongespräche der Mitarbeiter eines Markt- und Meinungsforschungsunternehmens in einem gewissen Umfang mithören, wenn er die Mitarbeiter allgemein darüber informiert hat und den Grundsatz der Verhältnismäßigkeit beachtet.

Eine Mitarbeiterin eines Markt- und Meinungsforschungsinstituts beschwerte sich darüber, dass ihre Telefongespräche teilweise mitgehört werden.

Das Mithören von Telefongesprächen ist ein Erheben von Mitarbeiterdaten, das nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig ist, wenn es zur Wahrnehmung berechtigter Interessen des Unternehmens erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der Betroffenen am Ausschluss des Datenumgangs überwiegen.

Bei einem Markt- und Meinungsforschungsinstitut besteht die Hauptaufgabe der Interviewer im Telefonieren. Der Geschäftserfolg lässt sich nur durch ein hohes Qualitätsniveau der Telefonate erzielen, so dass das Mithören der Gespräche in einem gewissen Umfang erforderlich ist. Der Grundsatz der Verhältnismäßigkeit war hier beachtet worden, da das Mithören nicht dauerhaft erfolgte. Bei neuen Interviewern oder erhöhtem Schulungsbedarf können die Kontrollen häufiger vorgenommen werden

als bei Interviewern mit sehr langer Berufserfahrung.

Die notwendige Transparenz gegenüber den Interviewern hinsichtlich des Mithörens war hier dadurch gewährleistet, dass sie im Vertrag umfassend darüber informiert wurden und außerdem eine Einverständniserklärung unterzeichneten. Dies hielten wir für ausreichend. Wenn das einzelne Mithören verdeckt erfolgte, war das insoweit unschädlich. Aufzeichnungen fanden nach Mitteilung des Unternehmens nicht statt.

Die Belange der Befragten werden durch das zeitweise Mithören telefonischer Interviews, ohne dass sie informiert werden, nicht verletzt. Die Befragten werden zu Beginn des Interviews über den Zweck des Telefonanrufs informiert und geben durch ihre Einwilligung in das Interview zu erkennen, dass sie mit der Auswertung ihrer Angaben durch das Forschungsinstitut einverstanden sind. Ein telefonisches Interview zu Zwecken der Markt- und Sozialforschung ist kein vertrauliches Gespräch zwischen zwei Privatpersonen, sondern seine Inhalte sind bei Wahrung der Anonymität der Befragten explizit für Dritte bestimmt. Die Anonymität der Befragten wurde hier dadurch gewahrt, dass ein Aufschalten des Supervisors erst nach der Kontaktphase erfolgte.

Insgesamt gesehen war somit die Vorgehensweise des Unternehmens beim Mithören der Telefongespräche datenschutzrechtlich nicht zu beanstanden.

15.7 Einschaltung von Personalberatern bei Bewerbungsverfahren

Wenn ein Unternehmen im Rahmen eines Bewerbungsverfahrens einen Personalberater einschaltet, hängt es von den konkreten Umständen ab, ob dieser Auftragsdatenverarbeiter oder eigene verantwortliche Stelle ist.

Ein Unternehmen, das als Personalberatung tätig ist, fragte an, inwieweit es mit Daten der Bewerber umgehen und diese an Dritte weitergeben darf.

Wir wiesen darauf hin, dass es dafür auf die Umstände des Einzelfalls ankomme. Es kann sein, dass Personalberater im Rahmen von Stellenausschreibungen lediglich die Bewerbungen entgegennehmen, nach bestimmten Vorgaben sortieren und an den Arbeitgeber weiterleiten. Sie sind dann Auftragsdatenverarbeiter. Als Verantwortlicher, auch hinsichtlich des Handelns des Personalberaters, tritt nur der Arbeitgeber den Bewerbern gegenüber auf und haftet gegebenenfalls. Das Erheben der Bewerberdaten wird dem Arbeitgeber zugerechnet, auch wenn es tatsächlich durch den Personalberater erfolgt. Die Überlassung der Bewerberunterlagen durch den Personalberater an den Arbeitgeber ist keine Übermittlung, sondern eine interne Weitergabe und deshalb datenschutzrechtlich unproblematisch. Der Personalberater muss sich an die Vorgaben des Arbeitgebers halten. Zwischen Arbeitgeber und Personalberater ist in diesen Fällen ein Vertrag zur Auftragsdatenverarbeitung abzuschließen, der die Voraussetzungen des § 11 Abs. 2 BDSG zu erfüllen hat. Den Bewerbern muss frühzeitig, also bei der Stellenausschreibung bzw. im Online-Bewerbungsbogen, mitgeteilt werden, dass deren Daten auch Dritte erhalten, die für den Arbeitgeber unterstützend tätig werden (§ 4 Abs. 3 BDSG, Auftragsdatenverarbeiter ist Empfänger).

Trifft der Personalberater aus dem Kreis der Bewerber eine Vorauswahl, hat also diesbezüglich eine eigene Entscheidungsfreiheit, liegt eine Funktionsübertragung vor. Er ist dann eine eigene verantwortliche Stelle, d. h. er erhebt die Bewerberdaten selbst und übermittelt dann die Unterlagen der in die engere Auswahl gekommenen Bewerber an den Arbeitgeber. Er darf insoweit die gleichen Daten erheben wie auch der Arbeitgeber selbst, also alle, die für die Entscheidung über die Begründung des Beschäftigungsverhältnisses erforderlich sind (§ 32 Abs. 1 Satz 1 BDSG). Die Bewerber müssen rechtzeitig darauf hingewiesen werden, dass ihre Daten nur zum Zweck des Bewerbungsprozesses erhoben, gespeichert, verarbeitet oder genutzt werden und im gleichen Rahmen an bestimmte Dritte, nämlich Unter-

nehmen, die eine Stelle zu besetzen haben, für die der Bewerber in Betracht kommt, ggf. auch Sozialversicherungsträger, denen gegenüber eine gesetzliche Mitteilungspflicht besteht, weitergegeben werden. Auch für die Zulässigkeit der Übermittlung von Bewerberdaten an den Arbeitgeber ist maßgeblich, inwieweit dieser die Daten für das weitere Procedere benötigt.

Das Erheben, Verarbeiten und Nutzen der Bewerberdaten ist bei Beachtung der obigen Ausführungen, insbesondere bei entsprechender Information der Bewerber über die Weitergabe ihrer Daten, deshalb möglich, weil ein rechtsgeschäftsähnliches Verhältnis zwischen dem Bewerber und dem Personalberater bzw. dem potentiellen Arbeitgeber mit dem Inhalt zustande kommt, dass die Bewerberdaten – je nach dem – vom Arbeitgeber an den Personalberater oder umgekehrt weitergegeben werden können.

16

Gesundheit und Soziales

16 Gesundheit und Soziales

16.1 Prüfungen von Arztpraxen

Wie im letzten Tätigkeitsbericht angekündigt, haben wir unsere Prüfungen von Arztpraxen auch in den vergangenen beiden Jahren fortgesetzt. Hierzu haben wir Arztpraxen an Hand eines Fragebogens einer schriftlichen Prüfung unterzogen und diese schriftliche Prüfung in einigen Fällen durch eine Vor-Ort-Kontrolle ergänzt.

Ärzte sind im Hinblick auf die nach § 203 StGB strafbewehrte Schweigepflicht in der Regel für die Belange des Datenschutzes erheblich stärker sensibilisiert als viele andere Berufsgruppen. Zugleich sind in Arztpraxen wegen der hohen Schutzbedürftigkeit von Gesundheitsdaten aber besonders strenge Anforderungen an den Datenschutz und die Datensicherheit zu erfüllen. In der Praxis besteht häufig Unsicherheit, welche konkreten Vorgaben sich aus den datenschutzrechtlichen Regelungen ergeben bzw. wie diese Vorgaben im Praxisalltag umzusetzen sind.

In dem Fragebogen, der unserer Prüfung von Arztpraxen häufig zugrunde liegt, werden Fragen der Praxisorganisation ebenso angesprochen wie materiell-rechtliche Themen des Datenschutzes und technisch-organisatorische Aspekte der Datensicherheit. Bei unseren Prüfungen haben wir festgestellt, dass bestimmte Punkte immer wieder besondere Herausforderungen für die Praxen darstellen oder nicht ausreichend berücksichtigt werden. In vielen Fällen lassen sich bereits durch vergleichsweise einfache Veränderungen große Verbesserungen erzielen.

Dies gilt insbesondere für den häufig zu beobachtenden Missstand, dass die unbefugte Kenntnisnahme von Patientendaten durch andere Patienten nicht konsequent genug durch geeignete Gegenmaßnahmen verhindert wird. Dies ist zugleich ein Manko, das im Rahmen von Eingaben uns gegenüber besonders oft von Bürgern bemängelt wird. So können wartende Patienten durch Sitzgelegenheiten in unmittelbarer Nähe des Empfangsbereichs bzw. infolge mangelnder Trennung von Empfangs- und Wartebereich Gespräche oder Telefonate des Praxispersonals mithören. Patientenakten werden oftmals vom Praxispersonal auf dem Empfangstresen oder im Behandlungszimmer für den Arzt bereit gelegt oder vom Arzt nach der Behandlung dort abgelegt; Patienten, die sich gerade am Empfang anmelden, können dadurch Daten anderer Patienten leicht einsehen. Gleiches gilt, wenn Bildschirme von Praxisrechnern oder von medizinischen Geräten so ausgerichtet sind, dass ohne größere Schwierigkeiten ein Mitlesen durch Dritte ermöglicht wird, oder bei Abwesenheit von Mitarbeitern nicht gesperrt werden. All diese Situationen bergen die Gefahr, dass Dritte sensible Patientendaten zur Kenntnis nehmen und dadurch gegen datenschutzrechtliche Vorschriften verstoßen wird. Organisatorische Veränderungen können hier oft Abhilfe leisten, ohne übermäßig stark in den Praxisbetrieb einzugreifen. Von zentraler Bedeutung für einen zuverlässigen Datenschutz in der Arztpraxis ist in jedem Fall die regelmäßige Schulung und Sensibilisierung der Mitarbeiter für die Erfordernisse eines datenschutzgerechten Umgangs mit Patientendaten.

Ein Punkt, der häufig übersehen wird, ist die angemessene Sicherung von Backupmedien vor unbefugtem Zugriff. Auch wenn Backupmedien in einem gesonderten Schrank oder Raum verschlossen werden, stellt dies allein im Falle eines Einbruchsdiebstahls keinen ausreichenden Schutz der darauf befindlichen Daten dar. Sind die auf einem Datenträger gespeicherten Daten nicht durch eine kryptographische Verschlüsselung gesichert, führt der Diebstahl eines Datenträgers mit Patientendaten grundsätzlich zu einer Datenpanne im Sinn des § 42a BDSG. Eine solche Datenpanne ist nicht nur gegenüber der Aufsichtsbehörde zu melden; auch die Betroffenen müssen von der Arztpraxis über den Verlust der Daten informiert werden. Dies bedeutet für die Arztpraxis nicht nur einen großen organisatorischen Aufwand, sondern kann auch mit einem erhebli-

chen Imageschaden einhergehen. Wurden die Daten hingegen verschlüsselt abgespeichert und dadurch ausreichend vor dem Zugriff unbefugter Dritter geschützt, kann in der Regel davon ausgegangen werden, dass für die schutzwürdigen Interessen der Betroffenen keine schwerwiegenden Beeinträchtigungen drohen und deshalb das Vorliegen einer meldepflichtigen Datenpanne im Sinn des § 42a BDSG zu verneinen ist.

Immer mehr Arztpraxen bieten ihren Patienten auf ihren Internetseiten den Service einer schnellen und einfachen Kontaktaufnahme per E-Mail oder Web-Formular an. Einige Arztpraxen stellen ihren Patienten mittlerweile auch Apps zur Verfügung. Patienten sollen dadurch unkompliziert Termine vereinbaren, Rezepte bestellen oder medizinische Informationen erhalten können. Einige Web-Formulare und Apps sehen dabei vor, dass die Patienten Angaben über ihre Person, unter Umständen auch über ihre Krankenversicherung oder ihren Gesundheitszustand machen und ggf. zur Konkretisierung ihrer Anfrage auch Fotos hochladen können. Ärzte weisen in diesem Zusammenhang oft darauf hin, dass Patienten zunehmend einen solchen Service erwarten, um ortsunabhängig und flexibel die benötigten Auskünfte zu erhalten. In vielen Fällen werden dabei aber die datenschutzrechtlichen Anforderungen unterschätzt, die bei der Umsetzung solcher Serviceangebote zu beachten sind. In jedem Fall bedarf es zur Sicherung des Transportwegs einer SSL/TLS-Verschlüsselung sowie des Einsatzes von Perfect Forward Secrecy, um auch ein nachträgliches Entschlüsseln zu erschweren. Dabei handelt es sich jedoch nur um Mindestmaßnahmen, die bei Arztpraxen angesichts des hohen Schutzbedarfs der betroffenen Daten in der Regel nicht ausreichen, um einen angemessenen Schutz der Daten zu gewährleisten. Soweit Arztpraxen Web-Formulare oder Apps einsetzen wollen, ist daher eine sorgfältige Prüfung im Einzelfall erforderlich, welche Maßnahmen ergriffen werden müssen, um die datenschutzrechtlichen Vorgaben, insbesondere die in der Anlage zu § 9 Satz 1 BDSG genannten Anforderungen, zu erfüllen. Bei der Kommunikation per E-Mail kann hierfür neben der ohnehin erforderlichen Transportverschlüsselung (s. o.) beispielsweise eine Ende-zu-Ende-Verschlüsselung eingesetzt werden. Hinweise zur sicheren E-Mail-Verschlüsselung und zu den hierfür geeigneten Verfahren S/MIME und PGP bzw. GPG finden sich auf den Internetseiten des Bundesamtes für Sicherheit in der Informationstechnik.

>>>
https://www.bsi.bund.de

16.2 Fernwartung medizinischer Geräte mit Einschaltung von Subunternehmern

Ein Vertrag zur Fernwartung von medizinischen Geräten, der auch die Einschaltung von Subunternehmern außerhalb der EU bzw. des EWR vorsieht, ist ausnahmsweise zulässig, wenn die Wartung bzw. der Einsatz des Subunternehmers für das einwandfreie Funktionieren der Geräte erforderlich ist und der Vertrag hierzu transparente Regelungen enthält.

Von einer Reihe von Krankenhäusern haben wir Anfragen zu einem Fernwartungsvertrag erhalten, der ihnen von einem Unternehmen, das medizinische Geräte herstellt, zur Unterschrift zugesandt worden war. Da das Unternehmen nicht ausschließen konnte, dass im Wartungsfall ein Zugriff auf personenbezogene Daten erfolgt, sollten mit diesem Vertrag die Anforderungen nach § 11 Abs. 5 BDSG erfüllt werden. Eine Besonderheit des Vertrags bestand darin, dass das Unternehmen als Auftragnehmer berechtigt sein sollte, zur Vertragserfüllung Subunternehmer einzusetzen; als Subunternehmer sollten dabei auch Unternehmen beauftragt werden dürfen, die ihren Sitz außerhalb der EU bzw. des EWR haben. Hierzu enthielt der Vertrag detaillierte Regelungen; für die Einschaltung von Subunternehmern mit Sitz außerhalb der EU bzw. des EWR sah der Vertrag u. a. den Abschluss eines sogenannten EU-Standardvertrags vor. Das Unternehmen begründete die Notwendigkeit, ggf. auch Subunternehmer in die Wartung einzubeziehen, insbesondere damit, dass in den medizinischen Geräten häufig Technologie anderer Unter-

nehmen zum Einsatz komme; in einem solchen Fall verfügten oftmals nur diese anderen Unternehmen über das technische Spezialwissen, um eine Wartung durchführen zu können. Vor diesem Hintergrund fragten Krankenhäuser bei uns nach, ob gegen die Unterzeichnung des vorgelegten Vertrags datenschutzrechtliche Bedenken bestünden und ob bzw. unter welchen Voraussetzungen auch Subunternehmer mit Sitz außerhalb der EU bzw. des EWR im Rahmen der Fernwartung eingeschaltet werden dürften.

Werden Unternehmen im Rahmen einer Fernwartung nach § 11 Abs. 5 BDSG tätig, sind sie grundsätzlich nicht als Dritte im Sinn des § 3 Abs. 8 Satz 2 BDSG anzusehen; dies hat zur Folge, dass Daten, die sie erhalten, nicht „übermittelt" werden und demnach hierfür keine gesonderte Rechtsgrundlage erforderlich ist. Abweichend hiervon sind beauftragte Unternehmen angesichts der Regelung in § 3 Abs. 8 Satz 3 BDSG jedoch dann als „Dritte" anzusehen, wenn sie ihren Sitz außerhalb der EU bzw. des EWR haben. Eine Beauftragung von Unternehmen außerhalb der EU bzw. des EWR ist daher trotz Vorliegens eines Vertrags nach § 11 BDSG nur dann zulässig, wenn eine Rechtsvorschrift die Datenübermittlung erlaubt oder der Betroffene eingewilligt hat. Als gesetzliche Rechtsgrundlage kommt im vorliegenden Fall insbesondere Art. 27 Abs. 5 des Bayerischen Krankenhausgesetzes in Betracht, wonach eine Übermittlung im Rahmen des Behandlungsverhältnisses zulässig ist. Das Behandlungsverhältnis erstreckt sich dabei nicht nur auf die durch den Arzt oder das sonstige Krankenhauspersonal durchgeführten Behandlungen, sondern umfasst auch das Bereitstellen ordnungsgemäß funktionierender Geräte, die eine einwandfreie Behandlung des Patienten gewährleisten sollen. Im Ergebnis kann daher die Fernwartung durch einen Subunternehmer außerhalb der EU bzw. des EWR ausnahmsweise als zulässig angesehen werden, wenn dies für das ordnungsgemäße Funktionieren medizinischer Geräte erforderlich ist. Wie bei jeder (Fern-)Wartung sind dabei zur Gewährleistung der Datensicherheit technische und organisatorische Maßnahmen zu treffen, die dem hohen Schutzbedarf der betroffenen Daten Rechnung tragen; insbesondere setzt die Möglichkeit, auf personenbezogene Daten zuzugreifen, eine Freischaltung durch das Krankenhaus voraus.

Um auch bei Unternehmen mit Sitz außerhalb der EU bzw. des EWR ein angemessenes Datenschutzniveau sicherzustellen, sah der Vertrag, der den Krankenhäusern zur Unterschrift vorgelegt wurde, hierfür den Abschluss von EU-Standardverträgen für Auftragsdatenverarbeiter gemäß der Kommissionsentscheidung 2010/87/EU vor. Damit das Krankenhaus auch bei der Beauftragung von Subunternehmern „Herr der Daten" bleibt, legten wir bei der Prüfung der Verträge zudem großen Wert darauf, dass das Krankenhaus transparent über die eingeschalteten Subunternehmer informiert wird und unter bestimmten Voraussetzungen auch ein Widerspruchsrecht gegen neue Subunternehmer erhält. Vor diesem Hintergrund haben wir darauf hingewirkt, dass das Krankenhaus nicht nur eine Liste der vom Auftragnehmer aktuell eingesetzten Subunternehmer einsehen kann, sondern auch über ggf. neu in die Wartungsprozesse eingebundene Subunternehmer in geeigneter Weise rechtzeitig informiert wird. Zudem muss das Krankenhaus grundsätzlich der Verwendung eines neuen Subunternehmers widersprechen können, wenn es gegen dessen Auswahl datenschutzrechtliche Bedenken hat; unter Umständen kann dies jedoch den Auftragnehmer zur Kündigung des Wartungsvertrags berechtigen, wenn der Wartungsvertrag infolge des Widerspruchs nicht mehr erfüllt werden kann.

Ein Wartungsvertrag, der die oben genannten Vorgaben erfüllt, ist daher aus unserer Sicht auch dann nicht zu beanstanden, wenn im Rahmen der Wartung auch Subunternehmer mit Sitz außerhalb der EU bzw. des EWR eingeschaltet werden können. Entscheidende Bedeutung kommt dabei jedoch der Tatsache zu, dass eine Wartung für das einwandfreie Funktionieren medizinischer Geräte und damit für die ordnungsgemäße Behandlung der Patienten erforderlich ist. Dieses Ergebnis ist damit nicht auf andere Konstellationen im Gesundheitswesen übertragbar, in denen externe Dienstleister zu anderen Zwecken, z. B. zur Archivierung, für Schreibarbeiten oder zur Abrechnung, eingeschaltet werden sollen.

16.3 Datenübermittlung von Hilfsmittelerbringern an Krankenkassen

Welche Daten Hilfsmittelerbringer im Rahmen der Abrechnung an gesetzliche Krankenkassen übermitteln dürfen, richtet sich allein nach § 302 Abs. 1 SGB V. Die Befugnis der Hilfsmittelerbringer, die hierfür erforderlichen Daten zu erheben, folgt aus § 294 SGB V.

Hilfsmittelerbringer, z. B. Orthopädie-Techniker oder Sanitätshäuser, erheben und verarbeiten im Rahmen der Leistungen für ihre Kunden häufig sensible Daten. Insbesondere im Rahmen der Abrechnung von Leistungen, die für gesetzlich Versicherte erbracht werden, bestehen oftmals Unsicherheiten, welche Daten vom Hilfsmittelerbringer an die Krankenkasse übermittelt werden dürfen, insbesondere ob die Übermittlung auch sensible medizinische Daten oder Fotos umfassen darf. Zudem wurde uns die Frage gestellt, auf welcher Rechtsgrundlage Hilfsmittelerbringer beim Betroffenen Daten erheben dürfen, wenn diese Daten von der Krankenkasse zwecks Abrechnung der Leistung benötigt werden.

Rechtsgrundlage für die Erhebung, Verarbeitung und Nutzung von Gesundheitsdaten durch Hilfsmittelerbringer ist grundsätzlich § 28 Abs. 7 Satz 3 BDSG, der ausdrücklich auf die Angehörigen von Berufen abstellt, deren Ausübung die Herstellung oder den Vertrieb von Hilfsmitteln mit sich bringt. Für das Abrechnungsverfahren mit den gesetzlichen Krankenkassen enthält das SGB V jedoch Spezialregelungen, die gemäß § 1 Abs. 3 Satz 1 BDSG den Vorschriften des BDSG vorgehen. So sind gemäß § 294 SGB V die Leistungserbringer verpflichtet, die für die Erfüllung der Aufgaben der Krankenkassen notwendigen Angaben, die aus der Erbringung von Versicherungsleistungen entstehen, aufzuzeichnen; „aufzeichnen" bedeutet im datenschutzrechtlichen Sinn, dass die entsprechenden Daten erhoben und gespeichert werden dürfen. Hinsichtlich der Mitteilung dieser Daten an die Krankenkassen verweist § 294 SGB V auf die nachstehenden Vorschriften, d. h. die §§ 295 ff. SGB V. So sind die Hilfsmittelerbringer nach § 302 Abs. 1 SGB V verpflichtet, den Krankenkassen die von ihnen erbrachten Leistungen zu bezeichnen und dabei u. a. die Verordnung des Arztes mit der Diagnose und den erforderlichen Angaben über den Befund anzugeben. Die Verpflichtung des Hilfsmittelerbringers, der Krankenkasse gegenüber die Leistungen „zu bezeichnen" und Daten „anzugeben", stellt datenschutzrechtlich die Befugnis des Hilfsmittelerbringers dar, diese Daten an die Krankenkasse zu übermitteln.

Der Umfang der zulässigen Datenerhebung und -verarbeitung richtet sich im Rahmen der Abrechnung mit den Krankenkassen allein nach diesen datenschutzrechtlichen Vorschriften des SGB V und kann auch mit Einwilligung des Versicherten nicht erweitert werden. Denn der Gesetzgeber hat mit den detaillierten Vorschriften zum Abrechnungsverfahren in der gesetzlichen Krankenversicherung eine abschließende Regelung getroffen, von der auch mit Einwilligung des Betroffenen nur dort abgewichen werden kann, wo dies im SGB V ausdrücklich vorgesehen ist (vgl. Urteil des BSG vom 10.12.2008, Az. B 6 KA 37/07 R). Der Vollständigkeit halber sei darauf hingewiesen, dass diese Einschränkung bezüglich der Zulässigkeit einer Einwilligung nur für Datenerhebungen und -verarbeitungen gilt, die Leistungserbringer im Zusammenhang mit Aufgaben nach dem SGB vornehmen. Für Datenerhebungen und -verarbeitungen, die in keinem direkten Zusammenhang mit der gesetzlichen Krankenversicherung bzw. mit der Erfüllung von Aufgaben nach dem SGB stehen, ist auch bei gesetzlich Versicherten ein Rückgriff auf die allgemeinen Regelungen des BDSG und somit eine Einwilligung nach § 4a BDSG möglich.

Auf der Grundlage des § 302 Abs. 1 SGB V dürfen nur die für die Abrechnung erforderlichen Angaben an die Krankenkasse übermittelt werden. Davon werden beispielsweise solche Daten nicht erfasst, die nicht für die Abrechnung der Leistung benötigt werden, sondern der Krankenkasse die Aufklärung ermöglichen sollen, ob ein drittverursachter Gesundheitsschaden (z. B. Behandlungs- oder Pflegefehler) vorliegt, auf Grund dessen der Krankenkasse möglicherweise Ansprüche gegen einen Dritten

zustehen. So befand sich in einem Fragebogen, den Hilfsmittelerbringer für eine Krankenkasse ausfüllen sollten und uns zur Prüfung vorgelegt haben, u. a. die Frage, wo der Dekubitus eines Patienten entstanden ist (z. B. Krankenhaus). Eine solche Mitteilung kann zwar an die Krankenkasse nach anderen Vorschriften (z. B. § 294a SGB V) zulässig sein, wenn die entsprechenden Voraussetzungen vorliegen. Da es sich dabei aber um keine zur Abrechnung der Leistung erforderliche Angabe über den Befund handelt, ist eine Übermittlung nach § 302 Abs. 1 SGB V unzulässig. Auch sensible medizinische Daten, deren Kenntnisnahme dem Medizinischen Dienst der Krankenversicherung (MDK) vorbehalten ist, dürfen nicht an die Krankenkasse übermittelt werden.

Diese Grundsätze gelten auch für die Frage, ob Hilfsmittelerbringer zur Veranschaulichung des Sachverhalts der Krankenkasse Fotos übermitteln dürfen. Denn auch bei einem Foto, das der Hilfsmittelerbringer von einem Körperteil des Kunden anfertigt, handelt es sich um ein personenbezogenes Datum, dessen Übermittlung sich nach den oben genannten datenschutzrechtlichen Vorschriften richtet. Vor diesem Hintergrund kann grundsätzlich auch die Übermittlung eines Fotos an die Krankenkasse nach § 302 Abs. 1 SGB V zulässig sein. Wie bei sonstigen Daten ist aber zu prüfen, ob es sich dabei um eine erforderliche Angabe über den Befund handelt bzw. ob wegen der besonderen Sensibilität der gemachten Aufnahme nur eine Übermittlung an den MDK in Betracht kommt. Ein Verfahren, das unabhängig von den Umständen des Einzelfalls generell die Übermittlung von Fotos an die Krankenkasse vorsieht, genügt diesen Anforderungen nicht. Welche Daten umgekehrt die Krankenkassen von den Leistungserbringern erheben dürfen, richtet sich nach den §§ 284 ff. SGB V; diese Frage entzieht sich jedoch angesichts der Tatsache, dass es sich bei den gesetzlichen Krankenkassen um öffentliche Stellen handelt, unserer Beurteilung.

16.4 Datenübermittlung von Ärzten an das Versorgungsamt

Übermittelt ein Arzt im Rahmen eines Schwerbehindertenverfahrens medizinische Unterlagen an ein Versorgungsamt, trägt er auch dann die Verantwortung für das Vorliegen einer wirksamen Einwilligungs- und Schweigepflichtentbindungserklärung des Patienten, wenn die Übermittlung der Unterlagen auf Ersuchen des Versorgungsamts erfolgt.

Im Rahmen von Verfahren zur Feststellung des Grads einer Behinderung ersuchen die Versorgungsämter regelmäßig die von den Antragstellern benannten Ärzte um Übersendung von aktuellen Befundberichten oder sonstigen medizinischen Unterlagen. Ärzte dürfen derartige Unterlagen nur dann an das anfragende Versorgungsamt übermitteln, wenn der Patient, d. h. der Antragsteller, eine entsprechende Einverständniserklärung abgibt, die den Arzt zugleich von seiner Schweigepflicht entbindet. Da die Patienten ihre Einwilligungserklärung in der Regel gegenüber dem Versorgungsamt abgeben, haben Ärzte bei uns angefragt, ob sie das Versorgungsamt um Vorlage (zumindest einer Kopie) der Einwilligungserklärung bitten müssen oder ob sie auf den Hinweis des Versorgungsamts vertrauen dürfen, dass der Patient eine solche Erklärung abgegeben hat. Den Anfragen der Ärzte lag ein Schreiben des Versorgungsamts zugrunde, wonach dessen schriftliche Zusage, dass die Übermittlung datenschutzrechtlich zulässig sei, für den Arzt genüge, um dem Ersuchen rechtmäßig nachzukommen. Da das Versorgungsamt als ersuchende Stelle dem Schreiben zufolge nach § 67d Abs. 2 Satz 2 SGB X bzw. § 15 Abs. 2 Satz 2 BDSG die Verantwortung für die Richtigkeit des Übermittlungsersuchens trage, entbinde die Befundanforderung des Versorgungsamts den Arzt von der Verpflichtung, die Einhaltung datenschutzrechtlicher Bestimmungen selbst zu prüfen. Die tatsächliche Vorlage der Entbindungserklärung werde weder vom SGB X noch von anderen Gesetzen gefordert.

Wir mussten die anfragenden Ärzte darauf hinweisen, dass wir diese rechtliche Einschätzung nicht teilen, sondern davon ausgehen, dass auch bei einem Ersuchen des Versorgungsamts der Arzt die Verantwortung für die Zulässigkeit der Datenübermittlung trägt. Insbesondere setzen die vom Versorgungsamt zitierten Vorschriften, wonach die Verantwortung auf die anfragende Stelle übergeht, voraus, dass die Übermittlung durch einen Sozialleistungsträger bzw. durch eine öffentliche Stelle erfolgt; auf eine Übermittlung durch nicht-öffentliche Stellen finden diese Vorschriften hingegen keine Anwendung. Da die Verantwortung nicht auf das Versorgungsamt übergeht, ist der Arzt nicht von seiner Verpflichtung entbunden, die Einhaltung datenschutz- und strafrechtlicher Bestimmungen selbst zu prüfen. Dem Versorgungsamt ist zwar insofern zuzustimmen, als das Vorliegen der Einwilligungserklärung beim Versorgungsamt genügt, um den Arzt von seiner Schweigepflicht zu entbinden und ihm die Übermittlung der betreffenden Daten zu erlauben. Auch der Hinweis des Versorgungsamtes, dass die tatsächliche Vorlage der Einwilligungserklärung weder vom SGB X noch von anderen Gesetzen gefordert wird, trifft zu. Die datenschutzrechtliche Verantwortung und insbesondere das strafrechtliche Risiko dafür, dass die Einwilligung tatsächlich vorliegt (und im Streitfall ggf. auch vorgelegt werden kann), trägt aber der Arzt. Vor diesem Hintergrund empfehlen wir Ärzten, sich vom Versorgungsamt die Einwilligungserklärung des Betroffenen vorlegen zu lassen.

16.5 Erhebung von Gesundheitsdaten durch einen Verein mittels Fragebogen

Auf die nach § 4a Abs. 1 Satz 3 BDSG erforderliche Schriftform einer datenschutzrechtlichen Einwilligung kann bei Datenerhebungen mittels Fragebögen verzichtet und eine konkludente Einwilligung durch Abgabe des Fragebogens als ausreichend angesehen werden. Allerdings setzt dies einen Hinweis auf die Freiwilligkeit der Abgabe und transparente Informationen über den Umgang mit den im Fragebogen erhobenen Daten voraus.

Um die Versorgungssituation von Menschen mit bestimmten Behinderungen durch konkrete Initiativen zu verbessern, hat ein Verein einen Fragebogen entwickelt und diesen im Internet veröffentlicht bzw. an Betroffene verschickt. Dabei wurden neben allgemeinen Angaben zur betroffenen Person, wie Name, Vorname und Geburtsjahr, Daten zur ärztlich festgestellten Diagnose, zum Grad der Behinderung und zur Pflegestufe abgefragt sowie Fragen zur aktuellen und erwünschten Versorgungssituation gestellt. Da der Fragebogen bzw. das Anschreiben keine konkreten Hinweise über den weiteren Umgang mit den erhobenen Daten enthielt, wurden wir auf die Angelegenheit aufmerksam gemacht und um Intervention gebeten.

Wir haben uns mit dem Verein in Verbindung gesetzt und den Verantwortlichen mitgeteilt, dass zwar die Abgabe eines Fragebogens als konkludente Einwilligung in die Verwendung der Angaben angesehen werden kann, jedoch nur, wenn die Betroffenen vorher transparent über den geplanten Datenumgang informiert wurden. Ein entsprechender Hinweis sollte neben Informationen, welche Daten ggf. an wen übermittelt werden, auch Ausführungen über die Maßnahmen zur Datensicherheit (z. B. wo werden die Fragebögen aufbewahrt und wie werden sie gesichert, wer hat Zugriff auf die Fragebögen, wie lange werden die Daten aufbewahrt usw.) enthalten.

Da zum Zeitpunkt unseres Tätigwerdens die Abgabefrist für den Fragebogen fast abgelaufen war und bereits Rückmeldungen eingegangen waren, war eine Änderung des Fragebogens bzw. des dazugehörigen Anschreibens nicht mehr möglich. Wir haben den Verein deshalb dazu angehalten, die erforderlichen datenschutzrechtlichen Hinweise zumindest nachzureichen und den Teilnehmern – anstelle einer Einwilligung – ausnahmsweise eine nachträgliche Widerspruchsmöglichkeit einzuräumen. Dies wurde vom Verein umgesetzt, wobei

das Informationsschreiben in Abstimmung mit uns erstellt wurde.

Grundsätzlich ist festzuhalten, dass die freiwillige Abgabe eines Fragebogens als konkludente Einwilligung in die Verwendung der gemachten Angaben anzusehen ist. Dies kann jedoch nur gelten, wenn ausreichend und transparent über den vorgesehenen Umgang informiert wird. Wir haben den Verein für den Fall weiterer Fragebogenaktionen auf diese ausführliche Hinweispflicht hingewiesen.

16.6 Einschaltung von ärztlichen Verrechnungsstellen

Bedient sich ein Arzt für die Abrechnung bei privat Versicherten einer ärztlichen Verrechnungsstelle, ist hierfür vom Patienten eine Einwilligungs- und Schweigepflichtentbindungserklärung einzuholen. Diese Erklärung ist häufig fehlerhaft.

Im Gegensatz zu gesetzlich Versicherten rechnen Ärzte bei privat Versicherten direkt mit dem Patienten ab. Um sich von dem mit der Rechnungsstellung verbundenen Verwaltungsaufwand zu entlasten, schalten Ärzte teilweise hierauf spezialisierte Unternehmen, sogenannte ärztliche Verrechnungsstellen, ein. Die Rechtslage für die Datenübermittlung an die ärztliche Verrechnungsstelle ist eigentlich klar: Patientendaten dürfen nur mit einer wirksamen Einwilligungs- und Schweigepflichtentbindungserklärung des Betroffenen dorthin übermittelt werden. Dennoch erreichen uns hierzu regelmäßig Beschwerden. Hier die häufigsten Fehlerquellen:

- **Fehlende Freiwilligkeit**

  Die nach § 4a Abs. 1 Satz 1 BDSG erforderliche Freiwilligkeit ist nur dann gewährleistet, wenn dem Patienten eine echte Wahlmöglichkeit verbleibt. Erklärt sich ein Patient nicht mit der Datenübermittlung an die ärztliche Verrechnungsstelle einverstanden, muss deshalb sichergestellt sein, dass die Rechnungsstellung durch die Praxis selbst erfolgen kann oder die medizinische Versorgung auf andere Weise gewährleistet ist.

- **Mangelnde Transparenz**

  Der Betroffene muss umfassend und verständlich darüber informiert werden, wie mit seinen Daten umgegangen wird. Diesbezüglich wurden uns im Berichtszeitraum Formulare vorgelegt, in denen die ärztliche Verrechnungsstelle nicht ausreichend konkret benannt wurde. Auch war den Formularen oft nicht zu entnehmen, welche Daten im Einzelnen übermittelt werden sollen. Insbesondere wurden Patienten in einigen Fällen nicht darüber informiert, dass Gesundheitsdaten, z. B. in Form von Diagnosen, an die ärztliche Verrechnungsstelle übermittelt werden. § 4a Abs. 3 BDSG schreibt jedoch vor, dass sich die Einwilligung ausdrücklich auf besondere Arten personenbezogener Daten im Sinn des § 3 Abs. 9 BDSG, also insbesondere auf Angaben über die Gesundheit, beziehen muss, wenn sie den Umgang mit diesen Daten rechtfertigen soll.

- **Fehlende Schriftform**

  Die Einwilligung bedarf nach § 4a Abs. 1 Satz 3 BDSG der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Im normalen Praxisalltag sind solche besonderen Umstände nicht erkennbar, weil der Patient persönlich anwesend ist und ohne Weiteres die Einwilligungserklärung unterschreiben kann. Eine mündliche Einwilligung oder ein Aushang im Wartezimmer genügt deshalb nicht.

- **Keine ausreichende Hervorhebung**

  § 4a Abs. 1 Satz 4 BDSG fordert eine besondere Hervorhebung, wenn eine datenschutzrechtliche Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden soll. Wird für die Einwilligungserklärung zur Datenübermittlung an die Verrechnungsstelle kein gesondertes Formblatt verwendet, sondern ist sie beispielsweise in einen allgemeinen Patientenaufnahmebogen

mit Fragen zu Vorerkrankungen, zur Medikation, etc. integriert, muss die datenschutzrechtliche Einwilligungserklärung deutlich vom allgemeinen Teil getrennt werden. In jedem Fall ist die Einwilligungserklärung mit einer aussagekräftigen Überschrift zu versehen. Darüber hinaus bedarf es einer zusätzlichen optischen Hervorhebung. Je nach Gestaltung des Formulars kommt hierfür eine farbliche Hinterlegung, eine Umrandung o. ä. in Frage.

- **Fehler in Sonderfällen, z. B. bei gesetzlich Versicherten**

  Immer wieder führen auch Fehler im Einzelfall dazu, dass ohne die erforderliche Einwilligung und damit unbefugt Patientendaten an eine ärztliche Verrechnungsstelle übermittelt werden. In einem Fall wurde beispielsweise übersehen, dass auch bei einem gesetzlich Versicherten eine Einwilligung zur Abrechnung über die Verrechnungsstelle dann erforderlich ist, wenn seine Behandlung nicht über die gesetzliche Krankenkasse abgerechnet, sondern die Rechnung vom Patienten selbst oder von einer privaten Zusatzversicherung beglichen wird; die Arztpraxis übermittelte in diesem Fall die Daten wie bei einem privat Versicherten zwecks Abrechnung an die Verrechnungsstelle, ohne hierfür jedoch eine Einwilligung einzuholen. Zur Vermeidung solcher Fehler ist es dringend anzuraten, in jedem Fall vor einer Datenübermittlung zu prüfen, ob die erforderliche Einwilligung eingeholt wurde und im Beschwerdefall nachgewiesen werden kann.

16.7 Identifizierung von Patienten mittels Foto oder Ausweiskopie

16.7.1 Identifizierung mittels Foto

Ein Foto, das in den Patientenstammdaten zu Identifizierungszwecken gespeichert werden soll, darf von einer Arztpraxis nur mit Einwilligung des Betroffenen aufgenommen werden.

Nach unserem Eindruck gehen Ärzte zunehmend dazu über, in der Patientenakte zu den Patientenstammdaten auch ein Foto des Patienten zu speichern. Als Begründung für dieses Vorgehen geben die Ärzte an, damit einem Missbrauch der Krankenversicherungskarte vorbeugen zu wollen oder sich anhand des Fotos besser an den Patienten erinnern zu können, z. B. wenn es später zu einem nicht persönlichen Kontakt mit dem Patienten kommen sollte.

Um für solche Zwecke ein Foto von Patienten aufnehmen und dieses in der Patientenakte speichern zu dürfen, bedarf es mangels gesetzlicher Erlaubnis einer Einwilligung des Betroffenen. Vor Erteilung der Einwilligung muss der Betroffene dabei ausreichend über die Zweckbestimmung der Datenerhebung, die Freiwilligkeit und die Möglichkeit eines Widerrufs informiert werden.

16.7.2 Identifizierung mittels Ausweiskopie

Das Erstellen und Speichern einer Ausweiskopie ist zur Identifizierung des Patienten nicht erforderlich und deshalb nicht zulässig.

Ein für die Rentenversicherung als Gutachter tätiger Arzt hat die Forderung der Rentenversicherung, die Identität der begutachteten Person zu prüfen, dahingehend verstanden, dass dies durch eine Ausweiskopie belegt werden muss. Aus diesem Grund kopierte er den vorgelegten Ausweis des Betroffenen gegen dessen Willen und speicherte diese Kopie in der Patientenakte.

Nachdem sich der Betroffene bei uns beschwerte, teilten wir dem Arzt mit, dass das Kopieren eines Ausweises nur in Ausnahmefällen zulässig sei (siehe dazu Kapitel 13.3). Insbesondere bestand im vorliegenden Fall trotz der Forderung der Rentenversicherung, die Identi-

tät der begutachteten Person zu prüfen, keine gesetzliche Verpflichtung zum Erstellen einer Ausweiskopie. Um zu vermeiden, dass sich in betrügerischer Absicht eine andere Person zur Begutachtung vorstellt, genügt es vielmehr, das Ausweisdokument einzusehen und die erfolgte Identitätsprüfung durch einen kurzen Vermerk in der Patientenakte zu dokumentieren. Auf unseren Hinweis hin hat uns der Arzt bestätigt, künftig von der bisherigen Verfahrensweise abzusehen, sämtliche Ausweiskopien vernichtet und eingescannte Dokumente gelöscht zu haben.

16.8 GPS für Demenzkranke

Der Einsatz von GPS-Ortungsgeräten bei demenzkranken Patienten kann deren Bewegungsfreiheit und Sicherheit verbessern, wirft aber datenschutzrechtliche Fragen auf.

Pflegeeinrichtungen erwägen seit kurzem bei demenzkranken Menschen den Einsatz von GPS-Ortungsgeräten (beispielsweise als kleine Sender im Gürtel oder am Arm), um sie im Notfall orten zu können. Dadurch soll es Demenzkranken, die krankheitsbedingt die Orientierung verlieren können, ermöglicht werden, sich auch ohne Begleitung sicher außerhalb des Heims zu bewegen. Der Einsatz eines solchen Geräts wirft aber nicht nur datenschutzrechtliche Fragen auf, sondern betrifft ganz allgemein den Umgang mit demenzkranken bzw. pflegebedürftigen Menschen. Technische Hilfsmittel bringen Pflegebedürftigen, ihren Angehörigen und Pflegekräften erhebliche Erleichterungen, können aber persönliche Fürsorge nicht gänzlich ersetzen. Auch im Hinblick auf die Würde des Menschen, die zugleich einer der Grundpfeiler des Rechts auf informationelle Selbstbestimmung ist, sind dem Einsatz technischer Geräte, die der Kontrolle demenzkranker Menschen dienen, daher Grenzen gesetzt.

Welche rechtlichen Anforderungen im Einzelnen zu beachten sind, hängt maßgeblich von der konkreten Ausgestaltung der Ortung ab. Denkbar ist es, das Gebiet um das Pflegeheim mit einem sogenannten Geo-Zaun zu markieren („Geofencing"); wird dieser Geo-Zaun überschritten, d. h. der voreingestellte Bereich verlassen, erfolgt beispielsweise per SMS eine Benachrichtigung des Heims. Von entscheidender Bedeutung ist dabei die Größe des umgrenzten Bereichs, in dem sich der Betroffene bewegen kann, ohne eine Meldung auszulösen und damit das Heim zu benachrichtigen. Ist der zugelassene Bewegungsradius sehr eng, kann dies einer unterbringungsähnlichen Maßnahme gleichkommen, für die ggf. eine betreuungsrichterliche Genehmigung erforderlich ist. Alternativ zu einem solchen Geofencing ist es möglich, den Betroffenen mit einem GPS-Sender auszustatten, dessen Position nur in Notfällen abgefragt wird. Dabei ist sicherzustellen, dass – abgesehen von Notfällen – kein Zugriff auf die Standortdaten erfolgt bzw. dass solche Zugriffe protokolliert werden; auch im Übrigen bedarf es ausreichender technischer und organisatorischer Maßnahmen, um die Sicherheit der Daten zu gewährleisten und Missbrauch vorzubeugen. Durch die Möglichkeit der Ortung dürfen zudem weder permanente Bewegungsprofile erstellt noch Dritte, die mit dem Betroffenen Zeit verbringen, überwacht werden. Grundvoraussetzung ist in jedem Fall das Vorliegen einer wirksamen Einwilligung, die bei demenzkranken Menschen in der Regel von deren Betreuer eingeholt werden muss.

16.9 Datenaustausch zwischen Zahnarztpraxen und Dentallaboren

Der Datenaustausch zwischen Zahnarztpraxen und Dentallaboren war Gegenstand einer Prüfungsaktion, in deren Rahmen 70 Zahnarztpraxen schriftlich befragt wurden.

Geprüft wurde im Wesentlichen, ob bzw. welche personenbezogenen Daten an Dentallabore übermittelt werden, in welcher Form die Daten ausgetauscht werden und ob bei der elektronischen Übertragung die Daten verschlüsselt werden. Aus dieser Prüfungsaktion möchten wir an dieser Stelle zwei Punkte, die

Übermittlung des Patientennamens an das Dentallabor sowie die Datensicherheit bei der elektronischen Rechnungsversendung vom Labor an den Zahnarzt, aufgreifen:

16.9.1 Übermittlung des Patientennamens an das Dentallabor

Dem Ergebnis der Prüfung zufolge übermitteln die meisten Zahnärzte den Patientennamen – zumindest im Papierauftrag – an das beauftragte Dentallabor. Als gesetzliche Rechtsgrundlage für diese Übermittlung kommt § 28 Abs. 7 Satz 2 BDSG in Betracht. Danach richtet sich die Zulässigkeit einer Übermittlung von personenbezogenen Gesundheitsdaten nach den für die Ärzte geltenden Geheimhaltungspflichten, d. h. nach den einschlägigen berufsrechtlichen Regelungen. Nach § 7 Abs. 1 der Berufsordnung für die Bayerischen Zahnärzte (BO) hat der Zahnarzt die Pflicht, über alles, was ihm in seiner Eigenschaft als Zahnarzt anvertraut oder bekannt geworden ist, gegenüber Dritten Verschwiegenheit zu wahren. § 12 Abs. 3 BO sieht jedoch die Möglichkeit der Weitergabe von Patientendaten an vor-, mit- oder nachbehandelnde Zahnärzte oder Ärzte vor, soweit das Einverständnis des Patienten vorliegt. Dieses Einverständnis ist – anders als die datenschutzrechtliche Einwilligung nach § 4a BDSG – an keine gesetzliche Form gebunden, weshalb es auch mündlich oder konkludent erteilt werden kann. Eine konkludente Einwilligung setzt zumindest voraus, dass der Patient darüber informiert wird, welches externe Labor beauftragt wird, und er dem nicht widerspricht. Durch ein solches Einverständnis wird der Zahnarzt zugleich von seiner strafbewehrten Schweigepflicht nach § 203 Abs. 1 Nr. 1 StGB befreit. Auch wenn die Schriftform demnach nicht vorgeschrieben ist, ist dies aus Nachweisgründen dennoch empfehlenswert.

16.9.2 Datensicherheit bei der Rechnungsversendung vom Labor an den Zahnarzt

Für die erbrachten Leistungen stellt das Labor dem Zahnarzt häufig (auch) einen elektronischen Abrechnungsdatensatz zur Verfügung. Hintergrund ist die Tatsache, dass die Vertragszahnärzte mit der Kassenzahnärztlichen Vereinigung nur noch papierlos abrechnen und hierfür die Laborabrechnungsdaten auch in elektronischer Form benötigen. Im Hinblick auf die bei der Übermittlung der Daten zu gewährleistende Datensicherheit wurde uns gegenüber die Ansicht vertreten, dass die bei der Auftragserteilung verwendete Auftragsnummer eine anonyme elektronische Datenübermittlung ermögliche und deshalb die Labordaten beispielsweise in Form einer XML-Datei ohne Verschlüsselung per E-Mail an die Zahnarztpraxis übermittelt werden könnten. Diese Auffassung teilen wir nicht.

Vom System ist vorgesehen, jeden Laborauftrag mit einer Auftragsnummer zu versehen, die zwar nicht den Klarnamen des Patienten, aber die in der Zahnarztpraxis verwendete Patientennummer enthält. Bei dieser Auftragsnummer handelt es sich um ein Pseudonym im Sinn des § 3 Abs. 6a BDSG. Denn nach der gesetzlichen Definition ist Pseudonymisieren das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren. Eine Anonymisierung im Sinn des § 3 Abs. 6 BDSG wird mit der Auftragsnummer nicht erreicht, denn der Auftrag muss zumindest in der Zahnarztpraxis wieder dem jeweiligen Patienten zugeordnet werden können; zudem kann in vielen Fällen auch das Labor den Patienten bestimmen, wenn der Zahnarzt im Laborauftrag auch den Patientennamen mitgeteilt hat. Da der Patient somit bestimmbar ist, sind die Labordaten als personenbezogene Daten im Sinn des § 3 Abs. 1 BDSG anzusehen.

Nach Nr. 4 der Anlage zu § 9 Satz 1 BDSG (Weitergabekontrolle) muss gewährleistet werden, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Eine Maßnahme in diesem Sinn ist gemäß Satz 3 der Anlage zu § 9 Satz 1 BDSG insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren. Mit der Pseudonymisierung der Datensätze wird

zwar insofern ein gewisser Schutz erreicht, als Angreifer nicht ohne Weiteres in der Lage sind, die Labordaten einer bestimmten Person zuzuordnen. Dies allein genügt jedoch nicht den Anforderungen an eine sichere Datenübermittlung. Zudem kann eine Pseudonymisierung keinen Schutz vor einem unbefugten Ändern oder Entfernen der Daten gewährleisten. Im Rahmen unserer technischen Bewertung haben wir es deshalb für die Versendung von pseudonymisierten Laborabrechnungsdaten als erforderlich, aber auch als ausreichend angesehen, den Übertragungskanal zu verschlüsseln (SSL-/TLS mit Perfect Forward Secrecy); eine zusätzliche Verschlüsselung der Inhalte vor der Übertragung der Daten haben wir nicht gefordert, sofern die an der Transportverschlüsselung beteiligten Systeme ein annähernd gleiches Sicherheitsniveau wie bei einer Inhaltsverschlüsselung gewährleisten.

17

Vereine und Verbände

17 Vereine und Verbände

17.1 Veröffentlichung der Ergebnisse von Sportwettkämpfen aus dem Amateurbereich im Internet

Die Veröffentlichung von Ergebnissen von Sportwettkämpfen aus dem Amateurbereich im Internet ist zwar – zumindest grundsätzlich – auch ohne Einwilligung zulässig, sofern es sich um öffentlich ausgetragene Wettkämpfe handelt. Die Veröffentlichung ist jedoch zeitlich zu begrenzen.

Immer häufiger erreichen uns Eingaben von Vereinsmitgliedern sowie Beratungsanfragen von Sportvereinen zur Frage der Zulässigkeit der Veröffentlichung von Ergebnissen von (Sport-)Wettkämpfen mit personenbezogenen Daten im Internet. So fragte uns ein Segelsportverein, ob und ggf. wie lange er Ergebnisse einer von ihm veranstalteten Regatta auf seiner Homepage veröffentlichen dürfe.

Da Veröffentlichungen personenbezogener Daten im Internet einen wesentlich höheren Verbreitungsgrad als sonstige Veröffentlichungen haben, greifen sie wesentlich stärker in die Datenschutzinteressen der Betroffenen ein als bspw. Veröffentlichungen in der Vereinszeitung. Daher ist die Internetveröffentlichung personenbezogener Daten von „einfachen Vereinsmitgliedern" zu Themen, die das Vereinsleben betreffen (wie z. B. Ehrungen, Jubiläen) grundsätzlich nur mit vorheriger Einwilligung des Betroffenen zulässig. Für die Internetveröffentlichung von Wettkampfergebnissen und persönlicher (z. B. sportlicher) Leistungen von Vereinsmitgliedern im Amateur- und Breitensportbereich wäre dies allerdings zu eng. Denn hierbei ist auch zu berücksichtigen, dass sportliche Wettkämpfe, die von einem Verein oder Verband ausgerichtet werden, jedenfalls in der Regel öffentliche Veranstaltungen darstellen, so dass es sich insoweit um „allgemein zugängliche Daten" handelt, deren Veröffentlichung daher an § 28 Abs. 1 Satz 1 Nr. 3 BDSG zu messen ist. Die schutzwürdigen Interessen der Betroffenen gebieten es aber auch bei solchen Daten, Internetveröffentlichungen nur für eine begrenzte Zeit als zulässig anzusehen. Pauschale Aussagen im Hinblick auf die zulässige Veröffentlichungsdauer sind indessen kaum möglich. Kriterien hierfür können etwa u. a. der Grad des öffentlichen Interesses am betreffenden Wettkampf, die Spiel- bzw. Wettkampfklasse („Liga") und die allgemeine Sensibilität der Daten sein. Was die Datenkategorien betrifft, wird in der Regel nur die Veröffentlichung des Namens, der Vereinszugehörigkeit und des Wettkampfergebnisses zulässig sein.

Organisiert ein Verein eine öffentlich zugängliche Wettkampfveranstaltung, an der auch Mitglieder anderer Vereine teilnehmen, wird man im Hinblick auf eine Veröffentlichung der Ergebnisse durch den veranstaltenden Verein keinen Unterschied zwischen den eigenen Mitgliedern und den Mitgliedern anderer Vereine machen müssen. Denn die Wettkampfergebnisse stellen bei den Angehörigen beider Gruppen gleichermaßen allgemein zugängliche personenbezogene Daten dar.

In dem uns vorgelegten konkreten Fall ging es um eine jährlich stattfindende Segelregatta. Hier haben wir die Veröffentlichung der Ergebnisse für eine Dauer von zwei Jahren auf der Homepage des veranstaltenden Vereins für noch vertretbar erachtet. Bei anderen Wettkämpfen könnte jedoch – je nach Fall – unter Umständen eine (ggf. auch deutlich) kürzere Dauer geboten sein.

Bei der Veröffentlichung von Wettkampf- und Spielergebnissen Minderjähriger kann jedoch die Interessenabwägung unter Umständen, insbesondere je nach Alter, zu Gunsten der minderjährigen Teilnehmer bzw. Spieler ausfallen, so dass § 28 Abs. 1 Satz 1 Nr. 3 BDSG nicht als Erlaubnis herangezogen werden kann. In solchen Fällen bedarf es einer Einwilligung der gesetzlichen Vertretung des minderjährigen Kindes.

17.2 Veröffentlichung des E-Mail-Verkehrs zwischen einzelnen Vereinsmitgliedern für alle Vereinsmitglieder

Bei der Kommunikation per E-Mail unter Vereinsmitgliedern muss der Absender grundsätzlich nur damit rechnen, dass die von ihm als Empfänger einer E-Mail bestimmten Personen Kenntnis von der E-Mail erhalten. Die Weiterleitung solcher E-Mails an alle Vereinsmitglieder ist ohne entsprechende Einwilligung des Absenders jedenfalls in der Regel unzulässig.

Mehrere bei uns eingegangene Beschwerden betrafen Fälle, in denen einige Mitglieder eines Vereins miteinander per E-Mail kommuniziert hatten und dann einzelne Mitglieder solche E-Mails an andere Vereinsmitglieder weitergeleitet hatten.

Bei der Kommunikation per E-Mail muss ein Absender zumindest in der Regel nur damit rechnen, dass die von ihm als Adressaten gezielt angeschriebenen Personen Kenntnis von der E-Mail und deren Inhalt erlangen, nicht jedoch auch andere Personen.

Dies gilt grundsätzlich auch für die Kommunikation unter Mitgliedern eines Vereins und in der Regel auch dann, wenn die E-Mail (auch) Angelegenheiten betrifft, die als solche grundsätzlich auch anderen Vereinsmitgliedern in der Mitgliederversammlung mitgeteilt werden könnten. Denn daraus kann nicht automatisch geschlossen werden, dass der gesamte Inhalt der E-Mail an andere Vereinsmitglieder bekannt gegeben werden darf. Die Kommunikation wird mit den vom Absender im "An" bzw. "cc"-Feld angegebenen Personen geführt, die übrigen Vereinsmitglieder sind im Verhältnis dazu "Dritte". Die Weiterleitung von E-Mails an Letztere stellt daher eine Übermittlung personenbezogener Daten (jedenfalls auch) des Absenders dar, die gemäß § 4 Abs. 1 BDSG nur mit Einwilligung des Absenders oder bei Eingreifen einer erlaubenden Rechtsvorschrift zulässig ist.

In der Regel ist die Weiterleitung der E-Mail an andere Vereinsmitglieder nicht „zur Durchführung des Mitgliedvertrages erforderlich", so dass die Übermittlung nicht auf § 28 Abs. 1 Satz 1 Nr. 1 BDSG gestützt werden kann. Ob „berechtigte Interessen" des (ursprünglichen) Empfängers oder eines Dritten eine Übermittlung an andere Vereinsmitglieder rechtfertigen können (§ 28 Abs. 1 Satz 1 Nr. 2 oder Abs. 2a BDSG) ist eine Frage des Einzelfalls, dürfte aber im Ergebnis eher selten zu bejahen sein. Der Absender hat jedenfalls in vielen Fällen ein überwiegendes schutzwürdiges Interesse daran, dass die in seiner E-Mail enthaltenen Informationen nicht an „Dritte" weitergegeben werden.

Ausnahmen hiervon sind im Einzelfall denkbar, etwa wenn der Verein – als „Dritter" – gemäß § 28 Abs. 2 Nr. 2a BDSG ein berechtigtes Interesse an der Veröffentlichung einer derartigen E-Mail geltend machen könnte, namentlich sofern es sich weitgehend (oder gar ausschließlich) um vereinsinterne Sachverhalte handelt. Die Veröffentlichung wird jedoch auch hier in einer Reihe von Fällen am Überwiegen schutzwürdiger Interessen des Absenders scheitern. Wenn etwa der Absender in der E-Mail persönliche Wertungen oder andere potentiell kontroverse Aussagen getätigt hat, bei denen davon auszugehen ist, dass er sie etwa in einer Mitgliederversammlung nicht in derselben Art und/oder mit einem weitgehend ähnlichen Wortlaut tätigen würde, dürften die gewichtigeren Gesichtspunkte meist gegen die Zulässigkeit der Veröffentlichung sprechen.

Dies haben wir in mehreren bei uns eingegangenen Beschwerden dieser Art so bewertet. Die Beschwerdeführer hatten sich in den entsprechenden E-Mails z. T. kritisch und mit sehr dezidierter Wortwahl über einzelne Vereinsmitglieder bzw. -funktionsträger geäußert. Es kann nicht schlicht unterstellt werden, dass sie sich in derselben Weise und mit weitestgehend demselben Wortlaut auch z. B. in einer Mitgliederversammlung geäußert hätten.

Letztlich kommt es auf den Einzelfall an. Die Veröffentlichung ist aber jedenfalls dann nicht zulässig, wenn sich der E-Mail-Verfasser explizit dahingehend geäußert hat, dass er einer Veröf-

fentlichung der E-Mail z. B. in einem etwaigen „Mitgliederforum“ o. ä. nicht zustimmt.

17.3 Zulässige Kommunikation unter Vereinsmitgliedern

Meinungsäußerungen sind am Maßstab des Grundrechts auf Meinungsfreiheit zu beurteilen; dem Datenschutzrecht sind hierfür grundsätzlich keine eigenständigen Maßstäbe zu entnehmen. Steht eine tatsächliche Behauptung im Vordergrund, greift hingegen das Datenschutzrecht.

In mehreren Fällen erhielten wir – gerade aus Vereinen – Beschwerden darüber, dass sich jemand per E-Mail gegenüber anderen Personen kritisch über den jeweiligen Beschwerdeführer geäußert hatte. Die Beschwerdeführer sahen in der – aus ihrer Sicht unberechtigten oder überzogenen – Kritik gleichzeitig einen „datenschutzrechtlichen Verstoß“ und baten uns um aufsichtliche Reaktion.

In anderen Fällen monierten Beschwerdeführer Tatsachenbehauptungen durch andere Vereinsmitglieder, die nach Ansicht des jeweiligen Beschwerdeführers so nicht zutreffend seien.

Derartige Fälle sind zunächst am Maßstab der Meinungsfreiheit zu beurteilen. Es liegt nicht schon darin eine unzulässige Übermittlung personenbezogener Daten, dass Vereinsmitglieder miteinander (z. B. per E-Mail) kommunizieren und hierbei Mitglied A als Absender gegenüber Mitglied B als Empfänger eine Meinungsäußerung über (z. B.) Mitglied C tätigt; Meinungsäußerungen sind von der Meinungsfreiheit gedeckt, solange die Äußerung nicht gegen Strafgesetze (insbesondere den Straftatbestand der Beleidigung) verstößt. Die rechtlichen Maßstäbe für die Bewertung der Zulässigkeit von Meinungsäußerungen sind daher grundsätzlich nicht dem Datenschutzrecht zu entnehmen. Ist eine Aussage danach von der Meinungsfreiheit gedeckt, stellt sie keinen datenschutzrechtlichen Verstoß dar. Die Verantwortung für den Inhalt und die Form zwischenmenschlicher Kommunikation liegt bei der Person, die die Äußerung tätigt.

Bei Tatsachenbehauptungen kann freilich eine „unzulässige Übermittlung personenbezogener Daten“ vorliegen, wenn der Übermittelnde dem Empfänger eine Mitteilung über einen Dritten macht und diese Mitteilung im Einzelfall weder aufgrund Einwilligung des Dritten noch aufgrund einer Rechtsvorschrift zulässig ist. Sehr häufig hängt die datenschutzrechtliche Beurteilung von einer Interessenabwägung im konkreten Einzelfall ab, so dass sich pauschale Aussagen erübrigen. Was Tatsachenbehauptungen im Rahmen von Kommunikation unter Vereinsmitgliedern angeht, wird man berücksichtigen müssen, dass unter Umständen alle Mitglieder ein Interesse an bestimmten Informationen haben können, die (zumindest auch) Vereinsangelegenheiten betreffen, auch wenn eine solche Mitteilung auch Tatsachbehauptungen über andere Vereinsmitglieder enthält. Die datenschutzrechtliche Zulässigkeit solcher Mitteilungen kann jedoch letztlich nur im Einzelfall beurteilt werden.

17.4 Veröffentlichung von Kontaktdaten von Vereinsmitgliedern gegenüber anderen Vereinsmitgliedern

Ob ein Verein bestimmte Kontaktdaten der Mitglieder allen anderen Mitgliedern zur Kenntnis geben darf, richtet sich nach dem Einzelfall. Maßgeblich ist vor allem der satzungsmäßige Vereinszweck.

Die Mitglieder eines Vereins sind im Verhältnis zueinander „Dritte“, so dass eine Bekanntgabe von Kontaktdaten eines Vereinsmitglieds an andere Vereinsmitglieder datenschutzrechtlich eine Übermittlung personenbezogener Daten ist. Im Berichtszeitraum erreichten uns mehrere Eingaben von Vereinsmitgliedern, die mit der Bekanntgabe bestimmter ihrer personenbezogenen Daten durch den Verein an andere Mitglieder nicht einverstanden waren.

Ein Mitglied in einem Luftsportverein beschwerte sich bei uns darüber, dass der Verein in einer Datenbank die Telefonnummern aller

aktiven Vereinsmitglieder (Piloten) hinterlegt hatte. Jedes aktive Mitglied hatte darauf Zugriff. Der Verein begründete dies damit, dass andere Piloten die Möglichkeit haben sollten, für den Fall etwaiger (im sog. Bordbuch einzutragender) technischer Vorkommnisse bei Bedarf telefonisch kurzfristig ergänzende Fragen an das Mitglied zu stellen, das die Eintragung vorgenommen hat. Dies sei im Interesse der Sicherheit erforderlich. Zudem sollen bestimmte für die Flugleitung verantwortliche Personen für den Fall, dass eine Maschine vermisst werde, die Möglichkeit haben, grundsätzlich alle Piloten telefonisch zu kontaktieren. Aus Sicht des Beschwerdeführers war dies jedenfalls nicht zwingend erforderlich.

Dieser Fall zeigt, wie schwierig die datenschutzrechtliche Beurteilung gerade beim Umgang mit personenbezogenen Daten durch Vereine häufig ist. Im vorliegenden Fall gab es zwischen den Beteiligten unterschiedliche Auffassungen darüber, wie wichtig die telefonische Kontaktmöglichkeit für alle Piloten untereinander ist.

Durch Einholung einer Stellungnahme der Luftfahrtaufsichtsbehörde haben wir geklärt, dass jedenfalls eine gesetzliche Verpflichtung zur Bekanntgabe von Telefonnummern in der dargestellten Weise nicht bestand. Letztlich mag man in derartigen Fällen – wie auch die Beteiligten – unterschiedlicher Meinung darüber sein, ob die Bekanntgabe der Telefonnummern auf diese Weise „zur Durchführung des Vertragsverhältnisses", das zwischen den Vereinsmitgliedern besteht, oder aufgrund berechtigter Interessen des Vereins bzw. seiner Mitglieder erforderlich ist. Eine explizite vereinsinterne Regelung zur Bekanntgabe von Kontaktdaten an andere Vereinsmitglieder – etwa in der Vereinssatzung, in einer „Datenschutzordnung" o. ä. – lag im konkreten Fall jedoch nicht vor. Die Vereinsführung hat uns zwar nachvollziehbar dargestellt, dass es für die Bekanntgabe der Telefonnummern plausible Gründe gibt, sofern jedoch ein Vereinsmitglied damit nicht einverstanden ist, bringt es sein Interesse am Unterbleiben der Bekanntgabe zum Ausdruck. Welche Interessen überwiegen, ist nicht leicht zu beurteilen. Jedoch sollte bedacht werden: Wenn der Beschwerdeführer im vorliegenden Fall mit der Veröffentlichung nicht einverstanden ist, wäre denkbar, dass der Verein die Auffassung vertritt, ihm unter diesen Umständen mit Berufung auf Sicherheitsgründe die Benutzung des vereinseigenen Flugplatzes und/oder von Maschinen nicht mehr zu erlauben. Ein solcher Streit wäre – sofern anderweitig keine Einigung gelingt – letztlich nur auf zivilrechtlichem Weg zu lösen. Mit datenschutzrechtlichen Mitteln konnte die Meinungsverschiedenheit daher nach unserer Auffassung nicht beigelegt werden.

Um die mit der Interessenabwägung verbundenen Schwierigkeiten zu vermeiden, haben wir dem Verein empfohlen, eine ausdrückliche Regelung dahingehend zu treffen, dass die Benutzung des Flugplatzes bzw. von Maschinen nur unter der Voraussetzung zulässig ist, dass der Pilot eine Telefonnummer angibt, unter der er grundsätzlich für Rückfragen in den dargestellten Fällen erreichbar ist. Liegt eine solche vereinsinterne Regelung vor, so kann sie die entsprechende Datenverarbeitung grundsätzlich legitimieren, da der Verein unter Inanspruchnahme der grundgesetzlich verbürgten Vereinsfreiheit (Art. 9 Abs. 1 GG) befugt ist, seine Angelegenheiten durch interne Regelungen frei zu gestalten, solange die getroffenen Regelungen die Grundrechte der Betroffenen – etwa das Recht auf informationelle Selbstbestimmung – nicht willkürlich oder grob unangemessen begrenzen. Trifft der Verein eine entsprechende ausdrückliche Regelung, so wäre die Bekanntgabe der Telefonnummer zur Durchführung des zwischen den Vereinsmitgliedern und dem Verein bestehenden mitgliedschaftlichen Verhältnisses erforderlich und somit grundsätzlich nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG gerechtfertigt; auf die (schwierige) Abwägung zwischen dem Interesse des Mitglieds und dem Vereinsinteresse (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG) käme es dann nicht mehr an.

17.5 Übermittlung der Kontaktdaten von Vereinsmitgliedern an Dachverbände

Für die Übermittlung personenbezogener Daten von Vereinsmitgliedern an Dachverbände ist häufig eine Einwilligung des Betroffenen erforderlich.

Ein Mitglied eines Sportvereins monierte, dass sein Verein personenbezogene Daten der Vereinsmitglieder an Dachverbände weitergebe, ohne dass den Vereinsmitgliedern eindeutig bekannt sei, welche Daten für welche Zwecke übermittelt würden.

Wir holten eine Stellungnahme des Vereins ein. Dieser fügte seiner Stellungnahme auch Stellungnahmen mehrerer Dachverbände bei. Es stellte sich heraus, dass der Verein im Wesentlichen Namen, Adressen und Geburtsdaten sowie z. T. ausgeübte Sportart der Vereinsmitglieder an (mehrere) Dachverbände übermittelte. Den Mitgliedern waren – soweit für uns ersichtlich – jedenfalls nicht alle Zwecke der Übermittlungen bekannt gegeben worden.

Einer der Dachverbände teilte mit, Namen, Adressen, Geburtsdaten sowie die ausgeübte Sportart aller Mitglieder der angeschlossenen Mitgliedsvereine zu benötigen, um die vom Verein an den Dachverband zu leistenden Mitgliedsbeiträge ermitteln zu können. Diese Beiträge bemessen sich ausweislich der Satzung des Dachverbands nach der Zahl der Mitglieder des Mitgliedsvereins sowie deren Sparte (Sportart).

Wir forderten den Mitgliedsverein auf, seine eigenen Mitglieder über diese Übermittlung an den Dachverband angemessen zu informieren. Die Betroffenen müssen gemäß § 4 Abs. 3 Nr. 2 BDSG bereits bei bzw. vor Eintritt in den Verein die Möglichkeit haben, diese Information zur Kenntnis zu nehmen. Der Verein musste zudem sicherstellen, dass darüber hinausgehende Daten (z .B. Telefonnummern) von der Übermittlung an den Dachverband ausgenommen werden.

Der Dachverband teilte zudem mit, dass er von bestimmten Funktionsträgern der Mitgliedsvereine zusätzlich Telefonnummern und E-Mail-Adressen benötige, um in eiligen Fällen Kontakt aufnehmen zu können. Nach unserer Auffassung kann dies zwar bei Funktionsträgern ein legitimer Zweck im Sinne von § 28 Abs. 1 Satz 1 Nr. 2 BDSG sein, der die Übermittlung rechtfertigen kann; die Betroffenen müssen jedoch über diese Übermittlung und ihre Zwecke gemäß § 4 Abs. 3 Satz 1 Nrn. 2 und 3 BDSG transparent informiert werden und es ist ihnen ein Recht zum Widerspruch gegen die Übermittlung einzuräumen. Nur unter diesen Voraussetzungen darf davon ausgegangen werden, dass die Funktionsträger, die insoweit nicht widersprochen haben, keine überwiegenden schutzwürdigen Interessen am Unterbleiben der Übermittlung ihrer Telefonnummer bzw. E-Mail-Adresse an den Dachverband haben.

Der Verein wurde von uns aufgefordert, eine umfassende, abschließende und verständliche Übersicht darüber zu erstellen, welche personenbezogenen Daten von Vereinsmitgliedern an welche Dachverbände für welche Zwecke übermittelt werden, und aktuelle und künftige Mitglieder unter Verwendung dieser Übersicht umfassend zu informieren.

17.6 Anforderung einer Urkunde im Rahmen satzungsgemäßer Aufgabenerfüllung in einem Verband

Bestimmte Funktionsträger, denen innerhalb eines Verbands nach geltendem Verbandsrecht bestimmte Aufgaben zukommen, dürfen grundsätzlich personenbezogene Daten erheben, ohne die sie diese Aufgabe nicht erfüllen können.

Die Teilnehmerin eines von einem Verband ausgerichteten Wettkampfs beschwerte sich bei uns über einen sog. Leistungsrichterobmann des Verbandes. Der Obmann, so die Eingabeführerin, habe sich einige Tage nach dem Wettkampf telefonisch an sie gewandt

und sie unter Vorspiegelung unzutreffender Tatsachen veranlasst, ihm ihre (beim Wettkampf erhaltene) Leistungsurkunde per Fax zuzuleiten; dies habe sie getan. Nachträglich habe sie festgestellt, dass der Obmann keine Zuständigkeit besessen habe, die Urkunde von ihr anzufordern, zudem habe er ihr gegenüber im Hinblick auf den Grund seines Ersuchens falsche Angaben gemacht. Die Eingabeführerin vertrat daher die Auffassung, der Obmann habe unberechtigt personenbezogene Daten zu ihrer Person erhoben bzw. sich die Daten sogar erschlichen.

Im Zuge unserer Überprüfung konnten die von der Eingabeführerin erhobenen Vorwürfe nicht bestätigt werden; vielmehr zeigte sich folgender Sachverhalt:

Einige Tage nach dem Wettkampf hatte sich ein anderer Wettkampfteilnehmer mit einem Einspruch gegen den (bei jenem Wettkampf agierenden) Leistungsrichter an den Leistungsrichterobmann gewandt. Der Einspruchsführer hatte dabei den Vorwurf erhoben, der Leistungsrichter habe die Leistungsurkunde einer anderen Wettkampfteilnehmerin – namentlich der Eingabeführerin, die sich später an uns wenden sollte – nachträglich rechtswidrig abgeändert, konkret die vergebene Punktzahl nachträglich erhöht. Wie unsere Prüfung ergab, war der Leistungsrichterobmann gemäß geltendem Verbandsrecht für die Prüfung eines derartigen Vorwurfs gegen den Leistungsrichter zuständig; Wettkampfteilnehmer können Einsprüche, in denen derartige Verstöße von Leistungsrichtern moniert werden, beim zuständigen Leistungsrichterobmann einreichen.

Es zeigte sich, dass der Leistungsrichterobmann im vorliegenden Fall die Leistungsurkunde bei der Eingabeführerin offenbar deshalb angefordert hatte, um aufgrund des bei ihm eingegangenen Einspruchs gemäß seiner Zuständigkeit den Vorwurf einer unzulässigen nachträglichen Abänderung der Leistungsurkunde durch den Leistungsrichter zu untersuchen. Die entsprechende Zuständigkeit war verbandsrechtlich ausdrücklich so festgelegt, wie ein Blick in die Verbandssatzung bestätigte. Da der Obmann im Rahmen seiner Zuständigkeit gehandelt hatte, stellte die Anforderung der Leistungsurkunde keinen datenschutzrechtlichen Verstoß dar. Für den (weiteren) seitens der Eingabeführerin gegen den Obmann erhobenen Vorwurf, dieser habe sie mit sachlich unwahren Angaben zur Übersendung der Urkunde aufgefordert, fanden sich im Rahmen unserer Prüfung keine Belege.

Dieser Fall zeigt exemplarisch die – gerade im Vereins- und Verbandsbereich nicht untypischen – mitunter erheblichen Schwierigkeiten, die für die Datenschutzaufsichtsbehörde angesichts sich bisweilen widersprechender Tatsachenbehauptungen der Beteiligten und vor dem Hintergrund spezifischen Verbandsrechts bestehen.

18

Wohnungswirtschaft und Mieterdatenschutz

18 Wohnungswirtschaft und Mieterdatenschutz

18.1 Weitergabe von Mieterdaten in Mieterhöhungsschreiben

Soweit zur Begründung einer Mieterhöhung Vergleichswohnungen zu benennen sind, dürfen diese auch so konkret bezeichnet werden, dass deren Mieter ohne nennenswerte Schwierigkeiten aufgefunden werden können.

Ein Mieter wandte sich an uns und monierte, dass sein Vermieter in einem Mieterhöhungsschreiben die Anschriften dreier anderer Wohnungen einschließlich Namen der Mieter, der Wohnfläche und der Grundmiete dieser Wohnungen angegeben hatte. Diese Angaben dienten zum Nachweis der ortsüblichen Vergleichsmiete und wurden vom Vermieter allen Mietern, bei denen er eine Mieterhöhung anstrebte, zugesandt.

Mieterhöhungsverlangen müssen gemäß § 558a Abs. 2 des Bürgerlichen Gesetzbuches (BGB) begründet werden. In § 558a Abs. 2 Nr. 4 BGB wird den Vermietern die Möglichkeit eröffnet, die Begründung anhand von drei Vergleichswohnungen vorzunehmen. Erfolgt die Begründung in dieser Weise, so soll der Mieter durch die Benennung einzelner Wohnungen die Möglichkeit haben, sich über die Vergleichswohnungen zu informieren und die behauptete Vergleichbarkeit nachzuprüfen (BGH, Urteil vom 18.12.2002, Az. VIII ZR 141/02). Die Vergleichswohnungen müssen deshalb so genau bezeichnet werden, dass der Mieter sie ohne nennenswerte Schwierigkeiten auffinden kann. Wenn sich in einem Mehrfamilienhaus mit mehreren Geschossen auf derselben Ebene mehr als eine Wohnung befindet, sind nach Auffassung des BGH für die Auffindbarkeit der Wohnung über die Angabe der Adresse und des Geschosses hinaus weitere Angaben erforderlich. Solche Angaben könnten z. B. die Lage der Wohnung im Geschoss, die Bezeichnung einer nach außen hin erkennbaren Wohnungsnummer oder der Name des Mieters sein.

Der Vermieter hat ein berechtigtes Interesse daran, ein Mieterhöhungsverlangen so zu begründen, dass es vor Gericht bestand hat. Aus § 558a Abs. 2 Nr. 4 BGB lässt sich mithin entnehmen, dass der Vermieter ein von der Rechtsordnung anerkanntes Interesse hat, die von ihm benannten Vergleichswohnungen so genau zu beschreiben, wie es erforderlich ist, damit die Begründung seines Mieterhöhungsverlangens rechtswirksam ist. Die Adressaten der Mieterhöhungsschreiben wiederum haben ein berechtigtes Interesse, die Berechtigung eines gemäß § 558a Abs. 2 Nr. 4 BGB begründeten Mieterhöhungsverlangens nachprüfen zu können, indem sie die genannten Vergleichswohnungen auffinden können.

Zwar haben die Mieter der Vergleichswohnungen, die im Mieterhöhungsschreiben angegeben werden, ein grundsätzlich schutzwürdiges Interesse dahingehend, dass ihre personenbezogenen Daten, die in derartigen Fällen auch die Privatsphäre betreffen und gewisse Rückschlüsse auf ihre Wohn- und Lebensverhältnisse zulassen, grundsätzlich nicht an Dritte bekannt gegeben werden. Dieses Interesse ist jedoch gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG mit dem o. g. berechtigten Interesse des Vermieters sowie gemäß § 28 Abs. 2 Nr. 2a BDSG mit dem o. g. berechtigten Interesse des Adressaten des Mieterhöhungsverlangens abzuwägen. Im Hinblick auf diese Abwägung ist § 558a Abs. 2 Nr. 4 BGB letztlich die gesetzliche Wertung zu entnehmen, dass dem Informationsinteresse des Adressaten eines Mieterhöhungsverlangens sowie dem Interesse des Vermieters an einer rechtlich tragfähigen Begründung seines Mieterhöhungsverlangens ein so hoher Stellenwert zukommt, dass demgegenüber das Interesse des Mieters der benannten Vergleichswohnung zurückstehen muss.

Die Mitteilung der Namen der zu Vergleichszwecken herangezogenen Mieter im Erhöhungsschreiben sowie weiterer Angaben, die im Hinblick auf die Beurteilung der Vergleichbarkeit der Wohnungen erforderlich sind, ist daher gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG und Abs. 2 Nr. 2a BDSG durch berechtigte Inte-

ressen des Vermieters und der Adressaten von Mieterhöhungsverlangen gerechtfertigt; einer (vorherigen) Zustimmung der Mieter, die als Vergleichsmieter benannt werden, bedarf es dabei nicht.

18.2 Verifizierung des Einkommens durch Zuleitung eines ausgefüllten „Mieterfragebogens" an Arbeitgeber des Mieters

Ein Vermieter darf Eigenangaben eines Mieters über sein Einkommen ohne Einwilligung des Mieters nicht an dessen Arbeitgeber zum Zwecke der Verifizierung übermitteln.

Ein Vermieter schickte den ausgefüllten Mieterfragebogen, worin ein Mieter vor Abschluss des Mietvertrags u. a. die Höhe seines Nettoeinkommens eingetragen hatte, ohne Wissen des Mieters an dessen Arbeitgeber und bat ihn, zu bestätigen, dass die Eigenangaben des Mieters zutreffend sind. Der Mietvertrag lief bereits seit mehreren Jahren; der Mieter zahlte seinen Mietzins ordnungsgemäß, hatte aber zuletzt wegen eines behaupteten Mangels die Miete gemindert.

Die Übermittlung war unzulässig. Zwar darf der Vermieter die Höhe des Nettoeinkommens erfragen und – jedenfalls, sofern der Mietvertragsabschluss unmittelbar bevorsteht – vom Mieter auch die Vorlage von Gehaltsnachweisen verlangen; Letzteres hatte der Vermieter allerdings seinerzeit vor Vertragsschluss nicht getan. Dies berechtigt ihn nicht, nach Abschluss des Mietvertrags bei ordnungsgemäßem Zahlungsverhalten des Mieters die Eigenangabe des Mieters gegenüber dem Arbeitgeber mitzuteilen. Da der Mieter seine Mietzahlungspflichten ordnungsgemäß erfüllte, fehlte es bereits an einem berechtigten Interesse des Vermieters im Sinne von § 28 Abs. 1 Satz 1 Nr. 2 BDSG an der Übermittlung. Dass dem Arbeitgeber die tatsächliche Einkommenshöhe seines Arbeitnehmers – des Mieters – bekannt ist, ändert hieran nichts. Denn die Eigenangabe stellt als solche ein (gegenüber der tatsächlichen Einkommenshöhe) eigenständiges personenbezogenes Datum des Mieters dar.

18.3 Übermittlung von Adressdaten von Wohnungseigentümern durch Verwalter einer Wohnungseigentümergemeinschaft (WEG) an die anderen Wohnungseigentümer

Immer wieder gibt es Streit über die Mitteilung von Kontaktdaten von Eigentümern einer Wohnungseigentümergemeinschaft (WEG) durch den Verwalter an andere Eigentümer. Die Rechtsprechung erkennt zwar ein umfassendes Einsichtsrecht des einzelnen Eigentümers in die Verwaltungsunterlagen der WEG an. In bestimmten Fällen kann es für den Verwalter dennoch geboten sein, bestimmte Kontaktdaten der einzelnen Eigentümer nicht an andere Eigentümer weiterzugeben.

Mehrere Beschwerden betrafen die Übermittlung von Adressdaten von Mitgliedern von Wohnungseigentümergemeinschaften an die anderen Mitglieder durch den Verwalter der WEG.

Der einzelne Wohnungseigentümer in einer Wohnungseigentümergemeinschaft hat ein umfassendes Einsichtsrecht in die Verwaltungsunterlagen der WEG (BGH, Urteil vom 11.02.2011, Az. V ZR 66/10). Inhaltliche Beschränkungen dieses Einsichtsrechts z. B. dergestalt, dass bestimmte Daten dabei nicht eingesehen werden dürften, sind der Rechtsprechung, soweit ersichtlich, nicht zu entnehmen. Die Rechtsprechung betont bisweilen sogar, dass das Datenschutzrecht der Einsichtnahme nicht entgegensteht. So hat das Landgericht Nürnberg-Fürth im Beschluss v. 27.10.2006 (Az: 14 T 4826/06; vom OLG München als nächsthöhere Instanz mit Beschluss v. 09.03.2007, Az. 32 Wx 177/06 bestätigt) ausdrücklich erklärt,

dass jeder Wohnungseigentümer ein Recht auf Einsicht in sämtliche Verwaltungsunterlagen einschließlich der Einzelabrechnungen aller Wohnungseigentümer hat, ohne dass hierbei datenschutzrechtliche Einschränkungen zu beachten wären. Das OLG München betont in der o.g. Entscheidung: „Diesem Anspruch (Anm.: auf Einsicht in die Verwaltungsunterlagen) steht das Bundesdatenschutzgesetz nicht entgegen, da die Wohnungseigentümergemeinschaft keine anonyme Gemeinschaft ist und die Einsichtnahme dem Zweck des Gemeinschaftsverhältnisses dient."

Mithin könnte ein einzelner Eigentümer im Wege der Wahrnehmung seines Einsichtsrechts, welches grundsätzlich in den Büroräumen des Verwalters auszuüben ist, (z. B. Kontakt-)Daten der anderen Eigentümer in rechtmäßiger Weise zur Kenntnis nehmen.

Dies bedeutet jedoch nicht, dass jegliche „proaktive" Weitergabe von Kontaktdaten einzelner WEG-Mitglieder, die sich bei den Verwaltungsunterlagen befinden, durch die Hausverwaltung an die anderen WEG-Mitglieder stets zulässig wäre. Vielmehr muss die Hausverwaltung im Einzelfall abwägen, ob einer Weitergabe schutzwürdige Interessen des Betroffenen entgegenstehen. Jedoch wird man aufgrund der o. g. Rechtsprechung nur in Ausnahmefällen zu dem Ergebnis kommen, dass die Weitergabe von Kontaktdaten der WEG-Mitglieder, die sich bei den Verwaltungsunterlagen befinden, an die anderen Mitglieder derselben WEG unzulässig ist. Denn das einzelne WEG-Mitglied könnte sich gemäß der o.g. Rechtsprechung im Wege der Einsichtnahme in die Verwaltungsunterlagen auf legalem Weg Kenntnis von diesen (bei den Verwaltungsunterlagen befindlichen) Daten verschaffen.

Eine zusätzliche Schwierigkeit bestand im Falle einer bei uns eingegangenen Eingabe jedoch darin, dass einer der Eigentümer dem Verwalter eine (nicht veröffentlichte) dienstliche Telefonnummer ausdrücklich nur zu dem Zweck zur Verfügung gestellt hatte, um für den Verwalter im Notfall unkompliziert erreichbar zu sein. Es ist bereits fraglich, ob solche Kontaktdaten – die allein für den Verwalter bestimmt waren – überhaupt zu den Unterlagen „der WEG" genommen werden müssen. Aber auch ohne eine solche ausdrückliche Bestimmung kann im Falle erkennbar dienstlicher E-Mail-Adressen oder Telefonnummern nicht ohne weiteres davon ausgegangen werden, dass der betroffene Eigentümer damit einverstanden wäre, von den anderen Eigentümern unter einer solchen dienstlichen Adresse bzw. Telefonnummer kontaktiert zu werden. Solche Daten sollte der Verwalter daher zumindest nicht aktiv an andere Eigentümer übermitteln und zudem – soweit nicht aus besonderen Gründen im Einzelfall erforderlich – auch kritisch prüfen, ob sie überhaupt zu den Unterlagen der WEG als solchen zu nehmen sind.

18.4 Einsicht in Unterlagen der Hausverwaltung durch die Revisionsabteilung der Muttergesellschaft des Hausverwaltungsunternehmens

Die Muttergesellschaft eines Hausverwaltungsunternehmens darf Verwaltungsunterlagen der Hausverwaltung grundsätzlich zu Revisionszwecken zur Kenntnis nehmen, ohne dass datenschutzrechtliche Interessen der Eigentümer der verwalteten WEG entgegenstünden.

Eine Wohnungseigentümerin innerhalb einer Wohnungseigentümergemeinschaft beschwerte sich über die Verwaltung der WEG. Als Verwalterin fungierte eine GmbH, die zu einem Konzern gehörte. Gegenstand der Beschwerde war, dass die Konzernrevisionsabteilung der Muttergesellschaft der Hausverwaltungs-GmbH im Rahmen ihrer Revisionstätigkeit Einsicht in die von der GmbH geführten Verwaltungsunterlagen der WEG genommen hatte.

Da die Muttergesellschaft ein von der Hausverwaltungs-GmbH verschiedenes Unternehmen (d. h. ein anderer Rechtsträger) war, stellt die Einsicht der Revisionsabteilung eine Bekanntgabe personenbezogener Daten der Wohnungseigentümer durch die Hausverwaltungs-GmbH an einen Dritten und somit gemäß § 3 Abs. 4 Satz 2 Nr. 3b BDSG eine Daten-

übermittlung dar. Die Übermittlung haben wir im vorliegenden Fall aufgrund berechtigter Interessen der Hausverwaltung und ihrer Muttergesellschaft gemäß § 28 Abs. 1 Satz 1 Nr. 2 und Abs. 2 Nr. 2a BDSG für zulässig erachtet.

Maßgeblich hierfür war, dass die Konzernmutter uns gegenüber plausibel erklärte, ein berechtigtes Interesse daran zu haben, Haftungsrisiken der mit ihr verbundenen Unternehmen, etwa der Hausverwaltungs-GmbH, zu überwachen und zu minimieren und zu diesem Zweck entsprechende Auskünfte einzuholen; dem habe die Einsicht durch die Revisionsabteilung gedient.

Die Konzern-Innenrevision hat dabei Vorgänge geprüft, die im Zusammenhang mit der Verwaltung der Wohnungseigentümergemeinschaft anfallen, z. B. Daten von Wohnungseigentümern, ggf. auch Handwerkern, Dienstleistern oder Lieferanten. Diese Arten von Daten unterliegen jedenfalls keinem in ganz besonderem Maße gesteigerten persönlichkeitsrechtlichen Schutz; sie gehören nicht zur Intimsphäre, sondern fallen in den Bereich der Privatsphäre und der Sozialsphäre. Gegenüber den anderen Eigentümern in einer WEG hat der einzelne Wohnungseigentümer im Hinblick auf die in den Verwaltungsunterlagen enthaltenen Daten des einzelnen Eigentümers nach der Rechtsprechung grundsätzlich ohnehin keine berechtigte Anonymitätserwartung (vgl. dazu den vorangegangenen Gliederungspunkt). Zudem war Gegenstand der Prüfung durch die Muttergesellschaft vorliegend die Tätigkeit der Hausverwaltungs-GmbH, nicht das Verhalten der einzelnen Wohnungseigentümer. Bei dieser Sachlage konnte die Übermittlung nach unserer Auffassung gemäß § 28 Abs. 2 Nr. 2a BDSG mit berechtigten Interessen der Muttergesellschaft als Dritter gerechtfertigt werden, da die Interessen der Eigentümer insoweit nicht entgegenstanden.

Ungeachtet dessen teilten wir der Hausverwaltung jedoch mit, dass die Eigentümer innerhalb der WEG gemäß § 4 Abs. 3 Nr. 3 BDSG über die in Rede stehende Übermittlung an die Revisionsabteilung der Muttergesellschaft zu informieren sind, da sie jedenfalls nicht ohne weiteres damit rechnen müssen.

18.5 Aushang eines Schreibens mit personenbezogenen Daten der Bewohner durch die Hausverwaltung im Treppenhaus eines Mehrfamilienhauses

Der Hausverwalter darf Schreiben mit personenbezogenen Daten einzelner Bewohner nicht in öffentlich zugänglichen Bereichen eines Mehrfamilienhauses aushängen.

Die Verwaltung einer WEG hängte ein von ihr verfasstes „Informationsschreiben" im Treppenhaus eines Mehrfamilienhauses aus. Darin informierte sie die Bewohner über die Ergebnisse einer in der Wohnanlage durchgeführten Legionellenuntersuchung. Bei dieser Untersuchung war das Warmwassernetz gemäß den Vorgaben der Trinkwasserverordnung auf etwaige Legionellenkontamination überprüft worden. Im Informationsschreiben führte die Verwaltung zwei Bewohner namentlich auf, in deren Wohnungen eine erhöhte Legionellenkonzentration festgestellt worden sei, und teilte mit, dass die Ursache vermutlich in einem fehlerhaften „Nutzerverhalten" liege. Das Schreiben enthielt ferner einige Verhaltensempfehlungen an die Betroffenen, etwa dahingehend, dass bestimmte Duschköpfe und Wasserhahnsiebe ausgetauscht werden sollten.

Wir haben den Aushang für datenschutzrechtlich unzulässig befunden, zum einen, weil sich auch Besucher im Treppenhaus aufhalten und so das Schreiben lesen können. Zum anderen war es aber auch nicht erforderlich und damit im Ergebnis unzulässig, die Namen der beiden Bewohner allen Hausbewohnern bekannt zu geben; vielmehr wäre es ausreichend und für die Hausverwaltung zumutbar gewesen, die Eigentümer der betroffenen Wohnungen persönlich zu informieren. Das von der Rechtsprechung anerkannte Recht des einzelnen Eigentümers auf Einsicht in die Verwaltungsunterlagen der WEG führt zu keiner anderen Bewertung, da in der „proaktiven" Mitteilung durch die Hausverwaltung schon deshalb ein eigenständiger Eingriff zu sehen ist, weil nicht fest-

steht, ob der einzelne Eigentümer tatsächlich Einsicht in die Verwaltungsunterlangen der WEG nehmen wird.

Die Hausverwaltung hat uns mitgeteilt, künftig auf vergleichbare personalisierte Aushänge zu verzichten.

Auch andere im Berichtszeitraum eingegangene Beschwerden betrafen das Aushängen von Schreiben durch Verwaltungen von Mehrfamilienhäusern im Treppenhaus. Allgemein gilt, dass WEG-Verwalter Schreiben mit personenbezogenen Daten z. B. zu einzelnen Eigentümern oder Mietern nicht in Gemeinschaftsbereichen – und erst recht nicht in öffentlich zugänglichen Bereichen wie z. B. Treppenhäusern oder Aufzügen – aushängen sollten. Soweit in einer Verwaltungsangelegenheit Bedarf an einer Information aller Wohnungseigentümer besteht und hierbei im Einzelfall eine namentliche Benennung einzelner Eigentümer oder Bewohner gerechtfertigt ist, sind solche Informationen z. B. in der Eigentümerversammlung oder mit Schreiben zu erteilen, die an die Eigentümer versandt werden.

19

Videoüberwachung

19 Videoüberwachung

19.1 Dashcam-Urteil VG Ansbach

Wenn ein Autofahrer mit einer in seinem Fahrzeug eingebauten on-board-Kamera (Dashcam) permanent Aufnahmen des von ihm befahrenen öffentlichen Bereichs in der Absicht macht, die Aufzeichnungen Dritten z. B. bei einem Unfall der Polizei, zur Verfügung zu stellen, ist dies datenschutzrechtlich unzulässig.

Ein Autofahrer hatte in seinem Fahrzeug eine on-board Kamera eingebaut und offensichtlich alle seine Fahrten aufgenommen. Er dokumentierte zahlreiche Fälle von ihm festgestellter Verstöße anderer Verkehrsteilnehmer, brachte diese bei der Polizei zur Anzeige und übergab teilweise zum Beleg dafür Videoaufnahmen. Dies ist datenschutzrechtlich unzulässig.

Wenn ein Kamerabetreiber die Absicht hat, die Aufnahmen gegebenenfalls Dritten zur Verfügung zu stellen, z. B. bei einem Unfall der Polizei oder einer Versicherung als Beweismittel oder durch Einstellen ins Internet, gilt das BDSG. Ein Fall persönlicher Tätigkeit, bei der das BDSG nicht anwendbar ist, liegt dann nicht vor, weil die Aufnahmen durch die Übergabe an Dritte den persönlichen Bereich verlassen. Da dabei auch die anderen Verkehrsteilnehmer erkennbar waren, war auch der notwendige Personenbezug vorhanden.

Eine Videoüberwachung von öffentlich zugänglichen Bereichen ist nach § 6b Abs. 1 Nr. 3 BDSG zulässig, wenn sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der Betroffenen überwiegen. Nach § 6b Abs. 2 BDSG sind der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen.

Diese Voraussetzungen sind beim Einsatz einer Dashcam nicht erfüllt, weil die schutzwürdigen Interessen der aufgenommenen Verkehrsteilnehmer überwiegen. Die Datenschutzaufsichtsbehörden haben dazu einen entsprechenden Beschluss gefasst.

> > >
http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/Beschluss_DK_26022014Unzulaessigkeit_von_Videoueberwachung_aus_Fahrzeugen.pdf

Aufgrund des informationellen Selbstbestimmungsrechts muss es jedem Einzelnen möglich sein, sich in der Öffentlichkeit frei zu bewegen, ohne befürchten zu müssen, ungewollt durch eine Videokamera überwacht zu werden. Ein permanentes Aufnehmen des vor dem Fahrzeug befindlichen Verkehrsraumes beeinträchtigt das informationelle Selbstbestimmungsrecht deshalb in unzulässiger Weise, zumal die allermeisten der betroffenen Verkehrsteilnehmer durch ihr Verhalten keinen Anlass dafür gegeben haben. Sie wissen auch nichts von den Kameraaufnahmen, da nicht darauf hingewiesen wird und haben keine Möglichkeit, den Aufnahmen auszuweichen. Das permanente Aufnehmen steht darüber hinaus in keinem angemessenen Verhältnis zu den sehr wenigen Anlässen, in denen die Aufzeichnungen einmal als Beweismittel benötigt werden könnten.

Unsere Behörde verbot deshalb dem betreffenden Autofahrer den Einsatz der Dashcam durch Bescheid, gegen den er Klage zum Verwaltungsgericht erhob. Das Verwaltungsgericht Ansbach hob zwar den Bescheid aus formalen Gründen auf, bestätigte aber inhaltlich unsere Auffassung (Urteil vom 13.08.2014, Az. AN 4 K 13.01634).

> > >
http://www.vgh.bayern.de/internet/media/vgansbach/presse/13a01634u_1.pdf

19.2 Videoüberwachung in Geschäften der Münchner Fußgängerzone

Wir haben die Zulässigkeit der Videoüberwachung in zahlreichen Geschäften

in der Münchner Fußgängerzone (Kaufingerstraße) überprüft und keine gravierenden Verstöße festgestellt.

Im April 2013 wurden von einer Münchner Tageszeitung unter der Überschrift „Die Fußgängerüberwachungszone" zahlreiche Videoüberwachungskameras in der Kaufinger- und Neuhauser Straße der Fußgängerzone Münchens unter die Lupe genommen und angegeben, dass mögliche Verstöße gegen das BDSG vorliegen würden (siehe Kapitel 3.4.10).

Aufgrund dieses Berichts haben wir bei 27 Unternehmen die eingesetzte Videoüberwachung dahingehend vor Ort überprüft, ob die Vorschriften zur Videoüberwachung von öffentlich zugänglichen Räumen nach § 6b BDSG eingehalten werden. Folgende Fragestellungen haben wir dabei besonders hervorgehoben:

- Findet tatsächlich eine Videoüberwachung statt, wenn ja, in welchen Bereichen?
- Welchem Zweck dient die Videoüberwachung?
- Wie werden bei der Videoüberwachung die Interessen der Betroffenen berücksichtigt?
- Weshalb sind keine anderen, milderen Mittel zum Erreichen des Zwecks möglich?
- Werden die Videoaufnahmen aufgezeichnet?
- Wer hat unter welchen Bedingungen Zugriff auf die Aufzeichnungen?
- Wann und wie erfolgt die Löschung der Aufzeichnungen?
- Werden auch Tonaufzeichnungen, die nach § 201 Strafgesetzbuch strafbar wären, angefertigt?
- Wurde gem. § 6b Abs. 2 BDSG auf die Videoüberwachung hingewiesen?

Insgesamt wurde dabei festgestellt, dass es zwar einige Unzulänglichkeiten bei der Videoüberwachung gegeben hat, gravierende Verstöße oder nachhaltiges Verweigern, den Anforderungen der Datenschutzaufsicht Rechnung zu tragen, mussten jedoch nicht festgestellt werden. In den Geschäften wurden sowohl funktionslose Kameraattrappen, Kundenzähler, die keine personenbezogenen Daten i. S. d. BDSG erfassen und optisch einer Videokamera ähneln können, als auch Videokameras (mit und ohne Aufzeichnung) eingesetzt. Die Anzahl der eingesetzten Videoüberwachungskameras bewegt sich dabei zwischen vier bis 70 Videokameras je verantwortliche Stelle. Die Geschäftsinhaber gaben bei der Prüfung meist an, dass damit hauptsächlich die Verkaufsflächen zum Schutz des Eigentums überwacht werden sollen.

Bereiche, die nicht videoüberwacht werden dürfen (wie z. B. Kundenumkleiden oder Aufenthaltsräume für Mitarbeiter), wurden nach Überprüfung des uns vorgelegten Bildmaterials – und auch nach dem Ergebnis der Vor-Ort-Prüfung – nicht erfasst. Ebenso haben sich Befürchtungen, dass weite Flächen der Fußgängerzone von den Geschäften aus videoüberwacht würden, in den allermeisten Fällen nicht bestätigt. Lediglich einzelne Unternehmen wurden aufgefordert, die Einstellungen der Kameras entsprechend abzuändern. Interessanter Weise werden die Daten nur bei gut der Hälfte der überprüften Unternehmen gespeichert, die anderen verzichteten auf diese Art der Datenverarbeitung. Zudem setzt erfreulicherweise keines der überprüften Unternehmen eine Tonaufzeichnung ein.

Alle Unternehmen kamen insgesamt der Kennzeichnungspflicht nach § 6b Abs. 2 BDSG nach. Teilweise wurde sogar darauf hingewiesen, obwohl keinerlei Überwachungsgeräte installiert waren. Die Vor-Ort-Überprüfung ergab jedoch bei manchen Händlern, dass die Hinweisschilder zu klein, an zweifelhaften Stellen oder durch Werbetafeln verdeckt waren. Hier haben wir zur Nachbesserung aufgefordert.

Im Ergebnis haben wir erkannt, dass es zwar einige Unzulänglichkeiten bei der Videoüberwachung gegeben hat, gravierende Verstöße oder nachhaltiges Verweigern, den Anforderungen der Datenschutzaufsicht Rechnung zu tragen, mussten jedoch nicht festgestellt werden. Die Prüfung hatte deshalb weder den

Erlass von Anordnungen zur datenschutzkonformen Nutzung von Videoüberwachungsanlagen noch den Erlass von Bußgeldbescheiden zur Folge.

19.3 Einsatz von Gesichtserkennungskameras für Marketingzwecke

Eine rein für statistische Zwecke vorgenommene Auswertung von Gesichtsdaten unterliegt nicht dem BDSG, wenn die personenbezogenen Daten nur für die technisch notwendige Zeitspanne der Auswertung verarbeitet werden und ein Zugriff auf die Klardaten oder eine Wiederherstellung dieser nicht möglich ist.

Im vergangenen Berichtszeitraum erhielten wir Anfragen zum Einsatz von Produkten zur statistischen Analyse von Kundenbewegungen in Ladengeschäften oder Einkaufszentren, bzw. zur Auswertung des Interesses einzelner Kunden an einer Werbung. Den vorgestellten Systemen war gemeinsam, dass eine Kamera bzw. ein Scanner die Gesichter von Kunden in einem Ladengeschäft oder von Personen, die eine auf einem Monitor gezeigte Werbung ansehen, erfasst und von einem direkt angeschlossenen Computer ausgewertet werden.

Die Bilddaten werden dabei nicht dauerhaft gespeichert, sondern einzig im Arbeitsspeicher RAM und nur für die Dauer der eigentlichen Datenbearbeitung für Sekundenbruchteile zwischengespeichert und danach umgehend irreversibel gelöscht. Aufgrund der Hardwarekonfiguration und -absicherung ist ein Zugriff auf die Klardaten nicht möglich. Als Ergebnisdaten werden an den Händler nur statistische Werte wie Geschlecht, Altersgruppe, ethnische Zuordnung, Verweildauer und Interesse ausgegeben.

Für die verarbeitende Stelle ist dabei die Identität der betroffenen Personen weder von Interesse noch hat sie zu irgendeinem Zeitpunkt Zugang zu identifizierenden Merkmalen. Die ihr zugänglich gemachten statistischen Auswertungen lassen keinen Bezug zu einer bestimmten oder bestimmbaren Person zu.

Fraglich ist, ob das BDSG bei diesem Sachverhalt anwendbar ist. Voraussetzung dafür wäre, dass mittels der Kamera personenbezogene Daten erhoben werden. Nach § 3 Abs. 1 BDSG sind personenbezogene Daten Einzelangaben einer bestimmten oder bestimmbaren natürlichen Person.

Nachdem biometrische Daten des Gesichts erhoben werden, sind wir zunächst unabhängig davon, was mit diesen Aufnahmen geschieht, davon ausgegangen, dass das BDSG anwendbar ist. Die Auswertung der Bilder beinhaltet lediglich statistisch weiter verarbeitbare, rein quantitative und anonymisierte Daten. Im Ergebnis fehlt damit jeglicher Personenbezug, so dass die entsprechende Nutzung aus datenschutzrechtlicher Sicht nicht beschränkt ist.

Selbst wenn der Zweck der Systeme der ist, den Nutzern Daten ohne Personenbezug anzubieten, darf nicht außer Acht gelassen werden, dass im Bearbeitungsvorgang mit personenbezogenen Daten umgegangen wird. Die Bildaufnahme ist insoweit als personenbezogenes Datum zu sehen. Das Bild soll allerdings nur für eine „technische Sekunde“ bis zum Abgleich mit dem vorhandenen Muster im Arbeitsspeicher gespeichert und für niemanden sichtbar sein. Da sichergestellt wird, dass es sich insoweit um einen geschlossenes System handelt, auf das mit an Sicherheit grenzender Wahrscheinlichkeit niemand Zugriff haben kann bzw. aus dem keine personenbezogenen Daten erhoben werden können, ist kein Personenbezug mehr vorhanden und eine datenschutzrechtliche Relevanz nach unserer Auffassung derzeit nicht gegeben.

19.4 Digitaler Türspion

Eine permanente Bildspeicherung eines digitalen Türspions scheitert an der Erforderlichkeit der verantwortlichen Stelle nach § 28 Abs. 1 BDSG und ist daher unzulässig.

Wir erhielten eine Anfrage zur datenschutzrechtlichen Bewertung eines „Digitalen Türspions". Dieses Gerät, das auf einen vorhandenen optischen Türspion aufgesteckt wird, besteht aus einer Digitalkamera und einem kleinen Monitor in einem Gehäuse. Wenn die Kamera auf Knopfdruck aktiviert wird, überträgt diese für 20 Sekunden das Geschehen vor der Tür auf den Monitor. Wird sie nicht aktiviert, bleibt dieser dunkel und befindet sich im Stromsparmodus. Dies ist zunächst aus datenschutzrechtlicher Sicht nicht zu beanstanden.

Allerdings bietet das Gerät die Möglichkeit, Bildaufnahmen anzufertigen: Sobald eine MicroSD-Speicherkarte eingesteckt wird, ist diese Funktion aktiviert. Automatisch werden bei Betätigen des o. g. Schalters drei Bilder der Ansicht aufgenommen. Diese Bilder werden auf der SD-Karte gespeichert bis sie über PC wieder gelöscht werden (das Gerät selbst bietet keine Löschfunktion).

Problematisch ist hierbei, dass jede Betätigung der Power-Taste (also auch, wenn ein bloßes Durchsehen beabsichtigt ist) sofort drei Aufnahmen anfertigt. In der Regel dürften Türspione in Mehrfamilienhäusern mit angeschlossenen Treppenhäusern, bzw. weiten Hausfluren eingesetzt werden. Diese Hausflure stellen keine öffentlich zugänglichen Räume dar, so dass die Speicherung der Aufnahmen mit einer optisch-elektronischen Einrichtung wie dem digitalen Türspion nicht nach § 6b BDSG, sondern nach den allgemeinen Vorschriften des § 28 Abs. 1 Nr. 2 BDSG zu bewerten ist.

Der Nutzer muss deshalb seine berechtigten Interessen mit den schutzwürdigen Interessen der Betroffenen abwägen. Als Datenschutzaufsichtsbehörde stehen wir dieser ständigen Aufnahmefunktion kritisch gegenüber, weil ein ständiger Einsatz der Aufnahmefunktion schon an der Erforderlichkeit scheitern dürfte.

19.5 Attrappen von Videokameras sind keine optisch-elektronischen Einrichtungen

Der Einsatz von Kameraattrappen fällt nicht unter das Bundesdatenschutzgesetz. Sofern diese wie echte Kameras im datenschutzrechtlich zulässigen Rahmen eingesetzt werden, sehen wir keine Veranlassung, diesen Umstand den Betroffenen mitzuteilen.

In einem Ladengeschäft wurden aufgrund vorangegangener erheblicher Sachbeschädigungen im Schaufensterbereich Kameraattrappen installiert. Ziel des Einsatzes der funktionslosen Geräte war es, Jugendliche davor abzuschrecken, das Schaufenster und die Fassade zu beschädigen bzw. zu verunreinigen. Die Attrappen waren von echten Videokameras kaum zu unterscheiden und vermittelten den Eindruck als würde der gesamte Gehweg vor dem Laden gefilmt. Ein Anwohner bat uns darum, die datenschutzrechtliche Zulässigkeit dieser Kameras zu prüfen.

Die Kameraattrappen, die tatsächlich funktionslos und nicht nur ausgeschaltete funktionsfähige Kameras sind, haben wir folgendermaßen beurteilt:

Das BDSG regelt in § 6b, unter welchen Voraussetzungen die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen und damit eine Videoüberwachung zulässig ist. Attrappen sind keine optisch-elektronischen Einrichtungen. Es werden damit keine personenbezogenen Daten erhoben oder verarbeitet, so dass das BDSG nicht anwendbar ist und wir als Datenschutzaufsichtsbehörde nicht zuständig sind (§ 1 Abs. 2 Nr. 3 BDSG).

Unbestritten können aber Kameraattrappen das Persönlichkeitsrecht von Menschen tangieren, die in den vermeintlichen Fokus einer derartigen Attrappe gelangen und unter diesem Eindruck zu einer Verhaltensänderung veranlasst werden. Ob und inwieweit der Einsatz derartiger Kameraattrappen rechtmäßig ist, ist von den Zivilgerichten zu entscheiden, wenn

ein Betroffener sich gegen den Einsatz einer derartigen Attrappe wendet. Nach unseren Erfahrungen gehen die Zivilgerichte davon aus, dass jedenfalls in den Fällen, in denen eine Videobeobachtung mit einer funktionsfähigen Kamera datenschutzrechtlich zulässig wäre, auch der Einsatz einer Attrappe nicht als rechtswidrig festgestellt wird.

Nach § 6b BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) für private Stellen insbesondere nur dann zulässig, soweit sie zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Im vorliegenden Fall hätten wir aufgrund der geschilderten Vorfälle ein berechtigtes Interesse an einer (tatsächlichen) Überwachung des Außenbereiches um den Laden als gegeben angesehen. In ähnlichen Fällen wurde ein Toleranzbereich von höchstens bis zu einem Meter, gemessen ab der Außenwand, für vertretbar angesehen. Wir haben den Betreiber daher gebeten, die Attrappen so auszurichten, dass sie nicht mehr den Eindruck erwecken, als würden sie den gesamten Gehweg vor dem Laden erfassen. Eine derartige echte Videoüberwachung hätten wir dann für diesen Fall für zulässig erachtet, so dass wir den datenschutzrechtlich geringeren Eingriff mit funktionslosen Dummies erst recht „billigten".

Soweit vertretbar, informieren wir die Betroffenen nicht über die Tatsache des Einsatzes einer Attrappe, sondern äußern uns in der Regel dahingehend, dass wir keine Veranlassung zu einem aufsichtlichen Einschreiten sehen.

Dem Betroffenen bleibt es selbstverständlich freigestellt, dagegen zivilrechtlich vorzugehen, wenn er sich in seinem Persönlichkeitsrecht verletzt fühlt.

19.6 Fotoabgleich bei Liftkartenbenutzern

Ein Abgleichen eines gespeicherten Fotos vom Nutzer eines Mehrtagestickets zur Unterbindung von unzulässiger Überlassung der Liftkarte an Dritte ist zulässig, wenn die Käufer auf die Bildspeicherung hingewiesen werden.

Mehrere Anfragen erhielten wir zu der zunehmenden Praxis von Skiliftanlagenbetreiber, Lichtbilder von Tageskartennutzern anzufertigen und diese bei jedem Einsatz der Karte abzugleichen.

Immer mehr Skiliftbetreiber gehen dazu über, eine entsprechend deren AGBs unzulässige Übertragung von Halbtages-, Tages- und Mehrtages-Skipässen auf andere Personen stärker zu kontrollieren. Um eine Weitergabe nicht übertragbarer Tickets ausschließen zu können, wird bei erstmaliger Nutzung der Karte an einem Liftzustieg ein Foto des Nutzers angefertigt und im System gespeichert. Dieses Foto wird dann bei jedem Einsatz der Karte dem Mitarbeiter auf einem Monitor angezeigt, damit dieser einen Abgleich mit dem momentanen Inhaber vornehmen kann. Ergeben sich hier Unstimmigkeiten, wird dem Karteninhaber der Zustieg zum Lift verweigert und die Liftkarte eingezogen. Auf die Unzulässigkeit der Übertragbarkeit von Tickets wird in den AGBs hingewiesen.

Der Liftbetreiber gab uns gegenüber an, dass zur Gewährleistung der Sicherheit der Fahrgäste und des Seilbahnbetriebes, sowie zur Vermeidung missbräuchlicher Nutzung von Fahrausweisen die Zugangsbereiche auch zeitweise mit einer Videoanlage überwacht würden. Die Aufzeichnung erfolge ausschließlich zur Wahrung des Hausrechts und der betrieblichen Sicherheitsinteressen, ein Hinweisschild mache darauf aufmerksam.

Den Sachverhalt haben wir wie folgt beurteilt:
Eine Überwachung der Zustiegstellen der Bahnen mittels einer Videoanlage halten wir entsprechend den Vorschriften nach § 6b BDSG für zulässig. Nach dieser Bestimmung ist die

Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) für private Stellen nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Als berechtigtes Interesse kann hier sowohl die vom Betreiber angeführte Wahrung des Hausrechts als auch die Überwachung der betrieblichen Sicherheit gewertet werden. Allerdings sehen wir die Speicherung und permanente, zumindest für die Dauer des Einsatzes der jeweiligen Karte, Nutzung eines Fotos nicht durch diese Vorschrift und auch nicht durch die Hinweise zur Videoüberwachung gedeckt.

Wir halten jedoch die Speicherung und Nutzung der Fotodaten zur Verhinderung von Missbrauch auf Grundlage des § 28 Abs. 1 Nr. 2 BDSG unter bestimmten Voraussetzungen für zulässig. Nach § 28 Abs. 1 Nr. 2 BDSG ist eine Speicherung und Nutzung für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

In der Bekämpfung von Missbrauch der Karten kann ein berechtigtes Interesse gesehen werden. Der Bildabgleich stellt ein praktikables Mittel dazu dar, da eine weitere, umfassendere Datenspeicherung damit vermieden werden kann. Zu beachten ist dabei jedoch, dass nur die zuständigen Kontrolleure diese Bilddaten einsehen können und ein Abrufen dieser Daten zu anderen Zwecken nicht zulässig ist, ferner eine Datenlöschung umgehend erfolgt, wenn ein Abgleich nicht mehr notwendig ist.

Allerdings ist auf die Datenerhebung, -verarbeitung und -nutzung mittels Fotoaufnahme explizit hinzuweisen (§ 4 Abs. 3 BDSG). Ein Hinweis auf die Erhebung von Fotodaten sollte in die Verkaufsbedingungen für die betroffenen Karten, sowohl an der Kasse vor Ort als auch im Internet, aufgenommen werden.

19.7 Anwendbarkeit des BDSG bei Botschaften und Konsulaten

Wiederholt haben uns Eingaben zur Videoüberwachung von in Bayern ansässigen Auslandsvertretungen erreicht. Teilweise wird dort mit einer großen Anzahl an Videokameras das umgebende Gelände überwacht.

Botschaften und Konsulate haben einen exterritorialen Status. Sofern sie eine Videoüberwachung auf ihrem Grundstück oder von ihrem Grundstück aus auch in den öffentlich zugänglichen Bereich hinaus betreiben, gehen wir nicht von der Anwendbarkeit des BDSG aus.

19.8 Orientierungshilfe zur Videoüberwachung

Aufgrund vielfacher Anfragen zum Thema Videoüberwachung durch nichtöffentliche Stellen haben sich die Datenschutzaufsichtsbehörden entschlossen, das Thema in einer Orientierungshilfe aufzugreifen, und die Chancen, Risiken und rechtlichen Voraussetzungen für die datenschutzgerechte Videoüberwachung zu veranschaulichen.

Die Datenschutzaufsichtsbehörden haben an Hand von Beispielen für öffentlich zugänglichen Räume (öffentliche Verkehrsflächen, Verkaufsräume, Gaststätten, etc.), für Situationen im Beschäftigtenverhältnis und zur Videoüberwachung in nicht öffentlich zugänglichen Räumen ihre datenschutzrechtlichen Anforderungen dargestellt. Allgemeine Ausführungen und ein Fragenkatalog, der Verantwortlichen und Datenschutzbeauftragten als Checkliste dienen kann, runden das Dokument ab.

Die Orientierungshilfe kann im Internet auf unserer Webseite abgerufen werden.

>>> *http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/Orientierungshilfe_Videoueberwachung_durch_nicht_oeffentliche_Stellen.pdf*

20

Fahrzeugdaten

20 Fahrzeugdaten

20.1 Verkehrsgerichtstag 2014

Ein Thema des Verkehrsgerichtstags vom Januar 2014 war: Wem gehören die Fahrzeugdaten?

Der Deutsche Verkehrsgerichtstag, eine alle Themen des Straßenverkehrsrechts behandelnde jährliche Expertenkonferenz, hatte sich in der Tagung vom 29. bis 31. Januar 2014 wieder einmal in einem eigenen Arbeitskreis mit den Daten in und aus Kraftfahrzeugen befasst, die infolge zunehmender IT-Komponenten in den Kraftfahrzeugen immer mehr werden.

Damit Innovationen für die Automobilität in Europa auch zukünftig gesellschaftlich akzeptiert werden, muss nach Ansicht des Verkehrsgerichtstags der Austausch von Daten und Informationen aus dem Fahrzeug Regeln unterworfen werden, die das informationelle Selbstbestimmungsrecht durch Transparenz und Wahlfreiheit der Betroffenen (z. B. Fahrzeughalter und Fahrer) sichern.

Für den Umgang mit Fahrzeugdaten hat der Verkehrsgerichtstag Empfehlungen verabschiedet, denen wir – worauf wir bei verschiedenen Beratungen hingewiesen haben – durchaus zustimmen (im Dokument: Empfehlungen Arbeitskreis VII).

>>>
http://www.mobilundsicher.de/media/empfehlungen_52_vgt.pdf

20.2 Arbeitskreis Verkehr der Datenschutzaufsichtsbehörden

Die neuen bzw. erweiterten IT-Systeme in Kraftfahrzeugen führen zu neuen datenschutzrechtlichen Risiken. Über den notwendigen datenschutzrechtlichen Rahmen muss deshalb mit der Automobilindustrie gesprochen werden, um auch für Fahrzeughalter und Fahrer interessengerechte Lösungen zu erreichen.

In einer früheren Runde von Gesprächen der Aufsichtsbehörden mit dem Verband der Automobilindustrie von 2009 bis 2011 waren vor allem die im Fahrzeug betriebsnotwendigen Datenspeicher auf der Tagesordnung. Als Ergebnis dieser Gespräche wurde eine Datenschutz-Information für die Betriebsanleitungen zu Fahrzeugen erarbeitet (siehe dazu auch die Pressemitteilung vom 6. Februar 2012 auf unserer Webseite).

>>>
http://www.lda.bayern.de/lda/datenschutzaufsicht/p_archiv/2012/pm002.html

Inzwischen haben viele neue Fahrzeuge Zusatz-IT-Systeme wie Mobilitäts-, Notruf- und Ortungssysteme sowie umfangreiche und vernetzte Infotainment-Komponenten (Telefon /Navigation/Radio/Internet, usw.), wodurch sich eine Reihe von neuen Fragestellungen zu Datenschutz und Datensicherheit ergeben.

In mehreren Sitzungen haben sich die Aufsichtsbehörden im Arbeitskreis Verkehr mit den Grundlagen der IT-Systeme moderner Kraftfahrzeuge befasst und deren datenschutzrechtliche Bewertung vorgenommen, was dann in eine Entschließung der Datenschutzkonferenz mündete.

>>>
http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/88DSK_DatenschutzImKfz.html?nn=5217228).

Einige Kernforderungen der Aufsichtsbehörden dabei sind:

Datenverarbeitungsvorgängen im und um das Fahrzeug muss das Prinzip der Datenvermeidung und Datensparsamkeit zu Grunde liegen. Daten sind in möglichst geringem Umfang zu erheben und umgehend zu löschen, nachdem sie nicht mehr benötigt werden.

Für Fahrer, Halter und Nutzer von Fahrzeugen muss vollständige Transparenz gewährleistet sein. Dazu gehört, dass sie umfassend und verständlich darüber zu informieren sind, welche Daten beim Betrieb des Fahrzeugs erfasst und verarbeitet sowie welche Daten über welche Schnittstellen an wen und zu welchen Zwecken übermittelt werden.

Schließlich muss durch geeignete technische und organisatorische Maßnahmen Datensicherheit und -integrität gewährleistet sein. Dies gilt insbesondere für die Datenkommunikation aus Fahrzeugen heraus.

Mit dem Verband der Automobilindustrie wird nun über die Umsetzung der aufsichtsbehördlichen Anforderungen für Datenschutz und Datensicherheit bei der Kraftfahrzeug-IT gesprochen.

20.3 Was „weiß" ein Kraftfahrzeug und wer erfährt davon? Fälle aus der Praxis

In einigen Fällen wandten sich Bürger an uns, weil sie aus ihrer Sicht überraschende Mitteilungen ihrer Fahrzeug-IT zur Kenntnis genommen haben.

20.3.1 Hinweis im Display: „Kupplung kühlen"

Ein betroffener Kfz-Halter teilte uns mit, dass im Display seines neuen Autos nach einer Fahrleistung von rund 1.000 km der Hinweis „Kupplung kühlen" erschienen sei. Daraus ergebe sich, dass in seinem Wagen ohne seine Kenntnis ein Gerät eingebaut sei, das die Auswirkung seines Fahrverhaltens auf die Kupplung registriere. Nach Auskunft seines Händlers könne eine einmal erfolgte Registrierung nicht gelöscht werden. Das bedeutet u. a., dass sie auch beim Verkauf des Wagens erhalten bleibe.

Wir haben den Kfz-Halter auf die allgemeinen Informationen über Fahrzeugdatenspeicher in der Betriebsanleitung seines Fahrzeugs aufmerksam gemacht, wo für konkrete Detailfragen auf die Mitarbeiter des Servicenetzes (einschließlich Hersteller) verwiesen wird. Hierzu haben wir den Kfz-Halter an den Datenschutzbeauftragten des Herstellers verwiesen, der das Anliegen des Kunden offensichtlich zufriedenstellend behandeln konnte. Jedenfalls hat der Kfz-Halter eine von uns angebotene weitere Unterstützung bei fortbestehenden Unklarheiten nicht mehr in Anspruch genommen. Uns hat der Datenschutzbeauftragte des Herstellers noch mitgeteilt, dass der betreffende Händler in diesem Fall eine falsche Auskunft an den Kfz-Halter erteilt habe, dass eine Löschung des Eintrags „Kupplung kühlen" durch den Händler in der Werkstatt möglich sei und nun im Nachhinein noch durchgeführt worden sei.

20.3.2 Batteriekontrollleuchte

Ein Fahrzeughalter sagte uns, dass er sein Auto zum Kundendienst gebracht habe, weil die Batteriekontrolllampe aufgeleuchtet habe. Der Monteur in der Werkstatt habe ihm erklärt, dass die Autobatterie wegen der vielen Kurzstreckenfahrten erschöpft sei. Der Kunde sei in den letzten Monaten laut Fahrzeugdatenspeicher 107 Mal nur jeweils vier Kilometer gefahren.

Wir haben auch hier den Kfz-Halter auf die allgemeinen Informationen über Fahrzeugdatenspeicher in der Betriebsanleitung seines Fahrzeugs aufmerksam gemacht, wo für konkrete Detailfragen auf die Mitarbeiter des Servicenetzes (einschließlich Hersteller) verwiesen wird. Dort konnte dem betroffenen Kfz-Halter offensichtlich in seinem Sinne geholfen werden, weil er die im Bedarfsfalle angebotene weitere Unterstützungsmöglichkeit durch uns nicht mehr in Anspruch nahm.

20.3.3 Onlinemeldung Bremsbeläge

Ein Fahrzeughalter wandte sich an uns, weil seine Vertragswerkstatt ihn angerufen und ihm mitgeteilt habe, dass bei seinem Fahrzeug laut Online-Meldung die Bremsbeläge ziemlich abgefahren seien und er deshalb mit seinem Fahrzeug die Werkstatt aufsuchen solle.

Wir haben nach Rücksprache mit dem betreffenden Kfz-Hersteller den Fahrzeughalter darauf hingewiesen, dass er beim Fahrzeugkauf vertraglich eine Online-Servicefunktion vereinbart habe, die auch diesen Hinweisdienst umfasse. Wenn er künftig diesen Online-Service nicht mehr haben möchte, könne er den Servicevertrag kündigen.

20.3.4 Ausdruck der Fahrzeugdaten für Arbeitgeber

Der Besitzer einer Fahrzeugflotte möchte von der Werkstatt für jedes seiner Fahrzeuge Ausdrucke bestimmter protokollierter Informationen aus den Fahrzeugdatenspeichern, wie beanspruchte Drehmomente und Drehzahlbereiche, Bremsbetätigung und Bremseinsatz, Kupplungsbetätigung und -verschleiß, Kraftstoffverbrauchswerte und Geschwindigkeitsklassen usw., um das Fahrverhalten seiner Beschäftigten anhand der für ihn personenbeziehbaren Fahrzeugdaten detailliert zu kontrollieren.

Wir haben die Auffassung vertreten, dass die Regelungen zum Beschäftigtendatenschutz (§ 32 BDSG) einer so weit gehenden Mitarbeiterkontrolle entgegen stehen und die Werkstatt in diesem Sinne für ihr weiteres Vorgehen beraten.

20.3.5 Auslesen von Fahrzeugdaten zu einem Dienstwagen

Um einen umfassenden Eindruck von den insgesamt in einem Kraftfahrzeug abgespeicherten Daten und deren Personenbeziehbarkeit zu gewinnen, haben wir die Rückgabe eines behördlichen Dienstwagens an den Hersteller nach Ablauf des Leasingvertrags dazu genutzt, um uns vom Hersteller alle Daten in den verschiedenen Steuergerätespeichern zu zeigen, zu erläutern und ausdrucken zu lassen.

Der Hersteller ist unserer Bitte gerne gefolgt, hat zu der Prüfaktion ca. 20 Mitarbeiterinnen und Mitarbeiter abgestellt, um uns das Auslesen der Daten aus den verschiedenen Komponenten zu zeigen, transparent zu machen, welche Daten nur der Hersteller und welche eine Werkstatt auslesen kann, und die Ergebnisse zu erläutern.

Einschließlich einer Reihe von rein oder eher technischen Daten, wie korrekte elektrische Spannungswerte für verschiedene Funktionen, den korrekten Kältemitteldruck oder die Endwerte bestimmter Hebelfunktionen usw., ergaben sich dabei auch viele Daten, die bei Kenntnis des Halters, Fahrers oder Mitfahrers personenbeziehbare Aussagen erlauben. Zeit und gefahrene Wegstrecke seit der letzten Inspektion lassen z. B. erkennen, wie sorgfältig ein Halter sein Fahrzeug pflegt. Das Beispiel des Prozentwertes „Fahrzeitanteil sportlich" lässt Rückschlüsse auf die Fahrweise des Fahrers zu. Und Sitzbelegungswerte können im Zusammenwirken mit Daten über nicht geschlossene Sicherheitsgurte in einer Unfallsituation gegebenenfalls Aussagen über das Verhalten von Mitfahrern erlauben.

Selbstverständlich haben wir vorher die Einwilligung des Fahrers und seines Hauptfahrgastes, die diesen Wagen in den letzten Jahren fast ausschließlich genutzt haben, eingeholt. Der Fahrer hat an der Prüfung teilgenommen und war, wie wir auch, durchaus überrascht, welche Erkenntnisse über das Fahrverhalten auslesbar waren. Anhaltspunkte dafür, dass mit diesen Daten durch Hersteller oder Werkstatt datenschutzrechtlich unzulässig umgegangen worden wäre, haben sich nicht ergeben.

Unsere dabei gewonnenen Erkenntnisse fließen in die unter Kapitel 20.2 erwähnten Gespräche mit dem Verband der Automobilindustrie zur Umsetzung der Entschließung der Datenschutzkonferenz mit ein.

20.4 GPS-Ortung von Mietwagen

Die GPS-Ortung von Mietwagen ohne Information des Mieters ist auch dann unzulässig, wenn es sich um hochpreisige Kraftfahrzeuge handelt und ein Dienstleister die Ortung im Rahmen eines Geofencing übernimmt.

Von der Staatsanwaltschaft haben wir ein Schreiben mit der Information erhalten, dass sich in einem Verfahren wegen Unterschlagung bzw. versuchter Unterschlagung eines gemieteten Kraftfahrzeuges herausgestellt habe, dass dieses Kfz mit einem GPS-Sender versehen war und die Mieter dahingehend überwacht wurden, ob sie sich den Landesgrenzen näherten. Dabei seien die Mieter bei Abschluss des Mietvertrages nicht über den Einsatz des GPS-Gerätes informiert worden. Dem uns von der Staatsanwaltschaft zugesandtem Mietvertrag konnten wir unter der Überschrift „Vertragsstrafe" lediglich die Information entnehmen, dass eine Vertragsstrafe fällig werde, wenn das Bundesgebiet verlassen würde oder Rennstrecken o. ä. befahren würden. Zugleich wird in den AGB geregelt, dass der Vermieter ausdrücklich berechtigt sei, die Fahrzeuge diesbezüglich zu überwachen.

Auf Nachfrage wurde uns dargestellt, dass derzeit kein GPS-Sender mehr in Mietfahrzeugen eingesetzt werde, dies aber bei besonderen Gefährdungslagen geplant sei. Die GPS-Sender und das Geofencing, d. h. die Technik zur Feststellung, wenn ein bestimmtes Objekt ein vordefiniertes Gebiet verlässt, würden durch einen Schweizer Dienstleister zur Verfügung gestellt. Lediglich wenn eines der Mietfahrzeuge den zuvor bestimmten Bereich verlasse, würde die Autovermietungsgesellschaft eine Kurznachricht erhalten, die einen Hinweis auf das Fahrzeug und den Standort enthalte und darüber informiere, dass ein bestimmter Bereich verlassen wurde.

Nachdem das Mietwagenunternehmen zunächst eine Einwilligung der Nutzer in die GPS-Ortung einholen wollte, schwenkte es später um und wollte von uns wissen, unter welchen Umständen eine Information des Mieters gegebenenfalls nicht notwendig sei. Hierzu wurde argumentiert, dass es sich bei den Mietfahrzeugen ausschließlich um hochpreisige Kfz (Wert bis zu 500.000 Euro) handle und nur ohne eine Information Straftaten verhindert werden könnten. Wenn nämlich die GPS-Ortung bekannt sei, würde der Sender ausgebaut oder durch Störsender so irritiert, dass eine Ortung nicht mehr möglich sei. Wäre also eine Information erforderlich, würden die Geschäftszwecke des Unternehmens erheblich gefährdet. Konkrete Informationen dazu, welche Anhaltspunkte vorliegen müssten, dass ein GPS-Sender eingebaut bzw. aktiviert würde, wurden uns hingegen nicht genannt.

Wir haben anhand dieser Argumentation nicht die Zulässigkeit einer verdeckten GPS-Ortung erkennen können. Insbesondere sahen wir kein derart pauschales gewichtiges Interesse des Mietwagenunternehmens an der verdeckten Ortung und die Ausnahme des § 33 Abs. 2 Nr. 7b BDSG nicht als einschlägig an, wonach eine Pflicht zur Benachrichtigung des Betroffenen nicht besteht, wenn die Geschäftszwecke aufgrund der Benachrichtigung erheblich gefährdet sein müssen und das Interesse an der Benachrichtigung die Gefährdung nicht überwiegt.

Diese Einschätzung nahm das Mietwagenunternehmen zur Kenntnis und teilte uns mit, dass „bis auf weiteres" keine GPS-Geräte mehr in den Mietfahrzeugen eingesetzt würden.

21

Informationspflichten bei Datenpannen (§ 42a BDSG, § 15a TMG)

21 Informationspflichten bei Datenpannen (§ 42a BDSG, § 15a TMG)

Bei bestimmten Datenschutzverstößen und Datenschutzpannen müssen die verantwortlichen Stellen die Datenschutzaufsichtsbehörden und die betroffenen Personen informieren, wenn schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Personen drohen (siehe dazu unseren Tätigkeitsbericht 2009/2010, Kapitel 17.1)

Deutlich zurückgegangen ist die Anzahl der gemeldeten Fälle des heimlichen Erfassens von EC-Kartendaten an Geldautomaten (das sog. Skimming), was zum einen mit der strittigen Rechtslage der Meldepflicht für solche Sachverhalte, aber auch mit verbesserten Sicherheitsmaßnahmen der Banken wie z. B. Chip-Technologie auf den EC-Karten statt Datenspeicherung auf dem Magnetstreifen zu tun haben kann.

Im Folgenden stellen wir auffällige Häufungen von Sachverhalten und einige besondere Datenpannen vor.

21.1 Diebstahl bzw. Einbruchdiebstahl von Datenträgern und IT-Geräten

Sowohl 2013 wie auch 2014 betraf die größte Gruppe von gemeldeten Datenpannen kriminelle Handlungen des Diebstahls oder Einbruchdiebstahls verschiedenster Arten von Datenträgern und IT-Geräten. Dem hätte häufig durch Datensicherheitsmaßnahmen wirksam abgeholfen werden können.

Zum Beispiel werden teilweise auf ganz banale Art aus Bankbriefkästen Überweisungs- oder Scheckformulare entwendet, zu den eigenen Gunsten der Täter verfälscht und dann wieder in den Verkehr gebracht. Besondere Sicherheitsbriefkästen können dem vorbeugen.

Eine sichere Geräteverschlüsselung von IT-Hardware wie Laptops oder Festplatten, zum Beispiel mit dem AES-256 Algorithmus, führt datenschutzrechtlich dazu, dass eine Kenntnisnahme von personenbezogenen Daten ausgeschlossen ist und lässt damit auch keine Informationspflichten der verantwortlichen Stelle gegenüber der Datenschutzaufsichtsbehörde und den betroffenen Personen entstehen.

Sachverhalt	2010	2011	2012	2013	2014	Gesamt
Hacking von Internet-Websites	6	2	2	7	2	19
Kopieren von EC-Kartendaten an Geldautomaten (Skimming)		4	6	8	1	19
Diebstahl bzw. Einbruch-Diebstahl von Datenträgern oder DV-Geräten	3	1	2	12	10	28
Fehlversendungen und Verlust von Datenträgern auf dem Transportweg	1		1	4	8	14
Verschiedene weitere Sachverhalte		3	2	1		6
Summe	10	10	13	32	21	86

21.2 Verlust von Daten bzw. Datenträgern auf dem Transportweg

Vergleichsweise häufiger betrafen informationspflichtige Datenpannen auch den Bereich des Transportwegs personenbezogener Daten, z. B. bei Fehlversendungen an Dritte, dem Verlust von Unterlagen auf dem Post- und sonstigen Transportweg oder der Beschädigung verschlossener Sendungen mit Kenntnisnahmemöglichkeit vom Inhalt für Dritte.

Bei elektronischen Datenträgern zum Datentransport, wie USB-Sticks, ist gleichfalls eine sichere Verschlüsselung geboten, siehe oben.

Fehlversendungen können nur durch sorgfältige Arbeitsweise und Überwachung der Technik verhindert werden, worauf durch organisatorische Maßnahmen hinzuwirken ist.

21.3 Hacking der Internet-Zugangsdaten bei einer Privatschule

Bei dem Homepage-Provider einer Privatschule wurden die Internet-Zugangsdaten (E-Mail-Adressen und Passworte) der Lehrer und Schüler mittels SQL-Injection gehackt und anschließend wohl als Beweis des Erfolgs auf einer Hacker-Plattform im Internet veröffentlicht. Da die verwendeten Passworte mangels technischer Vorgaben teilweise völlig unzureichend gestaltet waren, z. B. nur drei, vier oder fünf Ziffern oder Wörterbuchbegriffe als Passwort, und außerdem zu schwach verschlüsselt waren (MD5-Hashwerte ohne zusätzlichen SALT-Wert), konnten Dritte die meisten Passworte ohne größere Mühe entschlüsseln.

Weil verschiedene Personen aus Bequemlichkeit die gleichen Zugangsdaten für mehrere Internet-Dienste verwenden, z. B. auch bei Online-Bezahldiensten, versuchen Kriminelle, aus erlangten Zugangsdaten insoweit finanziellen Nutzen zu ziehen.

Es war deshalb eine sofortige Unterrichtung der betroffenen Lehrer und Schüler geboten, damit diese ihre Passwortvergaben prüfen und bei Bedarf ändern, um finanzielle Schäden zu vermeiden. Des Weiteren war bei der Schule und deren Homepage-Provider die Passwortvergabe und die Passwortverschlüsselung dem Stand der Technik (siehe Kapitel 22.7) anzupassen.

21.4 Hacking der Kundendaten eines Internetshops

Eine deutsche geschäftliche Internet-Handelsplattform mit knapp 700. 000 registrierten Nutzern hatte für die technische Umsetzung einen Provider in Litauen im Einsatz. Dort hatten Unbefugte Zugriff auf die Nutzerdatenbank und hatten mit den erlangten Daten versucht, Geld von der deutschen Internet-Plattform zu erpressen.

Erlangt wurden E-Mail-Adressen und nur unzureichend verschlüsselte Passwörter sowie teilweise auch Namen, Postadressen, usw.

Die betroffenen Nutzer mussten unverzüglich per Mail informiert und aufgefordert werden, sofort ihre Passworte bei der Handelsplattform zu ändern sowie in gleicher Form bei anderen Internet-Diensten verwendete Zugangsdaten zu ändern. Darüber hinaus waren die Sicherheitsmaßnahmen bei dem Dienstleister in Litauen zu verbessern, insbesondere eine ausreichende Verschlüsselung der Passwörter einzuführen.

21.5 Hacking bei einem Reisebuchungsdienstleister

Bei einem IT-Dienstleister für viele bundesweit verteilte Reisebüros und Online-Reisebuchungsportale wurden tausende Datensätze von Reisebuchungskunden einschließlich deren Post- und E-Mail-Adressen, Telefonnummern sowie Kreditkartennummern mit zugehörigen Sicherheitsnummern (CVV-Nummern) von Unbefugten in Erfahrung gebracht.

Die Reisebüros und Online-Reisebuchungsportale mussten unverzüglich alle betroffenen Kunden informieren und zur verstärkten Kontrolle ihrer Kreditkartenabrechnungen im Hinblick auf eventuelle Betrugssachverhalte auffordern.

21.6 Geiselnahme von Vereinsdaten

Der Kassierer eines Vereins wurde von einem vermeintlichen Service-Mitarbeiter eines Betriebssystemherstellers unaufgefordert kontaktiert. Dieser bot eine unkomplizierte und schnelle Beseitigung einer angeblichen Sicherheitslücke auf dessen PC an. Nachdem der Fremde Zugriff auf den Rechner hatte, konnte der PC nicht mehr gestartet werden. Der Kassierer sollte für ein Entsperren seines Rechners ein „Lösegeld" in Form anonymer digitaler Zahlung tätigen.

Es musste davon ausgegangen werden, dass Daten der Vereinsmitglieder einschließlich deren Bankverbindungsdaten abgegriffen wurden.

Weil Täter mit erlangten Bankverbindungsdaten immer wieder versuchen, über betrügerische Lastschrifteinzüge an das Geld der betroffenen Personen zu kommen, waren die Vereinsmitglieder über den Datendiebstahl zu informieren und auf die deshalb gebotene sorgfältige Überwachung ihrer Girokontoumsätze hinzuweisen. Natürlich war auch die Zugriffssicherheit für Externe bei dem PC des Vereinskassiers zu verbessern.

21.7 Diebstahl einer Datensicherungsfestplatte mit Gesundheitsdaten

Bei einem Unternehmen mit dem Tätigkeitsfeld der Eingliederung von Menschen mit seelischen Erkrankungen wurde eine unverschlüsselte Back-up-Sicherungsfestplatte mit den Daten zu gesunden und kranken Mitarbeitern gestohlen, einschließlich deren Bankdaten, Gesundheitsdaten in Berichten des Sozialdienstes, Schwerbehinderten-Status usw.

Die betroffenen Mitarbeiter mussten hierüber informiert werden, zum einen, weil Täter mit erlangten Bankverbindungsdaten immer wieder versuchen, über betrügerische Lastschrifteinzüge an das Geld der betroffenen Personen zu kommen, zum anderen, um sich auf die mögliche Offenlegung ihres teilweise schwierigen Gesundheitszustandes einstellen zu können.

Auch die Verschlüsselung von Backup-Sicherungsfestplatten ist mittlerweile mit dem AES-256 Algorithmus bei dem Unternehmen eingeführt worden – für die entwendeten Daten leider zu spät.

22

Technischer Datenschutz und IT-Sicherheit

22 Technischer Datenschutz und IT-Sicherheit

22.1 Technische Prüfung von Apps

Mit Hilfe von Techniken aus dem Bereich der Schadcodeanalyse können wir Apps gezielt analysieren, so dass wir deren internes Verhalten annähernd so verstehen wie der Entwickler, der die App ursprünglich programmiert hat.

Smartphones und Tablets sind mittlerweile Bestandteil des Alltags und haben eine feste Position bei der mobilen Nutzung von Internetaktivitäten eingenommen. Immer mit dabei sind Apps – mehr oder weniger kleine Anwendungen, die auf der einen Seite nützliche Dienste für den Anwender verrichten, aus Datenschutzsicht aber Risiken bedeuten, da das Smartphone bei vielen Menschen der zentrale Sammelpunkt der digitalen Identität geworden ist. Durch den Zugriff auf den Standort, die im Gerät gespeicherten Adressen und Termine, Fotos und Videos sowie auf Dateien, kann eine App, die unbefugt ihre Zugriffsmöglichkeiten „ausnutzt", schlimmen Schaden am Persönlichkeitsrecht der Nutzer anrichten.

In den Medien ist deswegen häufig von einem „Spion in der Hosentasche" die Rede, der als Bezahlung für seine vermeintlich kostenlosen Dienste die personenbezogenen Daten der Nutzer verwendet. Aus datenschutzaufsichtlicher Sicht stellt sich in diesem Zusammenhang die Frage, wie eine App technisch analysiert werden kann, um festzustellen, ob diese einen großzügigen Zugriff auf die Daten der Nutzer gestattet oder gar als „trojanisches Pferd" das Gerät in eine digitale Wanze oder in einen Sensor zur Erstellung von Bewegungsprofilen umwandelt. Basierend auf Methoden der Schadsoftwareanalyse hat das BayLDA deswegen zu Beginn des Jahres 2013 ein Prüflabor für mobile Anwendungen aufgebaut, mit dem folgende Analysen möglich sind:

- **Dynamische Analyse**

  Mit einer dynamischen Analyse werden Datenflüsse, die eine App mit den beteiligten Servern durchführt, sichtbar gemacht. Durch Protokollierung dieser Datenflüsse auf Netzwerkebene sowie „Man-In-The-Middle"-Techniken innerhalb der Laborumgebung kann damit festgestellt werden, mit welchen Servern eine App wann kommuniziert und in vielen Fällen sogar, welche Daten an diese übertragen werden.

- **Statische Analyse**

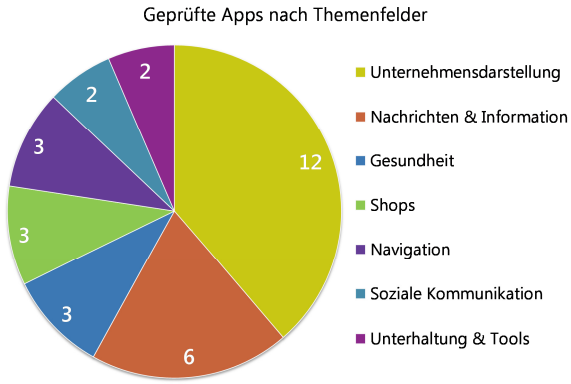
  Anhand einer statischen Analyse mittels Reverse-Engineering-Techniken wird der Quelltext einer App derart rekonstruiert, dass die genaue Implementierung nachvollzogen werden kann. So ist es zum Beispiel bei einer Android-App damit möglich, festzustellen, welche Daten mit der Berechtigung „Kontakte lesen" tatsächlich ausgelesen werden und was im Anschluss mit den Daten geschieht. So wurde zum Beispiel bei einer Navigations-App festgestellt, dass die genannte Berechtigung nur für die Anzeige von im Gerät gespeicherten Kontakten verwendet wurde. Eine ausgewählte Adresse wurde dann in eine lokale Navigationskomponente übergeben – eine Übermittlung von Adressdaten an den App-Betreiber oder Dritte fand dagegen nicht statt.

- **Forensischer Ansatz**

  Beim forensischen Ansatz werden die Datenspuren, die die Nutzung einer App auf dem Gerät hinterlässt, ausgewertet. Durch eine Umgehung der Sicherheitsrestriktionen durch „Jailbreak" bzw. „Rooting" kann das Dateisystem der Geräte ausgelesen werden. Da viele Apps Daten in eigenen, App-lokalen Datenbanken abspeichern, kann durch Auslesen dieser Datenbanken ein Rückschluss auf das interne App-Verhalten gezogen werden. So stellte sich uns zum Beispiel die Frage, wie mit einem Cookie, der die MAC-Adresse des Smartphones enthielt, umgegangen

wird oder auch, inwiefern ein in den Konfigurationsdateien im Klartext gespeichertes Passwort den Anforderungen an die Zugangskontrolle nach der Anlage zu § 9 BDSG noch erfüllen kann.

Nach Aufbau des Prüflabors haben wir im Berichtszeitraum bei 31 zufällig ausgewählten Apps bayerischer Unternehmen eine technische Prüfung mit den beschriebenen Ansätzen durchgeführt. Unter Berücksichtigung der Erfahrungen, die wir aus diesen Analysen gewonnen hatten, wurde unser technischer Prüfkatalog, der die aufsichtlichen Prüfungen strukturiert ablaufen lässt, weiter verfeinert. Bei Mängeln, die einen Verstoß gegen die technischen und organisatorischen Maßnahmen nach § 9 BDSG (samt Anlage) darstellten, wurde im Prüfungsfall ein aufsichtliches Verfahren gegen die Unternehmen eröffnet und eine Nachbesserung der App durchgesetzt.



Bei ca. 70% der geprüften Apps wurden Mängel unterschiedlicher Ausprägung festgestellt. Beispiele hierfür sind:

- Geräte- bzw. Kartenkennungen wurden oftmals ohne Erfordernis und Einwilligung übertragen.
- Standortdaten wurden unnötig häufig und zu genau erfasst.
- Logging wurde sehr intensiv eingesetzt (z. T. mit personenbezogenen Daten).
- Reichweitenmessungsverfahren wurden auch bei Apps mangelhaft eingesetzt.
- Unverschlüsselte Übertragung der Zugangsdaten über HTTP.
- Mangelhafte Löschung personenbezogener Daten bei Deinstallation der App.

Technische App-Prüfungen sind mittlerweile ein fester Bestandteil unseres „Werkzeugkastens" und werden sowohl bei Datenschutzbeschwerden über eine App als auch proaktiv und anlasslos für Kontrollen eingesetzt.

22.2 IT-Sicherheit im Kontext des Datenschutzes

Zur Vermeidung von Vorfällen sind geeignete und angemessene technische und organisatorische Maßnahmen zu treffen.

Der Begriff der IT-Sicherheit ist durch die Berichterstattung der Medien über spektakuläre Angriffe von Kriminellen oder die Massenüberwachung durch die Geheimdienste auch in den Blickpunkt einer breiten Öffentlichkeit geraten. Gerade personenbezogene Daten bergen ein hohes Risiko für den Einzelnen, sollten diese einmal in die Hände von Unbefugten gelangen. Dies können z. B. Bank- oder Kreditkartendaten, Kommunikationsinhalte (wie E-Mails oder Messenger-Nachrichten) als auch äußerst sensible Daten wie Gesundheitsdaten oder Informationen zu politischen Tätigkeiten sowie der ethnischen Herkunft sein. Auch Daten, die auf den ersten Blick etwas schwerer zu fassen sind, wie das Surfverhalten im Web oder das geographische Bewegungsverhalten (u. a. ermittelbar durch ein mitgeführtes Smartphone) bergen hohe Risiken für das Persönlichkeitsrecht, sollten diese mit der Person in Verbindung gebracht und ausgewertet werden.

Streng genommen wird der Begriff der IT-Sicherheit für die Sicherung von Informationstechnik (z. B. Netze durch Firewalls, Rechner, Serverräume) verwendet und umfasst damit nicht den Schutz der Daten, die sich in dem Begriff der Informationssicherheit wiederfinden. Heutzutage müsste sogar häufig auch von Cybersicherheit gesprochen werden, da viele Systeme weitmaschig über das Internet vernetzt und in Cloud-Diensten integriert sind. Im Folgenden wird aber der Begriff IT-Sicherheit

aufgrund der umgangssprachlichen Verbreitung in der Praxis für all diese Bereiche verwendet.

Das BDSG legt in § 9 (Technische und organisatorische Maßnahmen) fest, dass verantwortliche Stellen für den Schutz der ihnen unterliegenden Daten zu sorgen haben. Dabei sind sowohl technische als auch organisatorische Maßnahmen zu treffen, die (im Kontext der IT-Sicherheit) die Vertraulichkeit, Integrität und Verfügbarkeit der personenbezogenen Daten gewährleisten sollen. Dazu sind insbesondere, aber nicht nur, die Maßnahmen zu treffen, die in der Anlage zu § 9 BDSG aufgelistet sind. Da die IT-Sicherheit auch im Spannungsfeld von Kosten der Schutzmaßnahmen und der Anwendbarkeit im Alltag (durch die Anwender) steht, wird ein hundertprozentiges Schutzniveau nie praktikabel erreicht werden können. Aus diesem Grund fordert § 9 BDSG nur diejenigen Maßnahmen, deren Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht. Dieser Schutzzweck leitet sich aus dem potentiellen Schaden am Persönlichkeitsrecht ab, sollten Unbefugte Zugriff auf personenbezogene Daten bekommen. Als praxisnahe Methode eignet sich hier eine Einstufung in die Schutzbedarfskategorien „normal", „hoch" und „sehr hoch", die in der IT-Sicherheit, unabhängig vom Blickwinkel des Datenschutzes, häufig verwendet werden. Handelt es sich um besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG, so sind diese mindestens in die Kategorie „hoch" einzustufen, während zum Beispiel Adressdaten eines Online-Shops einem „normalen" Schutzbedarf zugeordnet werden. Im Unterschied zur Risikobewertung ohne Blickpunkt auf den Datenschutz ist die Prüfung der Verhältnismäßigkeit immer auf den einzelnen Betroffenen auszurichten. So mag es zum Beispiel für einen Online-Shop aus unternehmerischer Sicht tolerierbar sein, durch Hacking-Angriffe die Daten von zehn Kunden pro Jahr an Unbefugte zu offenbaren und deswegen auf einen aufwändigeren Penetrationstest zu verzichten – aus Sicht des Datenschutzes müssen die Maßnahmen in diesem Beispiel trotzdem getroffen werden.

Zur Feststellung, welche Maßnahmen getroffen werden müssen, kann es hilfreich sein, die konkreten Bedrohungen für die verantwortliche Stelle als Ausgangspunkt zu nehmen. Bedrohungen existieren immer und ergeben, sofern Schwachstellen in den technischen und organisatorischen Maßnahmen vorhanden sind, die von einer Bedrohung ausgenutzt werden können, eine Gefährdung. Wird diese tatsächlich ausgenutzt, so spricht man von einem Vorfall. Dies könnte zum Beispiel ein Smartphone-Trojaner sein, der auf das Auslesen einer Adressliste spezialisiert ist und erst dann tätig wird, wenn dieser aufgrund des organisatorischen Mangels eines Mobile Device Managements auf einem Smartphone installiert wird, das nicht die neueste Firmware-Version beinhaltet. Ein solcher Vorfall kann zu einem Schaden führen (die entwendeten Adresslisten werden für Spear-Phishing erfolgreich verwendet) oder, wenn man Glück hat, auch nicht (die entwendeten Adresslisten finden auf dem Schwarzmarkt keinen Käufer).

Geeignete Maßnahmen nach § 9 BDSG müssen, sofern diese dem Angemessenheitsgrundsatz nicht widersprechen, Gefährdungen so reduzieren, dass der Schutz personenbezogener Daten (der Einzelnen) gewährleistet wird. Welche Maßnahmen in einem angemessenem Verhältnis stehen, wird auch von uns in (Vor-Ort-)Kontrollen bewertet. Gegebenenfalls werden erforderliche Maßnahmen im aufsichtlichen Verfahren durchgesetzt.

22.3 IT-Sicherheitsorganisation

Eine Organisation von IT-Sicherheit ist notwendig, um den Schutz personenbezogener Daten zu gewährleisten.

In unserer aufsichtlichen Praxis wird bei Fragen zur IT-Sicherheit häufig seitens der Unternehmen argumentiert, dass eine Firewall sowie ein Antivirenscanner vorhanden und damit die notwendigen Schutzmaßnahmen nach § 9 BDSG umgesetzt seien. Eine – oder mehrere – Firewalls sind auch aus unserer Sicht sicherlich ein notwendiger Baustein zum Erreichen eines angemessenen Schutzniveaus. Auch Antivi-

rensoftware muss, trotz der zum Teil nicht hohen Erkennungsraten bei neuem oder spezialisiertem Schadcode, vorhanden sein. Die Wirksamkeit von IT-Sicherheitsprodukten ergibt sich jedoch nicht nur aus dem Zweck, zu dem diese eingesetzt werden (eine klassische Firewall wird z. B. keinen Schutz gegen Cross-Site-Scripting bieten können), sondern hängt vielmehr davon ab, ob diese sicher konfiguriert und administriert werden. Als Negativbeispiele in der aufsichtlichen Praxis treten hier IT-Systeme auf, die durch einen Einstellungsfehler (wie „allow all" auf der Paketfilterebene der Firewall) den Zugriff auf einen Datenbankserver ermöglichen, der nur mit einem einfachen Passwort geschützt ist und so den Zugriff auf alle gespeicherten Daten ohne wirksame Schutzmechanismen offenbart.

Die Verantwortung bei Szenarien dieser Art einfach auf den Administrator abzuwälzen, greift deutlich zu kurz. Vor allem die erforderlichen personellen Kapazitäten, die finanzielle und zeitliche Ausstattung für regelmäßige und hochspezialisierte Schulungen der Mitarbeiter sowie die Aufgaben- und Verantwortungsteilung im IT-Sicherheitsumfeld müssen im Unternehmen klar geregelt sein. Eine ausreichende Sicherheit der personenbezogenen Daten erreicht ein Unternehmen nämlich nur dann, wenn die IT-Sicherheit tatsächlich zur „Chefsache" wird und eine Organisation der IT-Sicherheit vorhanden ist.

Dazu sollte einerseits eine IT-Sicherheitsleitlinie entwickelt werden, die ein klares Bekenntnis der Geschäftsführung enthält und die notwendigen Ressourcen und Kompetenzen eindeutig regelt. Eine Umsetzung dieser Leitlinie in der Praxis findet sich wiederum in aktuell gehaltenen (und für die verantwortliche Stelle spezifischen) IT-Sicherheitsrichtlinien wieder. Durch den benannten IT-Sicherheitsverantwortlichen wird dann der Sicherheitsprozess mit Leben gefüllt (u. a. eine Identifizierung kritischer Daten und Anwendungen sowie eine Umsetzung von Schutzmaßnahmen). Eine regelmäßige Überprüfung und Anpassung an sich ändernde Gefährdungslagen stellt dann das eigene Sicherheitskonzept kritisch auf den Prüfstand.

Im Rahmen der aufsichtlichen Praxis prüfen wir deshalb neben den technischen Anforderungen des § 9 BDSG auch die organisatorischen Schutzmaßnahmen eines Unternehmens. Wenn es zum Beispiel zu einer unrechtmäßigen Übermittlung personenbezogener Daten an unbefugte Dritte gekommen ist, kann es im Einzelfall dazu führen, dass ein Bußgeld gegen die Geschäftsführung einer verantwortlichen Stelle verhängt wird, sollte sich herausstellen, dass die notwendigen Organisationsmaßnahmen zur IT-Sicherheit (grob) fahrlässig unterlassen wurden.

22.4 Verschlüsselung

Der Schutz personenbezogener Daten durch kryptographische Verschlüsselungsverfahren ist heute wichtiger denn je und muss deshalb sorgfältig umgesetzt werden.

Spätestens seit der Aussage von Edward Snowden, dass „Verschlüsselung funktioniert", sollte der Stellenwert geeigneter Verschlüsselungsverfahren zur Sicherung personenbezogener Daten bewusst geworden sein. Das BDSG sieht diesen Stellenwert explizit in der Anlage zu § 9 BDSG, wenn es um die Umsetzung der Schutzmaßnahmen der Zugangs-, Zugriffs- und Weitergabekontrolle geht. Insbesondere bei diesen Kontrollen sind Verschlüsselungsverfahren nach dem Stand der Technik einzusetzen. Damit wird die Wertigkeit und Notwendigkeit kryptographischer Verfahren benannt, die sowohl ausreichend (kryptographisch) sicher sind – also unter praktischen Szenarien und in absehbarer Zeit nicht „geknackt" werden können – als auch in der tatsächlichen Anwendung keine bekannten Schwachstellen besitzen, mit der die Verschlüsselung umgangen werden kann.

Ein in der aufsichtlichen Praxis häufig vorkommender Sachverhalt ist der Einsatz von Hashfunktionen, die fälschlicherweise als Verschlüsselungsverfahren benannt und auch eingesetzt werden. Bei Hash-Verfahren kann nur dann von Verschlüsselung gesprochen werden, wenn sogenannte „keyed-hash"-Verfahren eingesetzt

werden. Bei diesen Algorithmen wird immer noch ein kryptographischer Schlüssel mit verwendet, ohne welchen eine Rückrechnung eines Hashwertes auf den ursprünglichen Eingabetext nicht (praktikabel) möglich ist.

In der Praxis werden heutzutage vielfältige Verschlüsselungsverfahren eingesetzt: VPN-Verbindungen basieren meist auf dem IPSec-Protokoll, E-Mails können mit S/MIME oder PGP auf Inhaltsebene verschlüsselt werden, Backups werden durch eine AES-256-Verschlüsselung sicher bei Dritten aufbewahrt und SSL/TLS schützt die Kommunikation im Web (durch HTTPS) oder beim Transport von E-Mails (STARTTLS).

Werden personenbezogene Daten über das Internet versendet, so ist eine wirksame Verschlüsselung mit einem kryptographischen Verfahren nach dem Stand der Technik zwingend notwendig. Die Anwendung dieser Verfahren war und bleibt ein Schwerpunkt bei unseren Kontrollen. Sofern personenbezogene Daten über das Web (HTTP) übertragen werden, ist eine HTTPS-Verschlüsselung einzusetzen. Dies betrifft z. B. die Eingabe von Zugangsdaten im Rahmen einer Authentifizierung (Login-Name und Passwort), die Übermittlung von Inhaltsdaten als auch Session-Token, die einen mittelbaren Personenzug herstellen können. Für einen wirksamen Einsatz dieser Transportverschlüsselung müssen die Webserver so konfiguriert sein, dass die Verschlüsselung nicht umgangen werden kann. Das Protokoll SSL3 ist spätestens seit dem „Poodle"-Angriff, der Session-Cookies mit verhältnismäßigem Aufwand entwenden kann, nicht mehr als sicher einzustufen. Als Stand der Technik sollte deswegen das Protokoll TLS1.2 verwendet werden, das von allen modernen Browsern und Betriebssystemen unterstützt wird.

Ein besonderes Augenmerk ist auf die Problematik zu richten, dass verschlüsselte Verbindungen von einem Angreifer auf Vorrat gespeichert und ggf. zu einem späteren Zeitpunkt entschlüsselt werden könnten. Dies wäre zum Beispiel durch das Brechen eines in der HTTPS-Verschlüsselung verwendeten Algorithmus oder einfacher, durch das Entwenden des privaten Langzeitschlüssels auf Seiten des Webservers möglich. Werden auf dem System dagegen nur Verschlüsselungsalgorithmen mit Perfect Forward Secrecy unterstützt, so wird für jede verschlüsselte Verbindung ein neuer Verschlüsselungsschlüssel generiert, der sich nicht vom geheimen Langzeitschlüssel des Webservers ableitet. Ein Angreifer, der den privaten Schlüssel in Erfahrung bringt (möglich zum Beispiel über die Heartbleed-Lücke) könnte damit folglich auf Vorrat aufgezeichnete Verbindungen nicht nachträglich entschlüsseln. Selbst bei Brechen eines verschlüsselten Datensatzes, was nur mit immensem Aufwand möglich ist, wäre lediglich der Inhalt des geknackten Datensatzes offenbart und nicht die Inhalte aller anderen Datensätze.

Der Aufwand der Implementierung von Perfect Forward Secrecy ist im Allgemeinen äußerst gering, da nur die Menge aller Cipher-Suites auf diejenigen beschränkt werden müssen, die das sogenannte Diffie-Hellmann-Verfahren zum Schlüsseltausch einsetzen. Vereinzelt kann es bei verantwortlichen Stellen dazu führen, dass diese, sofern die bisher eingesetzte Soft- bzw. Hardware veraltet ist, ein Upgrade auf den aktuellen Stand durchzuführen haben. Da dies aber bei Einsatz von IT-Systemen grundsätzlich zur Sicherstellung eines ausreichenden Schutzes notwendig ist, stellt der Aufwand für die Umsetzung von Perfect Forward Secrecy ein verhältnismäßiges Mittel nach § 9 BDSG dar und ist daher umzusetzen.

Bei Einsatz von Verschlüsselungsverfahren hängt die Sicherheit auch wesentlich von den Schlüssellängen ab. Die Länge muss beim jeweiligen Algorithmus so gewählt werden, dass die Vertraulichkeit nicht nur zum Zeitpunkt der Verschlüsselung gewährleistet werden kann. Während bei der Übermittlung einer Transaktionsnummer bei Bankgeschäften ein Verschlüsselungsverfahren nur einige Minuten sicher sein muss, kann zum Beispiel bei Gesundheitsdaten, die über das Internet transportiert werden, die notwendige Vertraulichkeitsdauer mehrere Jahrzehnte lang sein. An diesen Zeitspannen orientieren sich unsere Anforderungen bei der Bewertung kryptographischer Verfahren. So sollte beim symmetrischen AES-Verfahren eine Schlüssellänge von 256-Bit gewählt werden, die nach heutigem Kenntnis-

stand auch eine langgültige Vertraulichkeit gewährleistet – auch nicht so bekannte Verfahren wie beispielsweise Blowfish eignen sich bei entsprechend langer Schlüssellänge. Bei Einsatz des asymmetrischen RSA-Verfahrens ist bei personenbezogenen Daten mit normalem Schutzbedarf eine Schlüssellänge von 2048-Bit als Stand der Technik anzusehen – bei erhöhtem Schutzbedarf und langgültiger Vertraulichkeit wäre eine Schlüssellänge bis zu 15360-Bit aus heutiger Sicht notwendig. Die Problematik liegt momentan aber darin, dass derart lange Schlüssel in der Praxis nicht effizient einsetzbar sind. In Anbetracht dieser momentanen Einschränkung sehen wir bei erhöhtem Schutzbedarf eine RSA-Schlüssellänge von 4096-Bit als zulässig aber auch zwingend notwendig an.

Durch Verfahren der sogenannten „Elliptischen Kurven" existiert neben dem RSA-Verfahren eine weitere Algorithmenklasse zur asymmetrischen Verschlüsselung, die effizienter berechenbar ist und heute schon ein höheres Sicherheitsniveau bei langgültiger Vertraulichkeit gewährleistet. Als Schlüssellänge sollten hier 512-Bit eingesetzt werden, sofern dies schon möglich ist. Zusätzlich muss der Kurventyp betrachtet werden, da es möglicherweise Verfahren gibt, die immanente Schwachstellen aufweisen und – zumindest von Seiten der Geheimdienste – ausnutzbar sein können.

22.5 Die Heartbleed-Lücke

Eine der schwerwiegendsten Sicherheitslücken der letzten Jahre fand sich im SSL-Protokoll und führte zum Verlust der Vertraulichkeit der verschlüsselten Kommunikation im Internet.

Im April 2014 wurde von einer Sicherheitslücke in der SSL-/TLS-Implementierung OpenSSL berichtet, die eine weite Verbreitung im Internet besitzt und zum Beispiel von vielen Webservern und E-Mail-Servern aber auch Firewalls eingesetzt wird. Durch einen Programmierfehler kann ein Server, der diese Lücke aufweist, derart angesteuert werden, dass ein Teilbereich des Hauptspeichers unbemerkt über das Internet ausgelesen werden kann. Durch häufig nacheinander ausgeführte Anfragen können zum Beispiel Teile des HTTPS-Verkehrs wie Session-Token, Adress- und Kreditkartendaten, aber möglicherweise auch der private Schlüssel des Webservers ausgelesen werden. Die Lücke tritt in den Versionen 1.0.1 bis 1.0.1f der OpenSSL-Bibliothek auf.

In vergangen Berichtszeitraum hatten wir auch in Bayern mehrere Eingaben zu dadurch verwundbaren Servern. Die betroffenen Unternehmen mussten schnellstmöglich ein Update der Systeme durchführen und ein neues SSL-Zertifikat beim Zertifikatsherausgeber beantragen. Während die meisten Webserver relativ zeitnah aktualisiert wurden, ergab sich durch eine Stichprobenprüfung bei E-Mail-Servern eine – für uns etwas überraschende – nicht so hohe Behebungsrate der Sicherheitslücke. Dies führte dazu, dass die Überprüfung der Heartbleed-Lücke im Rahmen der automatisierten E-Mail-Server Prüfung mit aufgenommen wurde (siehe Kapitel 3.4.3).

22.6 Datenschutzaspekte bei Webanwendungen

Webanwendungen sind durch Ihre meist weltweite Erreichbarkeit ein beliebtes Angriffsziel und müssen daher den Schutz personenbezogener Daten durch geeignete Schutzmaßnahmen sicherstellen.

Es vergeht kaum ein Tag, an dem in den Medien nicht von einem spektakulären Hacking-Angriff berichtet wird. So wurde im Jahr 2014 die Superlative bei der Zahl der Betroffenen solcher Vorfälle erreicht, indem Datensätze von Nutzern im sieben- oder gar achtstelligen Bereich „gestohlen" wurden.

Diese Entwicklung haben wir zum Anlass genommen, bei Datenschutzkontrollen von Unternehmen (siehe Kapitel 3) insbesondere auch Webanwendungen zu begutachten. Dabei muss die verantwortliche Stelle nachweisen, dass sie mit den Besonderheiten bezüglich der IT-Sicherheitsanforderungen, die diese Art von

Softwareanwendungen mit sich bringen, umgehen kann. So sind nicht nur der physikalische Schutz der Server und die Absicherung der Netzwerke durch Firewalls essentiell, sondern insbesondere auch das Bewusstsein, dass die eingesetzte Anwendung als solche die große Gefahr birgt, z. B. durch einen Softwarefehler eine ausnutzbare Schwachstelle zu offenbaren.

Im Rahmen der Kontrollen orientieren wir uns deshalb an Best Practice Ansätzen, die methodisch effizient umsetzbar sind und möglichst viele Schwachstellen bzw. Problemfelder aufdecken können. Dadurch haben die Unternehmen die Möglichkeit, proaktiv gezielte Maßnahmen zu treffen, bevor ein möglicher Schadensfall (z. B. Hacking) eintritt.

Zum einen verweisen wir dazu auf die OWASP Top 10 (2013), um potentielle Schwachstellen aufzuspüren, die möglicherweise anhand Injection-Angriffen, Cross-Site-Scripting oder Cross-Site Request Forgery Methoden ausgenutzt werden können. Ebenfalls wird überprüft, ob es zu einer Datenoffenbarung in den Webanwendungen kommen kann, indem auf vermeintlich geschützte Daten öffentlich zugegriffen werden kann. Verantwortliche Stellen müssen deshalb im Rahmen von Vor-Ort Kontrollen nachweisen, dass und ggf. wie sie mit diesen Arten von Schwachstellen in den eigenen Anwendungen umgehen.

> > >
https://www.owasp.org/index.php/Top_10_2013-Top_10

A1 – Injection

A2 – Broken Authentication and Session Management

A3 – Cross-Site-Scripting

A4 – Insecure Direct Object References

A5 – Security Misconfiguration

A6 – Sensitive Data Exposure

A7 – Missing Function Level Access Control

A8 – Cross-Site-Request Forgery

A9 – Using Components with Known Vulnerabilities

A10 – Unvalidated Redirects and Forwards

Einer der häufig von uns untersuchten Bereiche ist hierbei der Login. Sofern die Anmeldung an einer Webanwendung mittels Zugangsname und Passwort durchgeführt wird, stellt gerade der Schutz des Passwortes ein Hauptaugenmerk unserer Untersuchung dar. Das resultiert auch daraus, dass viele Anwender das gleiche Passwort bei mehreren Diensten (u. a. Soziales Netzwerk, Online-Shop, Email) verwenden und ein unbefugter Zugriff auf die Authentifizierungsdaten weitreichende Folgen wie z. B. Betrugsfälle, Identitätsdiebstahl und Verwendung der Daten für Cyberangriffe haben kann. Eine sichere Speicherung der Passwörter ist daher wichtig und mit dafür geeigneten Hash-Verfahren technisch mittlerweile problemlos möglich, da Verfahren wie bcrypt oder PBKDF2 in vielen Softwarebibliotheken einfach verfügbar sind. In der Praxis werden häufig aber immer noch ungeeignete Verfahren wie MD5 oder SHA für das Hashen von Passwörtern eingesetzt, die aufgrund ihrer effizienten Berechenbarkeit Mindestpasswortlängen von 12 bzw. 14 Stellen für einen sicheren Schutz gegen Brute-Force-Angriffe voraussetzen würden.

Ein Problemfeld ist nach wie vor auch der Umgang mit „vergessenen" Passwörtern. Diese werden auf Anforderung eines Kunden häufig immer noch im Klartext per E-Mail versendet. Wir bemängeln dies und fordern die Verantwortliche Stelle auf, diese Praxis abzustellen. Dabei verweisen wir auf einfache Verfahren wie zeitlich begrenzte Passwort-Ändern-Links, die zwar per E-Mail versendet werden, die Passworteingabe dann aber über eine HTTPS verschlüsselte Seite ermöglichen.

Die Überprüfung von Webanwendungen wird auch zukünftig ein fester Bestandteil unserer aufsichtlichen Prüfungen sein und wird im Augenblick – bezüglich der Anzahl der von uns gefundenen Schwachstellen – nur durch die personellen Kapazitäten des technischen Referats begrenzt.

22.7 Sicherer Umgang mit Passwörtern

Die Authentisierung eines Nutzers an einem System mit Zugangsname und Passwort birgt hohe Risiken des Identitätsdiebstahls.

Als Anfang 2014 das Bundesamt für Sicherheit in der Informationstechnik die Meldung über eine zugespielte Datenbank mit E-Mail-Adressen samt Passwörtern veröffentlichte und die Gefahr von unbefugten Offenbarungen eigener personenbezogener Daten für jedermann greifbar wurde, war kaum vorstellbar, dass eine Steigerung bezüglich der Anzahl Betroffener noch möglich sein könnte. Als im Jahr 2014 die unfassbare Zahl von mehreren hundert Millionen gekaperter Identitäten die Runde machte, stellte sich noch dringlicher die Frage, wie die Schäden solch massenhafter Datenbestände verringert werden können.

Ein bedeutender Negativ-Faktor, dem wir in unseren Vor-Ort-Kontrollen nach wie vor sehr häufig begegnen, sind ungenügend gesicherte Passwörter zu Benutzerkonten, beispielweise von Web-Shops, Portalen und Kommunikationsangeboten. Kommt es bei diesen Unternehmen zu einem unbefugten Abgreifen von Datensätzen (zum Beispiel durch Ausnutzung von Web-Hacking-Schwachstellen), dann stellt meist ein geeignet gespeichertes Passwort die einzige Hürde zwischen der Entwendung der personenbezogenen Daten (Name, Adresse, Einkaufshistorie, …) als solche und deren Verwendung mittels Identitätsdiebstahl, um weitere Straftaten zu begehen, dar.

Erschreckend ist, dass es im Berichtszeitraum immer noch Webangebote gab und wohl auch nach wie vor gibt, die Passwörter im Klartext speichern. Kommt es dann zu einem erfolgreichen Angriff, zum Beispiel mittels SQL-Injection oder forensischer Analyse eines gefundenen Smartphones, so kann ein Angreifer die digitale Identität, die an dem Benutzerkonto hängt, übernehmen und den ursprünglichen Nutzer durch eine einfache Passwortänderung aussperren. Da viele Bürger für mehrere Dienste sowohl die gleiche E-Mail-Adresse als auch das gleiche Passwort verwenden, kann ein unzureichend gesicherter Dienst weitreichende Folgen für die betroffenen Nutzer haben. Dies ist u. a. auch ein Grund, wieso wir bei Hacking-Vorfällen, bei denen neben einer E-Mail-Adresse das Passwort im Klartext gespeichert oder unzureichend gesichert ist, von einer meldepflichtigen Datenpanne nach § 42 a BDSG ausgehen, bei welcher alle Betroffenen informiert werden müssen.

Bevor ein Passwort gespeichert wird, muss es durch geeignete Hash-Verfahren so umgewandelt werden, dass eine Rekonstruktion des ursprünglichen Passworts aus dem Hash-Wert mit praktikablen Mitteln nicht möglich ist. Das weit verbreitete MD5-Verfahren sollte nicht mehr eingesetzt werden; zwar ist dessen bekannte Schwachstelle durch einen Kollisionsangriff nicht unmittelbar auf die Passwortspeicherung übertragbar – das Risiko, dass auch weitere Schwachstellen zu diesem Verfahren entdeckt werden, die eine Rückrechnung erheblich vereinfachen, ist jedoch auch aufgrund deutlich sichererer Alternativen zu hoch. Während Hash-Verfahren wie RIPEMED oder SHA-256 noch als kryptographisch sicher gelten, haben diese bezüglich Brute-Force-Attacken (Durchprobieren aller bzw. der wahrscheinlichsten Passwortkombinationen) den Nachteil, dass sich diese effizient berechnen lassen. Man muss heute davon ausgehen, dass bei diesen Verfahren ein leistungsfähiger Rechner 10 Milliarden Hash-Werte pro Sekunde berechnen kann – ganz zu schweigen welche Möglichkeiten große Organisationen oder staatliche Stellen bei entsprechender Finanzausstattung hätten. Aus diesen Gründen fordern wir bei personenbezogenen Daten mit normalem Schutzbedarf mindestens 10-stellige und bei personenbezogenen Daten mit erhöhtem Schutzbedarf 12-14-stellige Passwörter, um zumindest eine gewisse Hürde bei der

Rückrechnung von entwendeten Passwörtern zu erreichen. Empfehlenswert sind für die Transformation von Passwörtern Hash-verfahren, die bezüglich Brute-Force-Attacken ineffizient sind, im Tagesgeschäft bei entsprechend performanten Servern aber zu einer akzeptablen Reaktionszeit bei den Anmeldevorgängen führen. Wir haben in diesem Zusammenhang Verfahren wie bcrypt oder PBKDF2 empfohlen, die für den Endkunden den Vorteil haben, dass auch 8-stellige Passwörter (bei entsprechender Zufälligkeit des Alphabets) ausreichend sicher sein können.

22.8 Konfiguration von Mailservern nach dem Stand der Technik

Mailserver müssen so konfiguriert werden, dass diese eine opportunistische Transportverschlüsselung mittels SSL/TLS unterstützen.

Die Kommunikation mit E-Mail erfolgt in vielen Fällen immer noch unverschlüsselt über das Internet, indem die Datenpakete über mehrere Router vom E-Mail-Sender zum E-Mail-Empfänger geleitet werden. Eine solche unverschlüsselte Verbindung ermöglicht es Dritten, den Inhalt der E-Mails zu lesen oder zu verändern. Selbst bei Einsatz einer Ende-zu-Ende-Verschlüsselung (z. B. mit PGP oder S/MIME) können bei einem Transport über einen unverschlüsselten Kanal noch sogenannte Meta-Informationen wie Absender, Empfänger, Zeitpunkt oder Betreff ermittelt werden. Aus diesem Grund müssen E-Mail-Server, die am Versand und Empfang personenbezogener Daten mit dem SMTP-Protokoll beteiligt sind, insbesondere auch STARTTLS zur Verschlüsselung unterstützen. Das STARTTLS-Protokoll, das im RFC 3207 beschrieben wird, erweitert das SMTP-Protokoll derart, dass bei dem Klartextverbindungsaufbau abgefragt werden kann, ob auch verschlüsselte Verbindungen über SSL/TLS möglich sind. Sofern dies der Fall ist und die beteiligten E-Mail-Server entsprechend konfiguriert sind, wird die Klartextverbindung durch das STARTTLS-Kommando in eine verschlüsselte Verbindung umgewandelt. Eine Absicherung der E-Mail-Kommunikation mit STARTTLS erhöht den Schutz der Vertraulichkeit von E-Mail-Kommunikation bezüglich passiver Angriffe (z. B. Mitlesen eines E-Mail-Inhalts an einem Internet-Knotenpunkt) deutlich. Wird dagegen eine Verbindung aktiv angegriffen, bspw. mit Man-In-The-Middle-Techniken, so kann der Aufbau des verschlüsselten Kanals, wenn auch erkennbar, unterbunden werden. Unterstützt ein E-Mail-Server keine STARTTLS-Verschlüsselung, so werden die E-Mail-Nachrichten trotzdem – wenn auch im Klartext – zugestellt (opportunistische Verschlüsselung). Aus diesen Gründen stellt das STARTTLS-Protokoll zwar nur einen geringen, aber nach unserer Auffassung mittlerweile notwendigen Baustein zur Absicherung elektronischer Kommunikation dar. Es muss allerdings ausdrücklich darauf hingewiesen werden, dass eine STARTTLS-Unterstützung keinen Ersatz für eine Ende-zu-Ende Verschlüsselung darstellt, die z. B. bei besonderen Arten personenbezogener Daten (u. a. Gesundheitsdaten) zwingend zusätzlich einzusetzen ist.

Werden (personenbezogene) Daten über das TLS-Protokoll ausgetauscht, so handeln die beiden beteiligten Stellen einen kryptographischen Schlüssel aus, mit dem die Inhalte verschlüsselt werden. Da bei Einsatz einer START-TLS-Verschlüsselung kryptographische Verfahren nach aktuellem Stand der Technik zu unterstützen sind (Anlage zu § 9 BDSG), muss der Schlüsseltausch durch Verfahren erfolgen, die Perfect Forward Secrecy unterstützen (Siehe Abschnitt 22.4).

22.9 Die richtige Konfiguration von Perfect Forward Secrecy bei SSL/TLS

Ein weitverbreitetes Missverständnis von der Funktionsweise von Perfect Forward Secrecy führt zu einer Abschwächung der Verschlüsselungsstärke oder gar zu entschlüsselbaren Verbindungen.

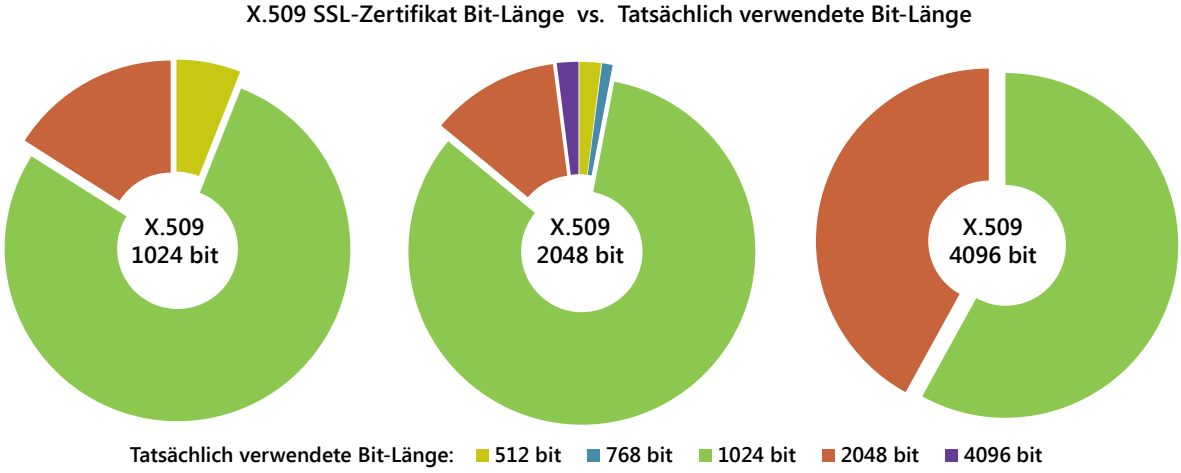
Eine vertrauliche Übertragung von Inhalten über das Internet ist ohne das SSL/TLS-Protokoll nicht vorstellbar. Fast alle webbasierten Dienste und viele Apps setzen dieses für

den Aufbau eines verschlüsselten Transportkanals ein. Die Sicherheit dieser Verbindungen hängt von vielen Faktoren wie Verschlüsselungsalgorithmen, Schwachstellen in der Implementierung (z. B. Heartbleed, „Change Cipher Spec"-Attacke), sowie Protokollversionen oder Verwendung eines vertrauenswürdigen Zertifikats mit ausreichender Schlüssellänge ab. Durch eine geeignete Konfiguration des Web- oder E-Mail-Servers kann Perfect Forward Secrecy (PFS) eingesetzt werden, bei dem für jede Verbindung ein eigener, zufällig generierter Verschlüsselungs-Key generiert wird. Das Server-Zertifikat wird in diesem Fall nicht für die Generierung des Schlüssels verwendet, sondern nur, um die Authentizität des Schlüsseltausches sicherzustellen.

Diese Besonderheit führt dazu, dass die Länge eines kryptographischen Schlüssels bei PFS nicht vom dem SSL-Zertifikat abhängt, das häufig von einer Zertifizierungsstelle erworben wird. Stattdessen hängt die Bitlänge von einer Einstellung in der SSL/TLS-Implementierung ab, die auch über Konfigurationsdateien abgepasst werden können sollte.

Im Rahmen der E-Mail-Server Prüfung wurde bei Einsatz von PFS auch überprüft, welche Schlüssellänge bei den jeweiligen Verbindungen zum Einsatz kam. Sehr häufig wurde festgestellt, dass die Bitlänge des Server-Zertifikats 2048-Bit (RSA) beträgt, die Bitlänge des Verschlüsselungsschlüssels aber nur 1024-Bit (RSA). In einigen Fällen waren die tatsächlichen Verbindungen sogar nur mit 512-Bit (RSA) abgesichert, wobei die Serverzertifikate 2048-Bit (RSA) hatten. In diesem Fällen kamen einzelne SSL-/TLS-Verbindungen mit so schwachen Schlüssellängen zustande, dass diese von entsprechend technisch versierten Angreifern in kurzer Zeit entschlüsselt werden könnten, obwohl vermeintlich „PFS mit 2048-Bit" zum Einsatz kam.

Im Rahmen unsere aufsichtlichen Aufgaben haben wir eine Erhöhung der Schlüssellänge von 512-Bit (RSA) gefordert. Zum jetzigen Zeitpunkt sehen wir RSA 1024-Bit als einen kritischen Grenzwert bezüglich der Schlüssellänge – es ist angedacht, nach Prüfung der Verhältnismäßigkeit entsprechend § 9 BDSG im Rahmen von weiteren automatisierten Online-Prüfungen eine Erhöhung der Schlüssellänge auf 2048-Bit (RSA) bei personenbezogenen Daten mit normalen Schutzbedarf und 4096-Bit (RSA) bei personenbezogenen Daten mit erhöhtem Schutzbedarf einschließlich Perfect Forward Secrecy als aktueller Stand der Technik aufsichtlich durchzusetzen.



22.10 Besucherstrommessung mit dem Smartphone

Gerätebezogene Identifikatoren wie die MAC-Adresse sollen zur Bewegungsprofilbildung von Besuchern in Einkaufszentren und Restaurants verwendet werden und werfen die Frage auf, wem denn die

Funksignale des eigenen Smartphones eigentlich gehören.

Das BayLDA wurde im Rahmen der aufsichtlichen Beratungstätigkeit von mehreren Herstellern von neu zu entwickelnden Produkten zu Rate gezogen, die Funksignale von mobilen Endgeräten für Marketing- und Prozessoptimierungszwecke auswerten möchten. Betroffene wären in den dargestellten Szenarien Besucher von Geschäften und Einkaufszentren sowie Kunden von Restaurantketten. Mit den vorgestellten Produkten werden von Smartphones die MAC-Adressen erhoben, die durch WLAN-Signale von jedem Gerät periodisch oder durch einen externen Auslöser ausgesendet werden. Zusätzlich sollen zum Teil die TMSI-Nummern erhoben werden, die ein Smartphone entsprechend einer momentan eingewählten Funkzelle zugeordnet bekommt. Anhand mathematischer Verfahren zur Triangulation, bei der neben einer eindeutigen Geräte-ID auch die Signalstärke aus mindestens drei Signalempfängern ausgewertet wird, kann ein auf wenige Meter genauer Standort eines Gerätes bestimmt werden. Anhand mehrerer zeitlich versetzter Datenerhebungen kann basierend auf der eindeutigen Geräte-ID ein Bewegungsprofil des Smartphones erstellt werden. Da eine MAC-Adresse fest der Netzwerkhardware eines Gerätes zugeordnet ist, ist ein so erstelltes Bewegungsprofil lange Zeit gültig und könnte auch mit anderen Bewegungsprofilen, die ebenfalls auf der MAC-Adresse des Gerätes basieren, verknüpft werden.

Aus datenschutzrechtlicher Sicht ist es von zentraler Bedeutung, ob MAC-Adressen (oder andere Geräte-IDs) sowie eine zeitliche Abfolge von verketteten Standorten als personenbeziehbare Daten angesehen werden. Die MAC-Adresse wird zum Beispiel bei Android im Rahmen einer Produktregistrierung, die mit dem Namen, der E-Mail-Adresse und häufig einer Kreditkarte einhergeht, an Google übertragen. Ebenso können Android-Apps, die Zugriff auf die Berechtigung „ACCESS_NETWORK_STATE“ erhalten, auf die MAC-Adresse des Geräts zugreifen und diese an Dritte übertragen. Auch ist es nicht auszuschließen, dass MAC-Adressen, die in WLAN-Signalen enthalten sind, gerade auch in Produkten zur Besucherstrommessung mit personenbezogenen Daten wie einer EC-Kartenzahlung verknüpft und an Dritte weitergegeben werden. Letzteres gilt auch für eine Abfolge von verketteten Standortdaten, die, sofern nur bei einem Standort Zusatzwissen zur Identifikation des Trägers vorhanden ist, zu einer Personenbeziehbarkeit von vermeintlich anonymen Bewegungsprofilen führen kann. Aus diesen Gründen sieht das BayLDA gerätebezogene Identifikationsdaten wie die MAC-Adresse als personenbezogenes Datum und damit die Anwendbarkeit des Bundesdatenschutzrechts als gegeben an.

Dies hat zur Folge, dass eine Erhebung der MAC-Adresse durch Dritte ohne Einwilligung des betroffenen Smartphonebesitzers datenschutzrechtlich problematisch ist. Eine Klärung mit dem Ziel einer einheitlichen Bewertung aller Datenschutzaufsichtsbehörden läuft derzeit noch.

22.11 Smart-TV-Prüfungen

Wir gehen der Frage nach, ob es den „Spion im Wohnzimmer“ wirklich gibt.

Die Vernetzung von bekannten Alltagsgegenständen mit dem Internet verändert nicht nur deren Einsatz weitreichend, sondern auch die Folgen für das informationelle Selbstbestimmungsrecht der Nutzer. Aus Handys wurden Smartphones, mit denen „auch noch telefoniert“ werden kann. PC-Programme, die früher von CDs installiert wurden, sind mittlerweile durch Apps ersetzt worden, die meist nur noch durch eine dauerhafte Internet-Anbindung funktionieren. Und so werden auch Fernsehgeräte – in früheren Zeiten Anschaffungen für längere Zeiten und unterscheidbar hauptsächlich in der Bildschirmgröße – durch interaktive und internetfähige Geräte ersetzt, die mit dem Namen „Smart-TV“ den Kunden zum Kauf animieren sollen.

Ähnlich den Smartphones sind die Änderungen, die sich bei Smart-TVs im Vergleich zu „normalen“ Fernsehgeräten ergeben, außerordentlich. Die Internetanbindung des Smart-TV beschränkt sich nicht nur auf einen Browser im

Fernseher (der erst mit zukünftigen Generationen praktikabel und benutzerfreundlich am TV selbst bedienbar sein wird), sondern erweitert das klassische Fernsehprogramm um sog. Mehrwertdienste, die unter dem Standardisierungsnamen HbbTV (Hybrid Broadcast Broadband TV) geläufig sind. Das lineare (Fernseh-) Signal wird hierbei um einen internetbasierten Rückkanal erweitert. Zunehmend bekannt werden darüber hinaus personalisierte Dienste wie z. B. ein elektronischer Programmführer (EPG), die dem Fernsehnutzer diejenigen Fernsehsendungen vorschlagen, die – zumindest anhand eines maschinell erstellten und ausgewerteten Nutzungsprofils – dem Betrachter wohl am besten gefallen könnten. Auch Apps, die zum Teil auf den Geräten vorinstalliert sind, können auf dem TV geladen bzw. ausgeführt werden und machen diese zum Informations-, Spiele- und Medienmittelpunkt einer jeden Wohnung.

Nachdem wir im Jahr 2013 die Smartphone-App-Prüfungen als einen unserer Schwerpunkte durchgeführt hatten, sollten im Jahr 2014 die Smart-TV-Geräte datenschutzrechtlich „erhellt" werden. Die genannte neue technologische Entwicklung ist aus Datenschutzsicht mit vielen Fragestellungen verbunden, die zeitnah abgeklärt werden müssen. Vor einer rechtlichen Klärung stellte sich uns zuerst die Frage, was die Smart-TV-Geräte hinsichtlich der technischen Datenübertragungen tatsächlich machen und wie dies verlässlich festgestellt werden kann. Im Vergleich zu Smartphones, bei denen es aktive Communities gibt und technisch interessierte Nutzer (u. a. mit Verlust der Garantie) in der Lage sind, über „Rooting" oder „Jailbreaks" einen Vollzugriff auf ein Gerät zu bekommen, ist der aktuelle Stand bei Smart-TV der, dass dieser ein für den Nutzer vollkommen geschlossenes System bzw. Gerät darstellt. Dies bedeutet, dass der TV zwar über die graphische Oberfläche so bedient werden kann, wie der Hersteller es vorgesehen hat – Einblick in die gespeicherten Daten innerhalb des Geräts kann aber i. d. R. nicht genommen werden. Auch das Löschen der eigenen Nutzerdaten, seien es Cookies oder personalisierte Anmeldedaten, sind im Vergleich zu einem PC über ein klassisches Dateisystem nicht möglich.

Da ein Smart-TV entweder über eine WLAN-Anbindung oder ein LAN-Kabel mit dem Internet verbunden ist, setzen wir die Möglichkeiten unseres Prüflabors (vgl. Kapitel 22.1) ein, um die entstehenden Datenflüsse gezielt zu analysieren. Anhand einer solchen dynamischen Prüfung können wir feststellen,

- wann ein Smart-TV mit welchen Servern kommuniziert (d. h. nach Nutzeraktion),
- welches Internetprotokoll eingesetzt wird (HTTP, HTTPS, ICMP,…) und
- was der Inhalt der Aufrufe ist (bei HTTP ggf. bei HTTPS).

Um einen aussagekräftigen Überblick über das Verhalten der in Deutschland erhältlichen Smart-TV-Geräte zu erhalten, haben wir in Abstimmung mit denjenigen Aufsichtsbehörden in Deutschland, in deren Bundesland ein Gerätehersteller seinen Sitz hat, ein datenschutzrechtliches Prüfprojekt gestartet (siehe Kapitel 3.4.8). Dazu wurden Testszenarien ausgearbeitet, die eine praxisnahe Nutzung der Geräte wiederspiegeln und eine technische Feststellung der jeweiligen Datenflüsse ermöglichen sollen. Folgende Kategorien standen im Fokus der Prüfungen:

1. Information bei Inbetriebnahme eines neuen Geräts
2. Datenflüsse bei Inbetriebnahme eines neuen Geräts ohne Nutzeraktion
3. Datenflüsse bei Nutzung des Smart-TVs als „normaler" Fernseher
4. Datenflüsse bei Nutzung von HbbTV
5. Datenflüsse bei Nutzung gerätespezifischer Hauptmenüs bzw. App-Panels
6. Datenflüsse bei Aufnahme (und anschließender Wiedergabe) einer Fernsehsendung auf einem USB-Datenträger
7. Datenflüsse bei Verwendung des elektronischen Programmführers
8. Datenflüsse bei Nutzung von Apps
9. Datenflüsse bei Wiedergabe von Medien (Videos, MP3s, Bilder) über den Smart-TV

Von besonderer Bedeutung ist aus Sicht des Datenschutzes, ob Datenflüsse existieren, die den Nutzer oder das konkrete Gerät eindeutig identifizieren (personenbezogene Daten) und/oder ob anhand der Gerätenutzung sog. Nutzungsprofile erstellt werden können, aus denen sich Aussagen über Interessen, das Alter, politische oder religiöse Ansichten sowie den Gesundheitszustand ableiten lassen (siehe Kapitel 7.7).

Im Rahmen von Amtshilfeverfahren hat das BayLDA im November/Dezember 2014 dreizehn aktuelle Smart-TVs (Modelle aus 2014) einer technischen Überprüfung unterzogen. Durch eine Marktabdeckung von ca. 90 % sollte ein repräsentativer Einblick in Funktionalitäten der Geräte genommen werden. Ziel der Prüfung war nicht, einzelne Geräte für gut oder schlecht zu befinden (was aufgrund der Produktvielfalt auf dem Markt und sich häufig änderbarer Firmware-Versionen auch nicht sonderlich praktikabel wäre), sondern anhand der beschriebenen Testszenarien eine Basis für eine (datenschutz-)rechtliche Bewertung und damit für eine aufsichtliche Kontrolle zu schaffen.

Ein Nutzer eines Smart-TV steht mehreren datenschutzrechtlichen Verantwortungssphären gegenüber, die sich je nach Smart-TV in einem oder mehreren Akteuren wiederfinden. Im Nachfolgenden stellen wir die unterschiedlichen Akteure kurz vor und beschreiben die jeweiligen Prüfungsergebnisse:

- **Geräte-Hersteller**

  Zur Aufrechterhaltung der Funktionalität des Gerätes sind Datenflüsse für regelmäßige Softwareupdates notwendig, die entweder Sicherheitslücken schließen oder neue Features anbieten. Es wurden von uns auch Aufrufe an Zeitserver und Inhaltsanbieter ermittelt, die z. B. Grafiken, Javascript-Code oder Textinformationen zur Darstellung über das Internet (mit HTTP) laden. Auffallend war, dass die Gerätehersteller i. d. R. eine eindeutige Geräte-ID (MAC-Adresse, Zufallszahl, Seriennummer) bei jedem Aufruf an die Server des Herstellers mitsenden. In manchen Fällen wurde auch festgestellt, dass grundlegende Bedienfunktionen (z. B. „Betreten des Einstellungsmenüs", „Öffnen des Medienplayers"), verknüpft mit der Geräte-ID, übertragen werden. Dies ermöglicht zumindest anhand der Datenbasis eine Einsichtnahme in die Art und Weise, wann und wie ein Gerät bedient wird.

- **HbbTV-Anbieter**

  HbbTV-Inhalte werden von den Fernsehsendern angeboten und stellen vom Grundsatz her speziell an den Fernseher angepasste HTML-Seiten dar. Zugriffe auf Fernsehfunktionalitäten sind nur über die im HbbTV-Standard definierten Javascript-Schnittstellen möglich. Wie bei einem Browser auf einem PC besteht dabei auch die Möglichkeit, Cookies zu setzen und diese dem HbbTV-Seitenanbieter mit einem HTTP-Request zuzusenden. Die Überprüfung von Fernsehsendern war nicht Schwerpunkt der Prüfung, da uns die grundlegende Funktionalität von HbbTV schon bekannt war. Dennoch wurden im Rahmen der Smart-TV-Prüfung exemplarisch Fernsehsender ausgewählt, um festzustellen, wie sich HbbTV-Inhalte auf den jeweiligen Geräten verhalten. Ebenso wurde in den Prüfszenarien analysiert, inwiefern auch Aufrufe an den Gerätehersteller gehen, wenn „nur" HbbTV-Inhalte angezeigt werden, da diese – zumindest aus Sicht des Endanwenders – mit dem Gerätehersteller nichts zu tun haben.

  Beispielhaft wurde auch gezeigt, wie ein senderübergreifendes Tracking von HbbTV-Inhalten bei manchen Sendern eingesetzt wird und damit prinzipiell festgestellt werden kann, wie Fernsehprogramme innerhalb einer Sendergruppe genutzt werden. Vom Ansatz ist dies insofern bedeutend, da damit zumindest technisch eine Möglichkeit besteht, Fernsehquoten mit einer hohen Wahrscheinlichkeit zu bestimmen, ohne dass die Fernsehzuschauer dazu einge-

willigt hätten oder dies überhaupt merken.

- **App-Store Betreiber**

  Die Verantwortlichkeit des Betriebs des App-Stores des jeweiligen Smart-TV liegt bei manchen Geräten bei dem Gerätehersteller, bei vielen jedoch bei einer unabhängigen verantwortlichen Stelle. Unsere Prüfung ergab, dass bei einem Teil der Geräte die Bedienung innerhalb des App-Stores an den Betreiber übermittelt wurde – damit ist es für diesen möglich festzustellen, wann welche App geöffnet wurde. Da bei diesen Aufrufen i. d. R. immer auch eine eindeutige Gerätekennung (z. B. MAC-Adresse) enthalten ist, kann zumindest anhand der Datenbasis ein Nutzungsprofil des Smart-TV-Nutzers erstellt werden.

- **App-Anbieter**

  Einzelne Apps standen nicht im Fokus unserer Prüfung. Da sich Smart-TV-Apps vom Grundsatz nicht von Smartphone-Apps unterscheiden (allenfalls im Augenblick noch in den geringeren Möglichkeiten, auf personenbezogene Daten wie Kontakte oder Standort zuzugreifen), liegt es nahe, diese datenschutzrechtlich auch identisch zu bewerten (siehe Kapitel 3.4.6).

- **Betreiber von Personalisierungsdiensten** (z. B. beim elektronischen Programmführer)

  Neben den Übertragungen von technischen Grundfunktionen standen Personalisierungsdienste ganz besonders im Fokus der Prüfung. Dies sind zum Beispiel Programmempfehlungen anhand des bisher angesehenen Fernsehprogramms oder Werbeeinblendungen auf Basis von aufgenommenen Sendungen oder gestarteten Apps. Da bei den Datenflüssen zur Generierung von personalisierten Diensten meist eine eindeutige Geräte-ID (z. B. MAC-Adresse) festgestellt wurde und diese Geräte-ID auch bei einer Registrierung (zum Beispiel mit einer E-Mail-Adresse) übertragen wird, sehen wir bei den Personalisierungsdiensten des Smart-TV – vom Grundsatz her – einen Personenbezug als gegeben an.

Insgesamt betrachtet können wir festhalten, dass eine detaillierte Prüfung von Datenübertragungen bei Smart-TVs bei aktuellen Modellen meist äußerst schwierig ist, da viele Übertragungen mit dem HTTPS-Protokoll abgesichert sind. Auch ist die Implementierung innerhalb der Geräte mittlerweile so, dass mit Man-In-The-Middle-Techniken die HTTPS-Verbindungen in unseren Laboraufbauten nicht mehr zu Prüfzwecken umgangen werden konnten (bei älteren Modellen war uns dies zum Teil noch möglich). Aus Gründen der IT-Sicherheit ist dies sehr zu begrüßen, da es damit Unbefugten unmöglich bzw. sehr schwer gemacht wird, in die Datenübertragungen der Smart-TVs Einblick zu nehmen. Viele Hersteller setzen das HTTPS-Protokoll nach dem Stand der Technik ein (TLS1.2, Perfect Forward Secrecy, Zertifikat mit 2048-Bit).

Die sich gleichzeitig daraus ergebende mangelhafte technische Prüftransparenz ist jedoch der größte Kritikpunkt – zumindest aus technischer Sicht. Smart-TVs sind als abgeschottete Geräte konzipiert, die interessierten und technikaffinen Kunden, der Forschung, Verbraucherzentralen sowie den Datenschutzaufsichtsbehörden keine einfache Möglichkeit geben, eine vollständige Transparenz der Datenflüsse herzustellen. Dies wäre zum Beispiel wie bei Smartphones dadurch möglich, dass eigene, selbstsignierte X.509-Zertifikate in die Vertrauenskette des eigenen Smart-TVs hinzufügbar sind.

In unseren Prüfungen wurden die HTTPS-Verbindungen an Server, deren Auslösung wir im jeweiligen Testszenario nicht erwartet hatten, durch Wiederholungen soweit eingegrenzt, dass Indizien für datenschutzrechtlich relevante Übertragungen geschaffen wurden. So war bei einem Hersteller zum Beispiel bei Einstecken eines USB-Sticks mit Musik und

Videos eine verschlüsselte und „unknackbare" Datenübertragung an den Server des Herstellers festzustellen. Durch eine Bewertung des Übertragungsvolumens und einer Erhöhung sowohl der Anzahl der Medien auf dem USB-Stick als auch der Länge der Dateinamen konnte festgestellt werden, dass die Länge der Übertragung gleich blieb. Dies legte die Vermutung nahe, dass Bedieninformationen (z. B. USB-Stick eingesteckt) übertragen werden, nicht aber die Inhalte des Mediums. Durch die Befugnisse aus § 38 BDSG ist es den Datenschutzaufsichtsbehörden möglich, beim Hersteller die Testszenarien derart nachzustellen, dass ein Einblick in die Verschlüsselung innerhalb eines Testaufbaus genommen werden kann. Bei einem Besuch im Labor des Herstellers, dessen Smart-TV Datenübertragungen nach Einstecken des USB-Sticks gestartet hat, wurde – übrigens ohne aufsichtliche Maßnahme, die aufgrund der Unzuständigkeit des BayLDA aufgrund des Bundeslandsitzes gar nicht möglich gewesen wäre – festgestellt, dass die Vermutung richtig war, dass lediglich Benutzeraktionen (USB-Stick eingesteckt) an diesen übertragen werden und keine Medieninhalte.

Im Nachgang der technischen Prüfung werden die Ergebnisse als Basis für eine rechtliche Bewertung dienen, die im Frühjahr 2015 beginnen wird. Anhand dieser Bewertung können dann die Datenschutzaufsichtsbehörden in ihrem Zuständigkeitsbereich die Einhaltung der Gesetze überwachen.

22.12 Unwirksamer Widerspruch bei Webtracking-Verfahren

Beim Tracking-Opt-Out von Webseitenbesuchern muss die Übertragung von Nutzungsdaten auch tatsächlich unterlassen werden.

Verfahren zur statistischen Auswertung von Nutzerverhalten einer Webseite finden sich heutzutage bei fast allen Angeboten wieder – seien es Shops, Nachrichtenseiten, Kommunikationsdienste oder Spiele. Immer häufiger übersteigt die Anzahl der hierfür eingesetzten Werkzeuge ein überschaubares Maß – bei manchen Webseiten befinden sich bis zu dreißig Trackingtools oder gar mehr im Einsatz. Dadurch wird ermöglicht, jeden Klick (und sogar auch jeden Nicht-Klick) eines Webseitenbesuchers aufs Genaueste zu erfassen.

Nach § 15 Abs. 3 Satz 2 TMG muss dem Webseitenbesucher eine Widerspruchsmöglichkeit gegen dieses Tracking angeboten werden. Durch einen Klick auf einen entsprechenden Link soll das Tracking des eigenen Nutzungsverhaltens dauerhaft unterbunden werden.

Im Rahmen von Webseitenprüfungen auf Basis von § 38 BDSG stellten wir in letzter Zeit bei mehreren Diensten fest, dass nach Klicken eines Opt-Out-Links zwar ein sog. Opt-Out-Cookie auf dem Browser gesetzt wird, dieser aber die Übertragung der Nutzungsdaten an den Tracking-Anbieter gar nicht unterbindet. Stattdessen wird der Opt-Out als zusätzlicher HTTP-GET Parameter mit den bislang übermittelten Daten des Nutzers übertragen. Diese Form der Implementierung des Opt-Out erinnert an das „Do-Not-Track"-Flag, mit dem ein Webseitenbesucher dem Betreiber einer Webseite lediglich seinen Wunsch mitteilen kann, nicht getrackt zu werden. Es stellt sich folglich die Frage, warum Webseitenbetreiber Nutzungsdaten in dieser Form auch bei einem bewussten Opt-Out des Nutzers erheben, obwohl diese überhaupt nicht verwendet werden dürfen. Auch ist zu hinterfragen, inwieweit ein Widerspruch in diesen Fällen wirksam sein kann, wenn der Webseitenbesucher keine Kontrolle mehr über das eigene Opt-Out besitzt und nur noch auf die datenschutzfreundliche Interpretation des Begriffs Nutzungsprofilbildung beim jeweiligen Tracking-Anbieter hoffen kann.

Selbst wenn ein solcher Widerspruch dazu führt, dass ein Nutzungsprofil nicht mehr erstellt wird und das jeweilige Verfahren somit den Anforderungen an eine Widerspruchsmöglichkeit i. S. d. § 15 Abs.3 Satz 2 TMG entspricht, bedeutet dies jedoch zugleich, das weiterhin Nutzungsdaten i. S. d. § 15 Abs. 1 TMG an den Diensteanbieter fließen. Eine Rechtsgrundlage für die Erhebung (und ggf. Verwendung) dieser Nutzungsdaten ist nicht ersichtlich, da dies

weder für die Ermöglichung der Inanspruchnahme des Dienstes noch zu Abrechnungszwecken erforderlich ist.

22.13 Unwirksame Anonymisierung der „Custom Audiences" von Facebook

Unternehmen, die das Facebook Produkt "Custom Audiences" einsetzen, riskieren die Eröffnung eines Bußgeldverfahrens.

Aufgrund mehrerer Beratungsanfragen haben wir uns mit dem Produkt "Custom Audiences" von Facebook Inc. beschäftigt. Hierbei werden personenbezogene Datensätze, die als Identifikationskennungen eine E-Mail-Adresse oder eine Telefonnummer besitzen, von Unternehmen – vermeintlich anonymisiert – an Facebook weitergegeben. Facebook vergleicht die Hashwerte der übermittelten Daten mit eigenen Hashwerten, die im Rahmen der Facebook-Nutzung erhoben wurden. Bei einer Übereinstimmung gehört der jeweils übermittelte Datensatz folglich einem Facebook-Nutzer und kann – entsprechend der Nutzungsbedingungen – von Facebook weiterverarbeitet werden.

Als Algorithmus kommt das bekannte MD5-Verfahren zum Einsatz, das aufgrund seiner effizienten Berechnung (siehe Kapitel 22.4) für Anonymisierungsverfahren im Allgemeinen ungeeignet ist. Im vorliegenden Fall kann eine Brute-Force-Attacke deutlich beschleunigt werden, wenn ursprüngliche Klartext-Eigenschaften der MD5-gehashten Werte berücksichtigt werden. E-Mail-Adressen bestehen oftmals aus Vornamen, Nachname, Punkten und Zahlen und sind dabei aufgrund einer statistischen Verteilung häufig bei wenigen E-Mail-Providern zu finden. Diese Annahme zu Grunde gelegt, gehen wir bei einer – sehr vorsichtigen – Schätzung davon aus, dass mindestens 70% bis 80% aller Hashwerte, die aus E-Mail-Adressen bestehen, von handelsüblichen PCs ohne größeren Aufwand "zurückgerechnet" werden können.

Bei Telefonnummern muss aufgrund des kleinen Nummernraumes sogar davon ausgegangen werden, dass weit über 90% solcher Hashwerte in sehr kurzer Zeit zurückgerechnet werden können.

Facebook könnte somit ohne wesentlichen Aufwand einen Hashwert bei der überwiegenden Zahl der Fälle zurückrechnen, wodurch auch Nicht-Facebook-Nutzer betroffen sind. Es bedarf somit einer Einwilligung der Personen, deren Daten im Rahmen der "Custom Audiences" an Facebook übermittelt werden. Da diese im Allgemeinen nicht vorliegen dürfte, ist von der Nutzung dieses Dienstes abzuraten. Der Einsatz der „Custom Audiences" ohne Einwilligung der Nutzer stellt eine Ordnungswidrigkeit dar, die entsprechend mit Bußgeldern sanktioniert werden kann.

22.14 Phishing und Malware

Neue zielgerichtete Angriffe auf einzelne Nutzer erschweren die Erkennung von Datendiebstahl und Betrugsversuchen.

Im Rahmen von Datenschutzbeschwerden haben wir uns regelmäßig mit den Themen Phishing und Schadsoftware beschäftigt. Die aktuelle Feststellung von IT-Sicherheitsunternehmen, dass eine Verschiebung von allgemeinen Massen-Phishing-Attacken hin zu zielgerichteten Betrugsversuchen einzelner Nutzer stattfindet, sehen wir in unserer aufsichtlichen Praxis bestätigt. Diese sogenannten Spear-Phishing-Attacken beinhalten sehr persönliche Bestandteile und sollen einen Anwender durch den persönlichen Charakter der Anfrage (z. B. die eines „Freundes" in einem sozialen Netzwerk) dazu bringen, seine Daten in gefälschte Webseiten einzugeben oder einen E-Mail-Anhang zu öffnen, der wiederum mit Schadcode infiziert ist. Insider-Informationen zum potentiellen Opfer werden vorher gezielt und sorgfältig aus dessen sozialem Umfeld im Web recherchiert (aus Blogs, Webseiten, Arbeitgeber). Stammt eine Hinweisquelle oder ein Link in einer Email oder auf einer Webseite von einem vermeintlichen Bekannten, hinter-

fragen Nutzer deutlich seltener den Wahrheitsgehalt des angebotenen Inhalts.

Bei Malware sehen wir als besonders problematisch die Entwicklung der vergangenen Jahre an. Hierbei ist festzustellen, dass Antivirensoftware Schadcode zu häufig (noch) nicht erkennt bzw. erkennen kann und damit die schädlichen Trojaner, Viren oder Würmer auf einem Rechner des Nutzers installiert werden können. Diese Entwicklung wird sich zukünftig stark in den Anforderungen an die IT-Sicherheit nach § 9 BDSG widerspiegeln, indem mittlerweile davon ausgegangen werden muss, dass einzelne Arbeitsplatzrechner nicht andauernd gegen Schadcode geschützt werden können. Basierend auf dieser Annahme gewinnen technische und organisatorische Maßnahmen zur Schadensbegrenzung nach Infizierung eines Systems – auch in unserer aufsichtlichen Praxis – zunehmend an Bedeutung.

23

Bußgeldverfahren

23 Bußgeldverfahren

Wir haben im Berichtszeitraum 117 Bußgeldvorgänge abschließend bearbeitet. In 37 dieser Fälle haben wir Bußgeldbescheide erlassen und in zwei Fällen Verwarnungen ausgesprochen. Zu den genannten 117 Verfahren zählen wir – unabhängig davon, ob wir im konkreten Fall ein Bußgeldverfahren im rechtlichen Sinne „eingeleitet" haben – auch alle Vorgänge, die wir als Bußgeldbehörde im Wege von Aktenabgaben von den Staatsanwaltschaften erhalten haben, da wir auch in solchen Fällen stets eine Prüfung unter dem Gesichtspunkt vornehmen müssen, ob ein Bußgeldverfahren einzuleiten ist. Ferner zählen wir zu den 117 Verfahren alle Eingaben, die eindeutig als Ordnungswidrigkeitenanzeigen zu behandeln waren.

Es wurden sowohl Geldbußen gegen natürliche Personen als auch gegen juristische Personen oder Personenvereinigungen (meist Unternehmen) festgesetzt. Geldbußen gegen Unternehmen betrafen häufig Fälle, in denen es aufgrund mangelhafter innerbetrieblicher Organisation oder Aufsicht im Sinne von § 130 Abs. 1 OWiG bei der unternehmerischen Tätigkeit zu einem Verstoß (eines oder mehrerer Mitarbeiter) gegen bußgeldbewehrte datenschutzrechtliche Vorschriften gekommen war. Ist ein derartiger Mangel in der betrieblichen Organisation oder Aufsicht einer Person mit Leitungsverantwortung innerhalb des Unternehmens (im Sinne von Fahrlässigkeit) vorzuwerfen, so kann nach den Vorschriften des Ordnungswidrigkeitenrechts eine Geldbuße gegen das Unternehmen selbst festgesetzt werden, wovon wir in derartigen Fällen häufig Gebrauch machten.

Die den 37 verhängten Geldbußen zugrunde liegenden Sachverhalte können wie folgt skizziert werden:

- Nichtbeantwortung eines Auskunftsersuchens der Aufsichtsbehörde (drei Bußgeldbescheide)
- Unzulässige Übermittlung von Adressdaten in einer großen Zahl von Fällen
- Entsorgung von Patientendaten aus einer Arztpraxis im Hausmüll (zwei Bußgeldbescheide)
- Übermittlung von Gesundheitsdaten einer Kundin durch Mitarbeiterin einer sozialen Einrichtung zwecks Spenden-Einwerbung
- Keine datenschutzrechtliche Auskunftserteilung an Betroffenen (zwei Bußgeldbescheide)
- Ausspähung des PCs eines Mitarbeiters durch Arbeitgeber mittels Spezialsoftware
- Massen-E-Mail mit offenem Verteiler (zwei Bußgeldbescheide)
- Kundendaten (Bestelldaten) in einem Webshop einsehbar
- Unzulässiger Abruf von Kontobewegungsdaten durch Bankmitarbeiter zu privaten Zwecken (zwei Bußgeldbescheide)
- Versicherungsmitarbeiter erhebt Versichertendaten bei einem Arzt trotz fehlender Einwilligung des Versicherten
- Stellenbewerbungen auf Unternehmenshomepage im offenen Internet abrufbar
- Unzulässige Datenverarbeitungen im Zusammenhang mit der Tätigkeit von Apothekenrechenzentren (drei Bußgeldbescheide)
- Ausspähung von Fahrtrouten durch Anbringung eines GPS-Peilsenders an Kraftfahrzeug (zwei Bußgeldbescheide)
- Immobilienmakler erhebt bei Gelegenheit einer Vermittlung unzulässig Daten von (nicht am konkreten Fall beteiligten) anderen Wohnungseigentümern
- Erschleichen von Daten (Chat-Inhalten) aus einem Smartphone durch Täuschung
- Betreiben einer Wildbeobachtungskamera ohne plausible Begründung mit Blick auf einen Waldweg

- Bonitätsabfrage ohne berechtigtes Interesse
- Erschleichen von Daten eines Kfz-Halters durch Veranlassung einer polizeiseitigen Kfz-Halterabfrage
- Mehrfache Werbung trotz Werbewiderspruchs (drei Bußgeldbescheide)
- Laufendes Filmen des Straßenverkehrs zu Beweissicherungszwecken mit einer Dashboard-Kamera im Kraftfahrzeug
- Versicherungsvermittler informiert unbefugt einen Dritten über die Vertragskündigung eines Versicherten
- Übermittlung ungekürzter IP-Adressen mittels „Google Analytics“, z. T. auch fehlende Einräumung eines Widerspruchsrechts gegen die Erstellung pseudonymer Nutzungsprofile durch „Google Analytics“ entgegen § 15 Abs. 3 S. 2 TMG (drei Bußgeldbescheide)
- Zuleitung einer ausgefüllten Mieterselbstauskunft durch den Vermieter an den Arbeitgeber des Mieters zur Verifizierung der Eigenangabe des Mieters (unzulässig, weil Mietverhältnis schon lief und Mieter den Mietzins laufend bezahlte)
- unterlassene Unterrichtung über das Werbewiderspruchsrecht entgegen § 28 Abs. 4 S. 2 BDSG

Wie aus dieser Zusammenstellung erkennbar ist, betrafen die Bußgeldbescheide eine breite Vielfalt von Lebenssachverhalten und sehr unterschiedliche Datenschutzverstöße. Hervorgehoben seien dennoch die drei Unternehmen, gegenüber denen wir die Verwendung des Webanalysetools Google Analytics auf Webseiten mit Geldbuße geahndet haben, weil die Unternehmen das Tool ohne eine sog. Anonymisierungsfunktion verwendet hatten, was zu Übermittlungen ungekürzter IP-Adressen der Websitebesucher an Google Inc. in die USA ohne Rechtsgrundlage führte. In zwei dieser Fälle hatten die Unternehmen zudem den Nutzern entgegen den Anforderungen des Telemediengesetzes keine Möglichkeit eingeräumt, der Erstellung anonymisierter Nutzungsprofile – eine solche findet beim Einsatz von Google Analytics statt – zu widersprechen, etwa indem ein Link zu einem Browser-Zusatzprogramm gesetzt wird, mittels dessen der Nutzer Google Analytics deaktivieren kann.

Hervorgehoben sei auch ein Bußgeldbescheid, den wir gegen einen Fahrzeugführer erlassen haben, der in seinem Fahrzeug eine sog. Dashboard Kamera installiert hatte, mit der er laufend den Straßenverkehr filmte. Dass derartige Aufnahmen unter datenschutzrechtlichen Gesichtspunkten in bestimmten Fällen unzulässig sind, wird unter Kapitel 19.1 dieses Berichts näher erläutert. Die Anfertigung der Aufnahmen stellte in den dort beschriebenen Fällen aus unserer Sicht eine unbefugte Erhebung und Verarbeitung personenbezogener Daten dar und erfüllte damit Tatbestände von Ordnungswidrigkeiten nach § 43 Abs. 2 Nr. 1 BDSG. Wir haben im Berichtszeitraum daher in einem ersten derartigen Fall einen – inzwischen bestandskräftigen – Bußgeldbescheid erlassen und in einer Reihe vergleichbarer Fälle ebenfalls Bußgeldverfahren eröffnet, die jedoch noch nicht abgeschlossen sind.

In drei Fällen setzten wir Geldbußen gegen Unternehmen wegen wiederholter Werbung trotz Werbewiderspruchs fest. In einem dieser Fälle hatte ein Unternehmen bei einer E-Mail-Werbeaktion Werbewidersprüche Betroffener missachtet. Ursache war, wie sich zeigte, ein Fehler im Rahmen von in Vorfeld stattgefundenen Programmierarbeiten hinsichtlich der verwendeten Datenbank, in denen die E-Mail-Adressen von Kunden gespeichert waren. Das Unternehmen hatte es versäumt, nach den Programmierarbeiten durch hinreichende Testläufe zu überprüfen, ob Werbewidersprüche noch ordnungsgemäß erkannt und die Betroffenen somit von E-Mail-Werbesendungen zuverlässig aussortiert werden. Derartige Testläufe im Anschluss an Programmierarbeiten sind jedoch zwingend erforderlich, da Programmierfehler letztlich nie gänzlich auszuschließen sind, so dass es eines Kontrollprozesses bedarf, um Rechtsverstöße als Auswirkungen derartiger Fehler zu verhindern. Es gehörte daher in dem von uns behandelten Fall zur Aufsichtspflicht des Betriebsinhabers im Sinne von § 130 Abs. 1 OWiG, sicherzustellen, dass

geeignete Testläufe stattfinden; die Verantwortung hierfür musste daher in dem Unternehmen jedenfalls auf Leitungsebene wahrgenommen werden, wobei eine Delegation dieser Aufgabe selbstverständlich möglich ist. Da das Unternehmen im konkreten Fall indessen keinerlei diesbezügliche Vorkehrungen nachweisen konnte, sind wir von einem Verstoß gegen die betriebliche Aufsichtspflicht (§ 130 Abs. 1 OWiG) durch eine Leitungsperson des Unternehmens ausgegangen und haben eine Geldbuße gegen das Unternehmen als solches verhängt.

Wie bereits angedeutet, erreichte uns ein nicht unerheblicher Teil der Fälle, über die wir in unserer Eigenschaft als Bußgeldbehörde zu entscheiden hatten, im Wege von Aktenabgaben durch Staatsanwaltschaften. Stellt die Staatsanwaltschaft ein von ihr geführtes strafrechtliches Ermittlungsverfahren ein, hält sie es jedoch für denkbar, dass der Sachverhalt eine datenschutzrechtliche Ordnungswidrigkeit nach § 43 BDSG oder § 16 Abs. 2 Nr. 2 bis 5 TMG darstellt, so gibt sie die Akte an die zuständige Bußgeldbehörde ab. Liegt in einem solchen Fall nach unserer Bewertung ein Anfangsverdacht auf eine Ordnungswidrigkeit vor und erscheint die Notwendigkeit einer Ahndung mit Geldbuße jedenfalls nicht von vornherein ausgeschlossen, so wird von uns ein Bußgeldverfahren eröffnet. Die erhebliche Anzahl an Akten, die wir auf diese Weise von Staatsanwaltschaften zur Bearbeitung erhalten haben, belegt, dass datenschutzrechtliche Verstöße auch bei den Staatsanwaltschaften mehr und mehr im Blickfeld stehen.

Neben Sachverhalten, die uns von den Staatsanwaltschaften vorgelegt wurden, haben wir auch in Fällen, die wir zunächst selbst in unserer Eigenschaft als Datenschutzaufsichtsbehörde bearbeitet haben, Bußgeldverfahren eröffnet, sofern sich ein Anfangsverdacht auf einen Verstoß gegen eine bußgeldbewehrte Vorschrift ergab und die Verfolgung und Ahndung mit Geldbuße im jeweiligen Fall überwiegend angezeigt erschien.

Schließlich gab es auch Fälle, in denen Personen direkt uns gegenüber erklärten, eine „Ordnungswidrigkeitenanzeige“ wegen eines bestimmten Sachverhalts erstatten zu wollen. In derartigen Fällen war und ist es stets notwendig, zunächst auszulegen, was das Ziel der betreffenden „Anzeige“ bzw. Eingabe ist. Häufig war bei verständiger Würdigung und Auslegung letztlich erkennbar, dass Ziel des „Anzeigeerstatters“ nicht eigentlich die Ahndung eines behaupteten Verstoßes war, sondern es ihm vielmehr um die Beseitigung eines Zustandes ging, bei dem er sich in seinen datenschutzrechtlichen Positionen verletzt sah. In solchen Fällen haben wir die „Anzeige“ daher als Eingabe an die Datenschutzaufsichtsbehörde interpretiert und sie als solche behandelt; dies machten wir den Anzeigeerstattern in den entsprechenden Fällen transparent. Neben solchen Fällen gab es auch Eingaben, die – auch nach verständiger Würdigung – sowohl auf eine Ahndung als auch auf ein datenschutzaufsichtliches Einschreiten gerichtet waren; solche Eingaben mussten wir dementsprechend sowohl im Rahmen unserer Zuständigkeit als Bußgeldbehörde als auch im Rahmen unserer Aufgaben als Datenschutzaufsichtsbehörde behandeln. Wie bereits in unserem Tätigkeitsbericht 2011/2012 betont, nehmen wir stets eine strikte verfahrens- und aktenmäßige Trennung zwischen datenschutzaufsichtlichem Verfahren und Bußgeldverfahren vor, da für die beiden Verfahrensarten unterschiedliches Verfahrensrecht gilt mit der Folge, dass für die Behörde unterschiedliche Befugnisse und für die Verfahrensbeteiligten unterschiedliche Rechte bestehen.

Von den 37 ergangenen Bußgeldbescheiden wurden 30 ohne Einlegung eines Rechtsmittels bestandskräftig. In einem Fall haben wir aufgrund Einspruchs des Betroffenen und nachgeschobener Begründung den Bußgeldbescheid aufgehoben, in einem anderen Fall die Geldbuße mit Blick auf die nachgeschobene Mitteilung des Betroffenen über seine wirtschaftlichen Verhältnisse reduziert. In vier Fällen wurde die verhängte Geldbuße nach eingelegtem Einspruch durch das Amtsgericht reduziert. Das bedeutet andererseits aber auch, dass die Gerichte auch in diesen vier Fällen die Geldbußen jedenfalls dem Grunde nach (wenn auch nicht in voller Höhe) bestätigt haben. In zwei dieser vier Fälle erfolgte die Reduzierung der Geldbuße durch das Gericht im Übrigen allein wegen

der wirtschaftlichen Verhältnisse der Betroffenen, die uns die Betroffenen vorher nicht mitgeteilt hatten, so dass sie von uns hatten geschätzt werden müssen. Dass es in solchen Fällen zur Reduzierung der Geldbuße durch die Amtsgerichte kommen kann, liegt in der Natur der Sache: Die Höhe der Geldbuße richtet sich gemäß dem Gesetz – neben Bedeutung des Verstoßes sowie Tatvorwurf – auch nach den wirtschaftlichen Verhältnissen des Betroffenen. Als Bußgeldbehörde können wir die tatsächlichen wirtschaftlichen Verhältnisse des Bußgeldadressaten nur berücksichtigen, wenn dieser sie uns mitteilt. Da diese Mitteilung freiwillig ist, machen einige Betroffene hierzu im Rahmen der Anhörung keine Angaben. In solchen Fällen müssen wir die wirtschaftlichen Verhältnisse schätzen. Teilt der Betroffene dann erstmalig im gerichtlichen Verfahren seine wirtschaftlichen Verhältnisse mit, muss das Gericht auf dieser Grundlage die Höhe der Geldbuße ggf. anpassen.

Im Berichtszeitraum haben wir in 76 Fällen, mit denen wir als Bußgeldbehörde befasst waren, kein Bußgeld- oder Verwarnungsverfahren eingeleitet oder aber das Bußgeldverfahren eingestellt. Dazu gehören auch einige Vorgänge, die uns als Aktenabgaben durch die Staatsanwaltschaften zugeleitet wurden. Die Gründe für die Einstellung bzw. die Nichteinleitung von Bußgeldverfahren waren vielfältig. In einer Reihe von Fällen zeigte sich, dass der der Anzeige zugrunde liegende Sachverhalt keine (unserer Zuständigkeit unterfallenden) Bußgeldtatbestände erfüllte. Als Beispiel sei eine Anzeige erwähnt, bei der der Anzeigeerstatter monierte, dass eine Auskunftei anlässlich einer von ihm dort eingeholten datenschutzrechtlichen Auskunft einen Scorewert zu seiner Person gebildet hatte. Hierin sah der Anzeigeerstatter eine anlasslose und unberechtigte Scorewert-Bildung. Unsere Prüfung ergab jedoch, dass das Verhalten der Auskunftei keinen datenschutzrechtlichen Verstoß darstellte. Auskunfteien sind gemäß § 34 Abs. 4 Satz 1 Nr. 2 BDSG verpflichtet, einem Betroffenen im Falle eines Auskunftsersuchens Auskunft zu erteilen gerade auch über die Wahrscheinlichkeitswerte, die sich zum Zeitpunkt des Auskunftsverlangens nach dem von der Auskunftei angewandten Verfahren für den jeweiligen Betroffenen ergeben. Die Auskunftei hatte sich daher rechtmäßig verhalten.

Daneben gab es auch eine Reihe von Fällen, in denen wir unter Ausübung pflichtgemäßen Ermessens (§ 47 Abs. 1 OWiG) von der Einleitung eines Bußgeldverfahrens abgesehen oder eingeleitete Bußgeldverfahren eingestellt haben, insbesondere weil es sich um vergleichsweise geringfügige Verstöße handelte und die Ahndung mit einer Geldbuße im konkreten Fall nicht überwiegend angezeigt war. Als Beispiel seien einige Ordnungswidrigkeitenanzeigen im Zusammenhang mit Videoüberwachungskameras genannt, die zur Überwachung von Häusern verwendet wurden, wobei jedoch das Kamerablickfeld so eingestellt war, dass davon in einem übermäßigen Umfang auch öffentlicher Gehweg und/oder Straßenbereich erfasst war. In derartigen Fällen war eine Ahndung mit Geldbuße meist nicht angezeigt. Vielmehr erweist es sich hier regelmäßig als zielführender, mit den Mitteln der Datenschutzaufsichtsbehörde dem Kamerabetreiber die datenschutzrechtlichen Anforderungen an eine Videoüberwachung nachdrücklich zu erläutern und für die Herstellung rechtmäßiger Zustände zu sorgen, was regelmäßig gelingt.

Stichwortverzeichnis