Bayerisches Landesamt für
Datenschutzaufsicht

7. Tätigkeitsbericht

2015/2016

7. Tätigkeitsbericht

des Bayerischen Landesamtes
für Datenschutzaufsicht
für die Jahre
2015 und 2016

Vorwort

Der Berichtszeitraum für diesen Tätigkeitsbericht, die Jahre 2015 und 2016, war datenschutzrechtlich besonders geprägt durch das spannende Trilog-Verfahren und das In-Kraft-Treten der Datenschutz-Grundverordnung (DS-GVO) im Mai 2016. Damit hat nicht nur die zweijährige Umsetzungsphase begonnen, sondern auch eine Zeit der gezielten Auseinandersetzung. Wir versuchen zu verstehen, was uns die DS-GVO im Detail sagen will. In der Praxis stellen wir mittlerweile fest, dass sich datenschutzrechtliche Veranstaltungen und Veröffentlichungen – und zunehmend auch Beratungsanfragen in unserem Haus – ausschließlich auf die Anwendbarkeit der DS-GVO beziehen. Wir haben großes Verständnis dafür, dass verantwortliche Stellen oder Verantwortliche, wie sie bald heißen werden, sich darauf einstellen wollen, was in Zukunft gilt – nicht nur, weil der Sanktionsdruck und auch der Sanktionsrahmen mit Bußgeldern von bis zu 20 Millionen dazu „motivieren", solange dabei nicht vergessen wird, die aktuellen gesetzlichen Vorgaben einzuhalten.

Uns ist bewusst, dass die Datenschutz-Grundverordnung nicht nur für die Verantwortlichen und Auftragsverarbeiter, sondern auch für uns Datenschutzaufsichtsbehörden gewaltige Herausforderungen mit sich bringen wird. Neben einer großen Erweiterung des Aufgabenkatalogs für Aufsichtsbehörden, verbunden mit einer ebenso deutlichen Erweiterung des Befugnisrahmens bei Sanktionen in der o. g. Höhe, dürfte die Zusammenarbeit mit den anderen Aufsichtsbehörden und dem Europäischen Datenschutzausschuss eine erhebliche Mehrarbeit bringen – zumal diese Arbeit ganz überwiegend in englischer Sprache erfolgen wird.

Wir haben in Bayern unter den mehr als 700.000 Unternehmen, Vereinen, Verbänden, freiberuflich Tätigen usw., für die wir als Datenschutzaufsichtsbehörde zuständig sind, auch zahlreiche Global Player, für die wir dann als federführende Aufsichtsbehörde in Europa zuständig sein werden.

Der bayerische Haushaltsgesetzgeber hat im Doppelhaushalt für die Jahre 2017 und 2018 vier neue Stellen (und damit die Hälfte, die wir beantragt haben) für uns ausgewiesen. Diese Entscheidung des Bayerischen Landtags hat zum Teil das umgesetzt, was wir seit Jahren zur Bewältigung der bestehenden Aufgaben nach den derzeit geltenden Vorschriften gefordert hatten. Mit an Sicherheit grenzender Wahrscheinlichkeit werden die neuen Stellen, für die wir dennoch dankbar sind, nicht ausreichen, um die anstehenden Aufgaben angemessen erfüllen zu können. Es lässt sich schon heute feststellen, dass wir die Aufgaben der umfassenden Kontrolle, der wirksamen, verhältnismäßigen und abschreckenden Sanktionierung fast aller Datenschutzverstöße, der Kooperation mit den europäischen Datenschutzbehörden und insbesondere der effektiven Beratung und Hilfestellung bei bayerischen Unternehmen in rechtlicher und technischer Hinsicht mit den vorhandenen Ressourcen nicht werden leisten können. Es wird sich zeigen, an welchen Stellen wir Abstriche bei der Erfüllung unserer gesetzlichen Pflichtaufgaben machen müssen.

Dass wir mit unserer Arbeit zunehmend wahrgenommen werden, zeigt sich durch den drastischen Anstieg von Beschwerden und Beratungsanfragen, die in den letzten beiden Jahren auf uns zugekommen sind. Die Steigerung der Beschwerden von 1.878 in den Vorjahren 2013 und 2014 auf insgesamt 2.527 in den aktuellen Berichtszeiträumen 2015 und 2016 mag ihre Ursache in einem wachsenden Datenschutzbewusstsein der Bürger haben – vielleicht auch, weil immer mehr Bürger selbst Opfer von Datenmissbrauch geworden sind und ihnen dadurch bewusst wird, wie schwer bis unmöglich es heute ist, selbst darüber zu bestimmen, wer was über sie weiß.

Die Steigerung der Beratungsanfragen von 3.554 in den Jahren 2013 und 2014 auf 3.853 in den Jahren 2015 und 2016, verbunden mit der Feststellung, dass zahlreiche Unternehmen uns wiederholt um Beratung bitten, zeigt uns ein starkes Bedürfnis vieler verantwortlicher Stellen, sich datenschutzkonform zu verhalten, aber auch, dass die Art und Weise, wie wir beraten, so schlecht nicht sein kann. Leider mussten wir gerade im letzten Jahr einige Beratungsanfragen ablehnen und andere so in die Länge ziehen, dass es für alle Beteiligten schlicht unzumutbar war. Wie wir die Entwicklung der seit Jahren steigenden Beratungsanfragen, die wir nach Wirksamwerden der DS-GVO teilweise dann innerhalb von acht Wochen mit einer schriftlichen Stellungnahme beantworten müssen, in den Griff bekommen sollen, wissen wir noch nicht.

Auch beschäftigen uns verstärkt die Sicherheitsrisiken der vernetzten Systeme. Die täglich stattfindenden Cybercrime-Angriffe stellen eine große Gefahr für uns alle dar. Viele der Attacken, bei denen Daten geklaut werden, verursachen eine Informationspflicht auch uns gegenüber. Dass aber die Meldung von solchen Datenpannen bei uns von 53 in den Vorjahren 2013 und 2014 auf nunmehr 113 in den Jahren 2015 und 2016 – und davon 85 alleine im Jahr 2016 – gestiegen sind, hat uns doch überrascht. Wir gehen jedoch davon aus, dass diese Zahl nur die Spitze eines großen Eisberges ist, der im Verborgenen ruht – die Dunkelziffer der nicht gemeldeten Fälle dürfte um ein Vielfaches höher sein.

Dies ist unser letzter Tätigkeitsbericht, der sich im Wesentlichen mit der Anwendung der Vorschriften des Bundesdatenschutz- und Telemediengesetzes befasst. Um den Blick in die Zukunft nicht völlig auszublenden, haben wir an einigen Stellen eine Prognose gewagt, wie die dort genannten Sachverhalte – vorbehaltlich entsprechender orientierenden Leitlinien des Europäischen Datenschutzausschusses unter Heranziehung der DS-GVO – zu lösen sein könnten. Dies mag eine Schnittstelle zu den folgenden Tätigkeitsberichten sein, die dann nach der DS-GVO jährlich zu veröffentlichen sein werden.

Ich selbst bin im August 2016 in meinem Amt als Präsident des Bayerischen Landesamtes für Datenschutzaufsicht bestätigt worden. Nun konnte ich nicht mehr sagen, wie noch nach der Ernennung im Jahr 2011, ich wusste nicht, worauf ich mich einlasse. Die rasante technologische Entwicklung, die Digitalisierung von allem „was nicht bei drei auf den Bäumen ist", ein steigendes Datenschutzbewusstsein, aber auch ein sehr nachlässiger Umgang mit den eigenen Daten durch viele Bürger, das alles in einer Situation, in der das neue Recht vor der Türe steht und man nur ahnen kann, wie es sich anfühlen wird, wenn es wirksam wird, macht das Aufgabengebiet des Präsidenten des Bayerischen Landesamtes für Datenschutzaufsicht so spannend wie wohl kaum ein anderes im öffentlichen Dienst in Bayern. Eine Chance für mich, in dieser letzten Amtsperiode meine berufliche Laufbahn ausklingen zu lassen, ergibt sich dadurch nicht. Und das ist gut so!

Die Tätigkeiten, über die in diesem Bericht geschrieben wird, habe nicht ich, sondern haben wir geleistet. Deshalb erlaube ich mir an dieser Stelle ein herzliches Dankeschön an alle meine Mitarbeiterinnen und Mitarbeiter für die geleistete Arbeit in den vergangenen beiden Jahren. Ich entschuldige mich für gelegentlich grenzwertige Anforderungen, vor die ich sie gestellt oder vor denen ich sie nicht bewahrt habe. Ich gelobe insoweit Besserung. Wie ich das in Bezug auf die obigen Ausführungen aber umsetzen kann, daran arbeite ich noch.

Ansbach, im März 2017

Thomas Kranig
Präsident

Inhaltsverzeichnis

1

Datenschutzaufsicht im nicht-öffentlichen Bereich

1 Datenschutzaufsicht im nicht-öffentlichen Bereich

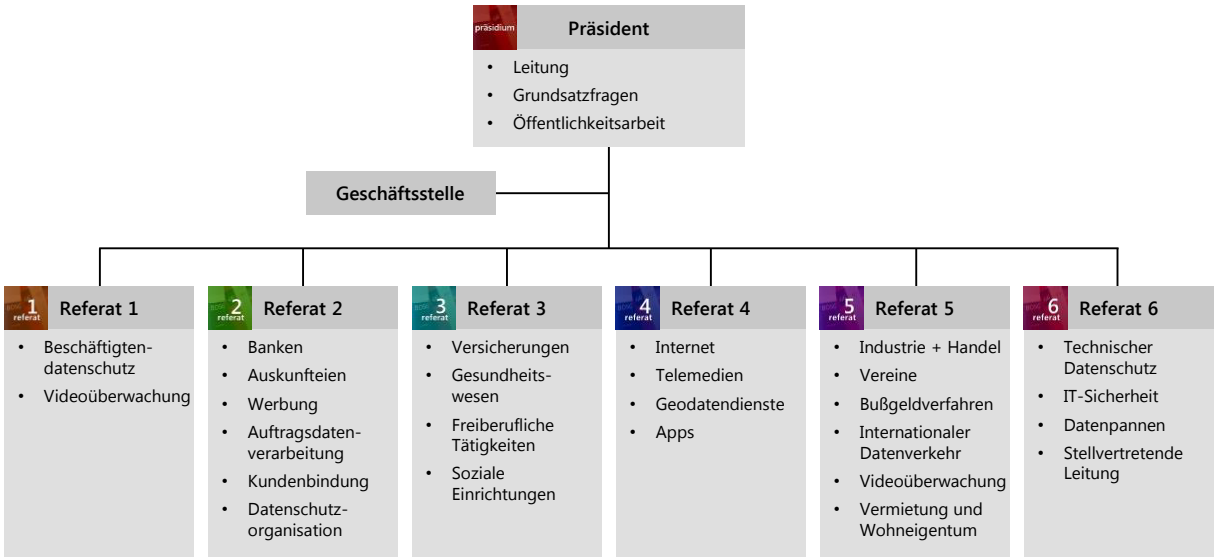
1.1 Die bayerische Datenschutzaufsichtsbehörde

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

Stellenmehrungen haben sich im Berichtszeitraum trotz wachsender Fallzahlen nicht ergeben. Nach wie vor hatten wir 16 Planstellen, die von 17 Mitarbeitern besetzt wurden.

1.2 Gesetzliche Grundlage für die Erstellung des Tätigkeitsberichts

Gemäß § 38 Abs. 1 Satz 7 des Bundesdatenschutzgesetzes (BDSG) haben wir als Datenschutzaufsichtsbehörde regelmäßig, spätestens alle zwei Jahre, einen Tätigkeitsbericht zu veröffentlichen. Der letzte Tätigkeitsbericht für die Jahre 2013 und 2014 wurde der Öffentlichkeit am 23. März 2015 vorgestellt. Hiermit kommen wir unserer Verpflichtung nach, im festen Turnus diesen Bericht zu publizieren. Nach der in Zukunft maßgeblichen Rechtsgrundlage (Art. 59 DS-GVO) werden wir dann wohl jährlich einen Tätigkeitsbericht der Öffentlichkeit zugänglich machen.



2

Allgemeiner Überblick über die Tätigkeit des BayLDA

2 Allgemeiner Überblick über die Tätigkeit des BayLDA

2.1 Statistik

Zunächst möchten wir über die grundsätzliche Entwicklung unserer zu behandelnden Vorgänge informieren und einen ersten Überblick geben, bevor in den nachfolgenden Unterkapiteln detailliert über die jeweilige Art von Vorgängen unterrichtet wird.

Bei Erfassung der Beschwerden und Beratungen wird für die Statistik kein Unterschied gemacht, ob diese uns per E-Mail (der meist genutzte Kommunikationsweg), per Telefon, über die Homepage oder per Post erreicht haben. Eingänge von Bürgern werden danach unterschieden, ob sie sich für uns erkennbar gegen verantwortliche Stellen richten (Beschwerden) oder auf Fragen im Umgang mit personenbezogenen Daten richten (Beratungen). Gelegentlich wird bei als Beratung erfassten Vorgängen erst im Laufe der Bearbeitung klar, dass tatsächlich eine Beschwerde dem Sachverhalt zu Grunde liegt. In diesen Fällen erfolgt eine Änderung des Vorgangs in eine Beschwerde. Bei Beschwerdevorgängen wird vor der Bewertung durch uns eine Stellungnahme der verantwortlichen Stelle eingeholt.

In die u. g. Statistik fließen die Fälle ein, die im jeweiligen Zeitraum erledigt wurden. Um ein Gefühl dafür zu gewinnen, wie lange die Bearbeitungszeiten dabei waren, haben wir in einer weiteren Grafik dargestellt, wie viele Tage wir durchschnittlich für die Abarbeitung von jeweils 25% der Beratungen und Beschwerden benötigt haben.

Dauer	25%	25%	25%	25%
Beschwerden	4 Tage	14 Tage	52 Tage	141 Tage
Beratungen Bürger	1 Tag	3 Tage	11 Tage	36 Tage
Beratungen Unternehmen	3 Tage	19 Tage	47 Tage	122 Tage

Eines unserer großen Ziele ist nach wie vor, darüber zu informieren, wie verantwortliche Stellen und Bürger sich gesetzeskonform verhalten können. Dies ist unserem Empfinden nach gerade beim Umgang mit Datenpannen, d. h. Sicherheitsvorfällen, nötig. Hier konnten wir vor allem im Jahr 2016 einen gewaltigen Anstieg an eingehenden Meldungen verzeichnen. Es ist absehbar, dass in diesem Bereich der Arbeitsaufwand weiterhin deutlich zunehmen wird, da die Schwelle für die Meldepflicht von „Datenpannen" nach der DS-GVO, d. h. Meldungen von Verletzungen der Datensicherheit, deutlich herabgesetzt wurde.

Der weiterhin spürbare Trend, dass verantwortliche Stellen und Bürger auf uns zukommen, betrachten wir als durchaus positiv, stellen aber auch fest, dass das zu einer grenzwertigen Belastung der Mitarbeiter führt, die wohl nur durch entsprechende Personalaufstockung und Zurückfahren der Beratungsleistung in den Griff zu bekommen sein wird.

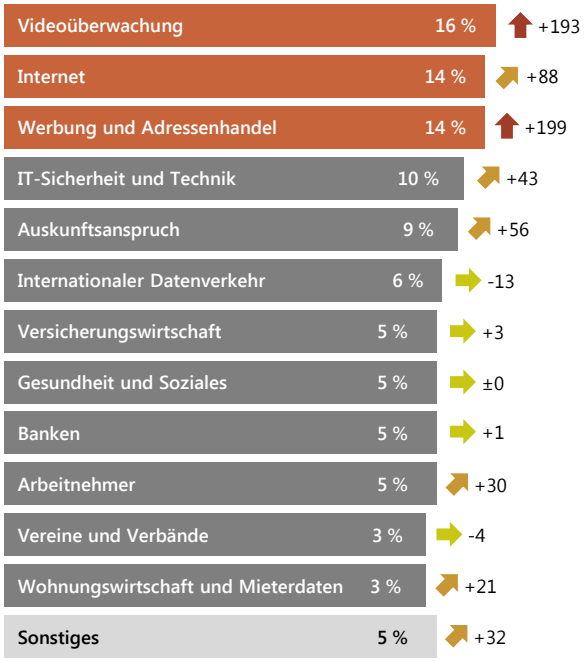
	2013	2014	2015	2016	Tendenz
Beschwerden	925	953	1103	1424	
Beratungen Bürger	799	991	877	1065	
Beratungen Unternehmen	1733	1821	1850	2003	
Bußgeldverfahren	53	64	94	79	
Datenpannen	32	21	28	85	

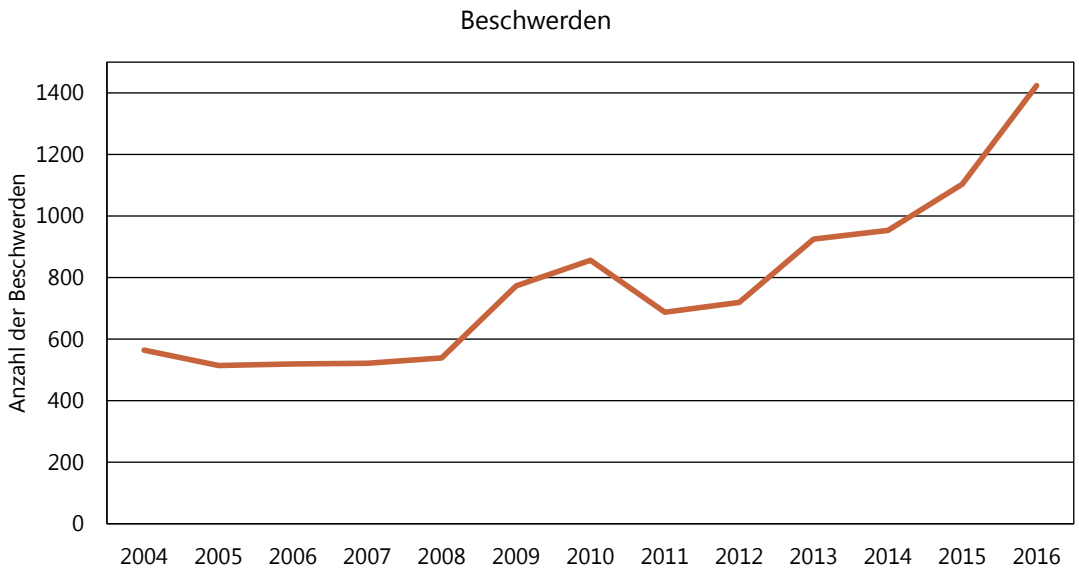
2.1.1 Beschwerden

Die Zahl der bei uns eingegangenen Beschwerden steigt permanent. Während wir im Jahr 2011 einen kleineren „Tiefpunkt" von 687 Beschwerden im Jahr hatten, waren es zuletzt im Jahr 2016 insgesamt 1424 Beschwerden. Grund für die Steigerung ist unseres Erachtens nicht nur eine gesteigerte Sensibilität der Bürger, sondern vor allem, dass wir als Anlaufstelle für Datenschutzbeschwerden bekannter geworden sind und seit Februar 2016 auch die Möglichkeit einer Online-Beschwerde anbieten. Bürger können uns ohne großen Aufwand auf eine sichere Art und Weise, d. h. auch inhaltsverschlüsselt, ihr Beschwerdeanliegen zukommen lassen. Durch diese strukturierte Eingabe ist den Bürgern eher klar, welche Informationen wir zur Bearbeitung benötigen, wodurch wir uns in vielen Fällen Rückfragen zum Beschwerdesachverhalt ersparen.

Im Zeitraum vom 11. Februar bis zum 31. Dezember 2016 haben wir alleine 375 Datenschutzbeschwerden über unser Online-Formular erhalten. Soweit sich Betroffene bei uns beschweren, weil sie indirekt Opfer einer Hacking-Attacke wurden (da sie einen Nutzer-Account auf einer unsicheren Webseite hatten, auf welcher Nutzerdaten gestohlen wurden), versuchten wir, sowohl den Betroffenen direkt zu helfen oder Maßnahmen zur Schadensminimierung anzubieten als auch im Rahmen der Datenpannenbearbeitung die verantwortliche Stelle bei der Behebung der Sicherheitsvorfälle zu unterstützen.

Die prozentuale Zuordnung der Beschwerdethemen wird nachfolgend dargestellt. Dahinter befindet sich ein Hinweis auf die jeweilige absolute Änderung der Beschwerdeanzahl im Vergleich zu den Vorjahren (z. B. 88 Beschwerden mehr im Bereich „Internet").





2.1.2 Beratung der Bürger und Betroffenen

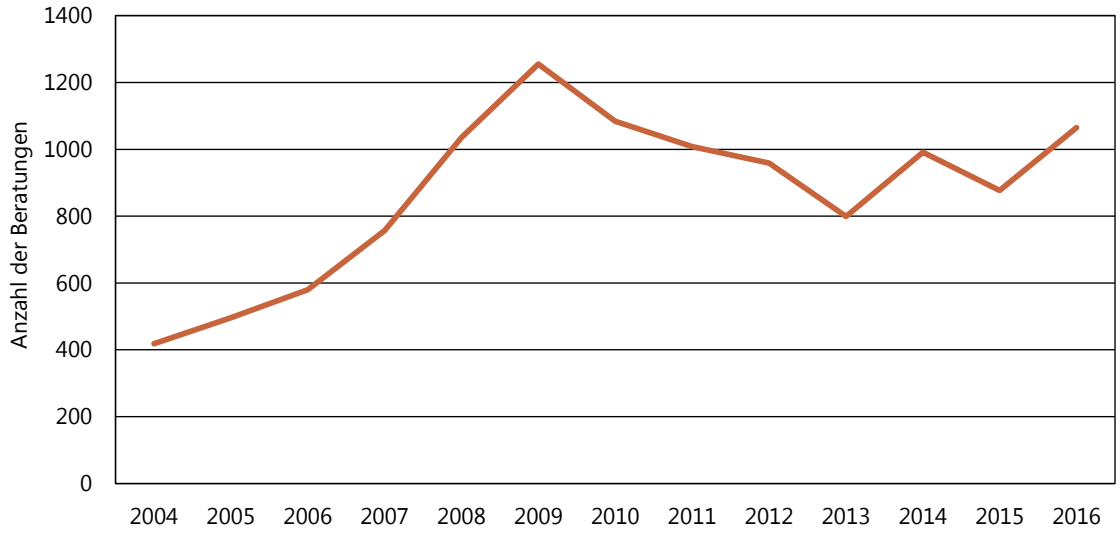
Die Beratung der Bürger und Betroffenen ist nach den derzeit geltenden Vorschriften des BDSG keine Pflichtaufgabe der Datenschutzaufsichtsbehörde. Dennoch haben wir es als eine unserer Aufgaben angesehen, entsprechende Anfragen entgegenzunehmen und – soweit zumutbar – zu bearbeiten.

Wenn man sich die Entwicklung dieser Beratungsanfragen über die letzten 12 Jahre ansieht, lässt sich feststellen, dass zu Beginn der unten dargestellten statistischen Aufzeichnungen das Interesse und das Bedürfnis nach unmittelbarer Beratung durch die Aufsichtsbehörde permanent gestiegen sind. Ab dem Jahr 2009 sind die Anfragen zurückgegangen und haben sich nun auf einer – immer noch sehr hohen – Zahl von etwa 1000 pro Jahr eingependelt.

Wir sehen den leichten Rückgang der Beratungsanfragen seit 2009 insbesondere darin begründet, dass wir unser Informationsangebot auf der Homepage permanent erweitert haben und auch künftig noch weiter ausbauen werden. Wir gehen deshalb davon aus, dass sich viele Beratungsfragen der Bürger dadurch erledigen, dass sie auf – für uns standardmäßige – Fragen auf unserer Homepage die gewünschte Antwort finden.

In Zukunft wird die Beratung der Bürger jedoch auch zu einer Pflichtaufgabe der Datenschutzaufsichtsbehörden. Nach Art. 58 Abs. 1 e) DS-GVO haben die Aufsichtsbehörden „auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund der Verordnung zur Verfügung zu stellen“. Wir sehen uns hierfür – abgesehen vom mangelnden Personal – gut gewappnet.

Beratungen von Bürgern und Betroffenen



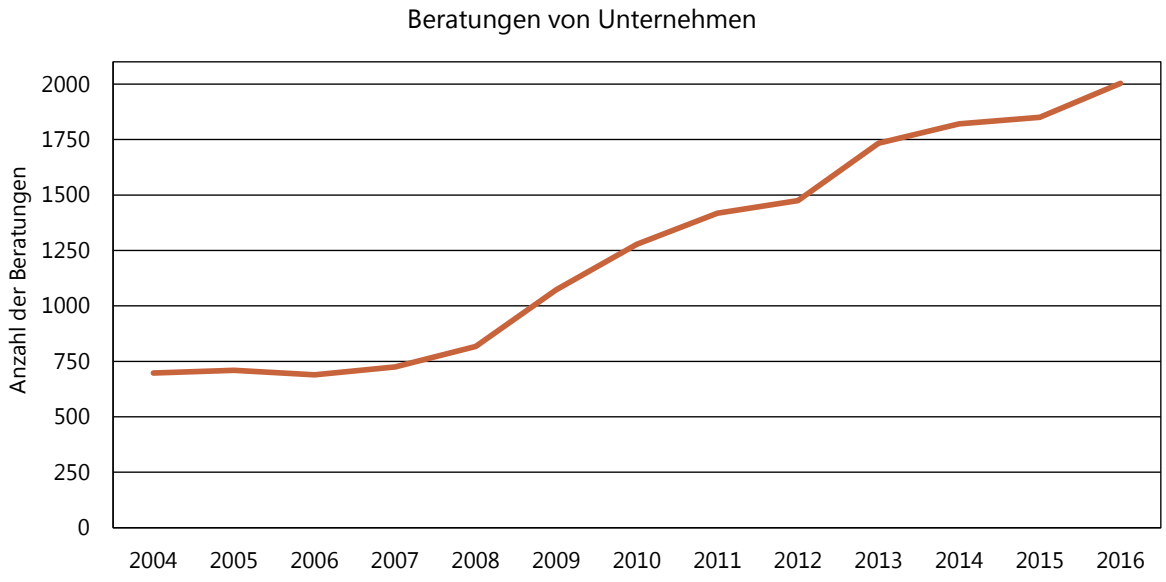
2.1.3 Beratung der verantwortlichen Stellen und der betrieblichen Datenschutzbeauftragten

Die Beratung der verantwortlichen Stellen und betrieblichen Datenschutzbeauftragten ist nach den geltenden Vorschriften des BDSG eine der Pflichtaufgaben der Datenschutzaufsichtsbehörde. In welchem Umfang und innerhalb welcher Zeit diese Aufgabe zu erfüllen ist, ergibt sich nicht unmittelbar aus dem Gesetz.

Wir sehen dies als einen ganz besonderen Schwerpunkt unserer Arbeit, weil wir dadurch steuern können, wie verantwortliche Stellen mit personenbezogenen Daten der Betroffenen umgehen und damit auch vorbeugenden Datenschutz betreiben können.

Beratungen, die teilweise mit einem erheblichen Aufwand für uns verbunden sind, tragen dazu bei, dass wir Informationen darüber erhalten, welche Projekte und Produkte entwickelt werden und welche datenschutzrechtlichen Fragestellungen dabei aufkommen. Dadurch können wir einerseits unsere Beratungsleistungen weiter verbessern, anderseits aber die gewonnenen Erkenntnisse auch gezielt bei Problembereichen im Rahmen von Prüfungen einsetzen.

Um zu verhindern, dass wir als „ausgelagertes Beratungsunternehmen der verantwortlichen Stellen" gebraucht und gelegentlich missbraucht werden, legen wir bei unserer Beratungspraxis großen Wert darauf, dass die verantwortlichen Stellen einerseits den zur Beratung erforderlichen Sachverhalt vollständig darstellen und bezogen auf die datenschutzrechtliche Fragestellungen eine eigene Bewertung abgeben. Dies kann dazu führen, dass unsere Beratungsleistung gelegentlich auch aus einem einfachen „ja, passt so" bestehen kann. Dass unsere Art des Beratens und Bemühens, vorgestellte Projekte oder Produkte nicht einfach als datenschutzrechtlich unzulässig zu bewerten, sondern in diesen Fällen auch daran mitzuwirken, eine rechtlich zulässige und praktisch durchführbare Lösung zu finden, auf Zustimmung stößt, zeigt die – aus unserer Sicht erschreckend – gestiegene Anzahl von Beratungsanfragen.



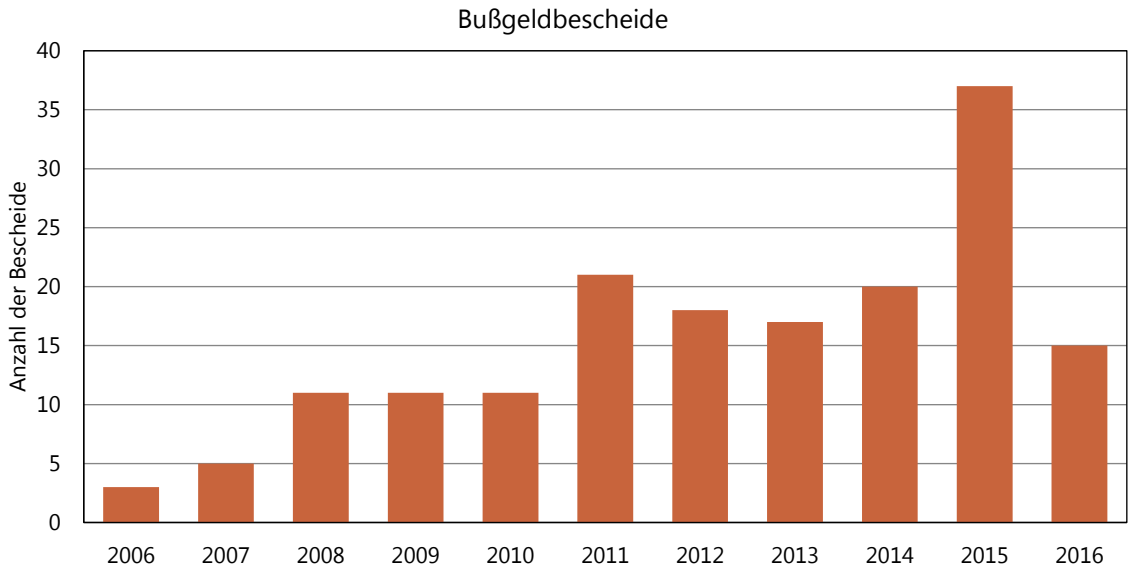
2.1.4 Bußgeldverfahren und Strafanträge

Im Berichtszeitraum haben wir insgesamt 173 Bußgeldverfahren eingeleitet und abgeschlossen – davon 52 mit Erlass eines Bußgeldbescheides. Anfragen zur konkreten Höhe einzelner Bußgelder haben wir – wie bereits im letzten Tätigkeitsbericht dargestellt – nicht detailliert beantwortet, da die Rahmenbedingungen für die Festsetzung eines Bußgeldes sehr vom Einzelfall abhängig und die Ergebnisse deshalb nur sehr beschränkt vergleichbar sind. Bei der Festsetzung des Bußgeldes fließen der Unrechtsgehalt und die wirtschaftlichen Verhältnisse des Adressaten mit ein, so dass gleiche Bußgeldsachverhalte mit deutlich unterschiedlichen Bußgeldern belegt werden können. Zudem ist immer zu beachten, dass bei vorsätzlich begangenen Ordnungswidrigkeiten der eröffnete Bußgeldrahmen doppelt so hoch ist wie für lediglich fahrlässige Verstöße.

Bei einem Blick auf die unten dargestellten Zahlen der Bußgeldbescheide fällt auf, dass im Jahr 2016 nur noch knapp die Hälfte der Bescheide erlassen wurden, die im vorangegangenen Jahr ergingen. Ein Grund dafür war auch, dass die personellen Ressourcen nicht ausgereicht haben, um noch mehr Ordnungswidrigkeitenverfahren zu betreiben. Insbesondere die Anforderungen des internationalen Datenverkehrs und die Mitwirkung an der Erstellung von Arbeitspapieren der Art. 29 Gruppe, die zusammen mit den Bußgeldverfahren in einem Referat bearbeitet werden, haben es erforderlich gemacht, die Prioritäten in diesem Jahr anders zu setzen.

Die Sachverhalte, die wir im Rahmen unserer Bußgeldverfahren behandelt haben, sind im Kapitel 23 dieses Berichts aufgelistet. Einzelne Verstöße, die mit einem Bußgeld geahndet wurden, sind in den Kapiteln 5.5, 6, 10.4, 12.1 sowie 15.1 angesprochen.

Ausblick zur DS-GVO:
Die DS-GVO fordert in Art. 83 Abs. 1, dass jede Aufsichtsbehörde sicherzustellen hat, dass die Verhängung von Geldbußen für Verstöße gegen die Verordnung in jedem Einzelfall „wirksam, verhältnismäßig und abschreckend" ist. Ob es in Zukunft noch vertretbar ist, von einem Opportunitätsprinzip bei der Einleitung von Ordnungswidrigkeitsverfahren auszugehen oder ob der Erlass eines Bescheides bei einer Datenschutzverletzung intendiert ist, ist noch zu klären. Jedenfalls hat der hohe Bußgeldrahmen von bis zu 20 Millionen bzw. 4 % des Weltjahresumsatzes eines Unternehmens schon heute erhebliche Vorwirkungen gezeigt.



2.1.5 Datenpannen

Im Vorfeld zum später folgenden Kapitel über die einzelnen Datenpannen im Berichtszeitraum (Kapitel 21) möchten wir die Entwicklung der Meldungen und die Informationspflichten bei Datenpannen nach § 42a BDSG und § 15a TMG 2015 allgemein erläutern und dabei einen Ausblick auf die DS-GVO gewähren.

Bereits heute sind bestimmte Datenschutzverstöße nach den o. g. Vorschriften meldepflichtig. Konkret müssen nach § 42a BDSG dafür zwei Voraussetzungen erfüllt sein:

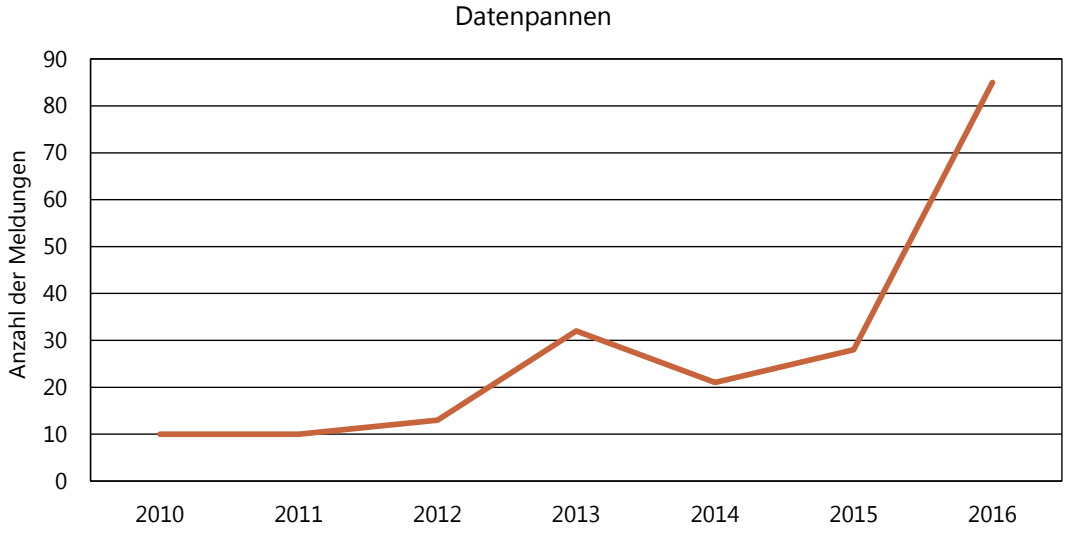
- Die vom Vorfall betroffenen personenbezogenen Daten müssen als sehr sensibel gelten, was z. B. bei Bank- und Gesundheitsdaten der Fall ist.
- Zusätzlich muss davon auszugehen sein, dass durch die Datenpanne ein hohes Risiko für den Betroffenen gegeben ist, d. h. schwerwiegende Beeinträchtigungen drohen.

Während wir in den ersten Jahren unserer Tätigkeit bis 2012 meist nur eine dieser Mitteilungen pro Monat erhalten haben (da die Verpflichtung zur Meldung wohl kaum jemandem bekannt war), hat sich gerade in den vergangenen Jahren eine deutliche Steigerung ergeben. Alleine 2016 sind uns 85 Datenpannen gemeldet worden. Darin enthalten sind nicht die Anfragen zu potentiellen Datenpannen, bei denen wir – meist telefonisch – direkt erkennen konnten, dass die Voraussetzungen der Meldepflicht nicht erfüllt waren. Wir haben diese Vorfälle dann zwar auch aufgearbeitet, jedoch intern nicht als Datenpannen-Vorgang behandelt.

Positiv festgestellt haben wir insbesondere, dass unser Online-Service zur Meldung von Datenpannen große Resonanz findet und die meisten Mitteilungen mittlerweile über diesen Kanal bei uns eingehen. Das Bewusstsein der bestehenden Meldepflicht ist unserem Empfinden nach deutlich gestiegen.

Link:
www.lda.bayern.de/de/datenpanne.html

Ausblick zur DS-GVO:
Künftig regelt die DS-GVO in den Artikeln 33 und 34 den Umgang mit solchen Datenschutzverletzungen, die im internationalen Kontext als „Data breaches" bezeichnet werden. Demnach hat grundsätzlich eine Meldung an die Aufsichtsbehörde zu erfolgen – lediglich dann nicht, wenn die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für den Betroffenen führt. Inwieweit wir deshalb mit einer steigenden Anzahl von Meldungen rechnen müssen, ist derzeit noch nicht absehbar.



2.2 Zusammenarbeit mit den anderen Datenschutzaufsichtsbehörden

Die Zusammenarbeit mit den anderen Datenschutzaufsichtsbehörden fand im Wesentlichen im Rahmen von Datenschutzkonferenzen, dem Düsseldorfer Kreis und den jeweiligen Facharbeitskreisen bzw. Arbeitsgemeinschaften statt.

Wir haben uns bereit erklärt und von der Datenschutzkonferenz den Auftrag bekommen, in Zukunft im Wechsel mit der Datenschutzbehörde von Berlin den Arbeitskreis Medien zu leiten.

Unser Ziel, die Zusammenarbeit bei Prüfungen noch stärker auszubauen, haben wir in dem Umfang, wie wir es uns gewünscht hatten, nicht erreicht. Zwar haben gemeinsame Prüfungen von Dating-Portalen, dem internationalen Datenverkehr und zu Wearables stattgefunden – allerdings haben zum allergrößten Teil wir diese Kontrollen angestoßen und die dazugehörigen Prüffragebögen und Auswertungskriterien erstellt. Dass auch andere Aufsichtsbehörden zu gemeinsamen Prüfungen einladen und entsprechende Vorarbeit leisten oder auch nur andere Aufsichtsbehörden über ihre Prüfungen informieren, ist trotz wiederholter Nachfrage und Bitte um Austausch bisher nicht erfolgreich gewesen.

2.3 Teilnahme und Mitwirkung bei Veranstaltungen

Das Datenschutzrecht ist im Vergleich zu anderen Rechtsgebieten, wie z. B. das Bau- oder Ausländerrecht, ein Gebiet, in dem es relativ wenig strukturierte Rechtsprechung und – bedingt durch die Unabhängigkeit der Datenschutzaufsichtsbehörden – keine Rechtsverordnungen, Vollzugshinweise o. ä. gibt. Für verantwortliche Stellen ist es deshalb von erheblicher Bedeutung zu wissen, welches Vollzugsverständnis Aufsichtsbehörden haben, um sich daran orientieren zu können.

Dies führte auch in diesem Berichtszeitraum wiederum dazu, dass wir bei einer erheblichen Anzahl von Veranstaltungen eingeladen waren, als Referenten mitzuwirken und dies in aller Regel auch gerne gemacht haben, um unsere Auffassung transparent zu machen, aber auch zu erfahren, wie Andere mit bestimmten Fragestellungen umgehen.

Einen ganz besonderen Stellenwert genießen nach wie vor die ERFA-Kreise, die von der Gesellschaft für Datenschutz und Datensicherheit (GDD) in Verbindung mit den zuständigen Industrie- und Handelskammern in München, Nürnberg, Würzburg, Bayreuth und Coburg angeboten werden. Bei diesen Veranstaltungen sind überwiegend betriebliche Datenschutzbeauftragte anwesend, mit denen ein Austausch über aktuelle Fragen für beide Seiten gewinnbringend ist.

Auch das Projekt des Berufsverbands der Datenschutzbeauftragten (BvD) „Datenschutz geht zur Schule" wird von uns nicht nur mit der Übernahme der angebotenen Schirmherrschaft, sondern auch dadurch unterstützt, dass nun zwei Mitarbeiter von uns auch als ehrenamtliche Dozenten in diesem Bereich tätig sind.

2.4 Öffentlichkeitsarbeit

Bei unseren Prüfungen, teils aufgrund von Beschwerden oder im Rahmen anlassloser Kontrollen, stellen wir immer wieder fest, dass viele Datenschutzverstöße – glaubhaft – aus Unkenntnis geschehen sind. Wir haben in Bayern ca. 700.000 verantwortliche Stellen, für die wir als Aufsichtsbehörde zuständig sind. Eine individuelle Beratung dieser Stellen ist nicht möglich. Um eine breite Masse zu erreichen, haben wir Pressemitteilungen zu Einzelfällen mit dem Ziel der Information und Sensibilisierung veröffentlicht und sind bei 169 Anfragen der Medien Rede und Antwort gestanden.

Im Frühjahr 2016 haben wir unsere Homepage – in vollständiger Eigenarbeit – grundlegend überarbeiten können. Dazu haben wir zunächst im Rahmen einer internen Arbeitsgruppe die bisherige Homepage analysiert, Erwartungen an die Neufassung eruiert und sind dann in die direkte Umsetzung eingestiegen. Ziel war es zum einen, Datenschutz-Informationen noch leichter zugänglich zu machen. Wir wollen ferner über unsere umfangreichen Kontrollaktivitäten transparenter informieren und haben uns deshalb entschieden, Prüffragebögen zu veröffentlichen, damit diejenigen verantwortlichen Stellen, die nicht in den „unmittelbaren Genuss" unserer Prüfung gekommen sind, die Möglichkeit haben, im Selbststudium zu testen, wie sie auf die entsprechenden Fragen geantwortet hätten.

Technisch herausfordernd war die Gestaltung des zu diesem Zeitpunkt einzigartigen Online-Beschwerdeformulars, mit dem Bürger sich Ende-zu-Ende-verschlüsselt an uns wenden können. Durch die Vorgabe der auszufüllenden Felder werden die Beschwerdeführer motiviert, die notwendigen Angaben zu machen, die uns unnötige Rückfragen ersparen und so die Bearbeitungszeiten erträglicher gestalten. Nachdem wir nun seit knapp einem Jahr die Möglichkeit der Online-Beschwerde anbieten, stellen wir fest, dass ungefähr jede dritte (elektronische) Beschwerde über dieses Formular eingereicht wird. Wir hatten nicht damit gerechnet, dass diese Funktion bereits im ersten Jahr so stark von den Betroffenen angenommen wird.

Im Zuge der permanenten Fortentwicklung unserer Homepage haben wir ein ebenfalls Ende-zu-Ende-verschlüsseltes Online-Formular zur Meldung von Datenpannen nach § 42a BDSG angeboten, das mittlerweile fast ausschließlich für die Meldung solcher Vorfälle genutzt wird.

In der Planung befindet sich derzeit unser dritter Online-Service, der zur Entgegennahme von Meldungen der Datenschutzbeauftragten dienen soll. Wir gehen einerseits davon aus, dass der Bundesgesetzgeber im Rahmen einer Öffnungsklausel der DS-GVO die Rahmenbedingungen für die Bestellpflicht eines Datenschutzbeauftragten so regeln wird, wie sie bisher im BDSG bestehen und andererseits die Verpflichtung aus der DS-GVO, dass die Verantwortlichen ihre betrieblichen Datenschutzbeauftragten der Aufsichtsbehörde zu melden haben, bestehen bleiben. Dies wird zu einer Masse von Meldungen führen, für die wir ein einfaches Formular mit den zu meldenden Daten (mit entsprechender Datenbank im Hintergrund zur Pflege der Daten) entwickeln.

Im Hinblick darauf, dass zunehmend Anfragen nach englischsprachigen Informationen eingehen, versuchen wir, viele Texte auf der Homepage zudem auf Englisch anzubieten. Auch dieses Angebot werden wir noch weiter ausbauen.

3

Kontrollen und Prüfungen

3 Kontrollen und Prüfungen

Nach § 38 Abs. 1 BDSG ist es Aufgabe für uns als Datenschutzaufsichtsbehörde, die Ausführung des BDSG sowie anderer Vorschriften über den Datenschutz zu kontrollieren. Eine derartige Kontrolle findet bei uns zwar täglich durch Bearbeitung jeder plausiblen Beschwerde statt. Jedoch kann es auch zu einer Kontrolle kommen, die von uns selbst initiiert wird – sei es anlasslos, im Rahmen von Großprüfungen oder auch dadurch, weil wir anderweitig, z. B. aus der Presse, „Wind" von einer Sache bekommen haben.

Wir hatten im 6. Tätigkeitsbericht für 2013/2014 – ebenfalls im Kapitel 3 – sehr ausführlich über diese Art von Kontrollen berichtet. Insbesondere hatten wir die unterschiedlichen Prüfungsanlässe und -formen dargestellt, so dass wir auf eine erneute detaillierte Darstellung unserer schematischen Vorgehensweise in diesem Bericht verzichten. Stattdessen möchten wir auf den nachfolgenden Seiten einen Überblick über die durchgeführten Prüfungen geben. Die Fragen, mit denen die verantwortlichen Stellen in der jeweiligen Prüfung konfrontiert wurden, lassen sich größtenteils von unserer Webseite herunterladen.

Hervorheben möchten wir vorab, dass wir es nicht unversucht haben lassen, koordinierte Prüfungen mit anderen Aufsichtsbehörden durchzuführen. So haben wir gemeinsame Kontrollen von Dating-Portalen, dem internationalen Datenverkehr und Fitness-Trackern (Wearables) mit deutschen Datenschutzaufsichtsbehörden angestoßen, dabei aber leider im Ergebnis feststellen müssen, dass der Aufwand, den wir als BayLDA hierbei für Vorbereitung, Koordination und Durchführung der Prüfungen hatten, in einem nicht vernünftigen Verhältnis zum Ertrag stand (siehe Ausführungen in Kapitel 2.2 Zusammenarbeit mit anderen Datenschutzaufsichtsbehörden).

Als gewinnbringend haben wir die Prüfungen im Rahmen des International Sweep Days betrachtet. Die von dem Global Privacy Enforcement Network (GPEN) organisierten Kontrollen waren bislang strukturiert vorbereitet und im Prüfumfang fokussiert. Unsere Beteiligung an diesen internationalen Prüfaktionen, bei denen zahlreiche Aufsichtsbehörden auf der ganzen Welt mitmachten, war daher mit einem überschaubaren Aufwand verbunden. Im Berichtszeitraum 2015 und 2016 haben wir an GPEN-Prüfungen zum Thema „Internet der Dinge" sowie hinsichtlich „Online-Dienste für Kinder" teilgenommen. In den Vorjahren standen Datenschutzrichtlinien und Apps im Vordergrund der Untersuchungen.

Link:
www.lda.bayern.de/de/kontrollen.html

3.1 Immobilienmakler

Anlass und Ziel der Prüfung

Immobilienmakler erheben und speichern branchenbedingt viele, mitunter auch sensible, personenbezogene Daten. Auf Grund der uns in der Vergangenheit immer wieder vorgetragenen Beschwerden von Betroffenen hatten wir den Verdacht, dass es in der Branche durchaus verbreitet ist, (Kunden-)Daten zu erheben, die eigentlich nicht benötigt werden. Wir wollten daher in Erfahrung bringen, welche personenbezogenen Daten auf welche Art und Weise im Detail erhoben werden. Das Ziel der Prüfung war in erster Linie die verantwortlichen Stellen darauf hinzuweisen, welche Daten für den Zweck der Vermietung bzw. des Kaufs einer Immobilie aus datenschutzrechtlicher Sicht benötigt und welche nicht benötigt werden. Somit stand die Sensibilisierung für den Datenschutz im Vordergrund.

Prüffragen

Nachfolgend stellen wir einen Auszug der Fragestellungen dieser Prüfung vor:

- Werden Kopien von Ausweisdokumenten angefordert bzw. angefertigt?
- Welche personenbezogenen Daten werden von Kunden erhoben, wenn sie sich vor einem Besichtigungstermin für ein konkretes Objekt interessieren?
- Besteht eine schriftliche Vertragsregelung nach § 11 Abs. 2 Satz 2 BDSG mit Auftragnehmern (z. B. Cloud-Computing-Dienstleister, IT-Wartungsunternehmen)?
- Haben Sie ein Kontaktformular auf Ihrer Webseite, über das sich potentielle Kunden an Sie wenden können?
- Besitzt Ihre Webseite eine https-Verschlüsselung mit Perfect Forward Secrecy?

Zeitraum

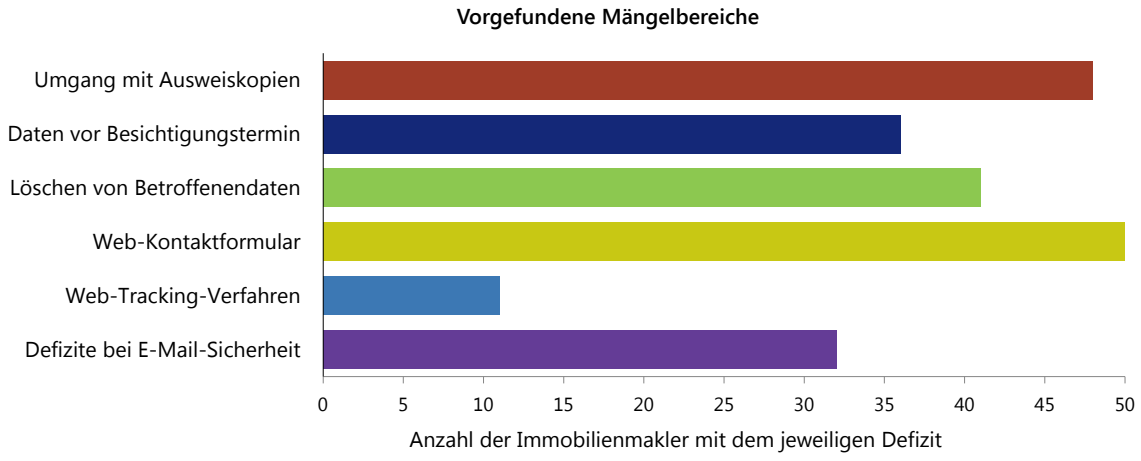
Beginn: Juni 2015
Abschluss: Mai 2016

Anzahl geprüfte Stellen

86 Immobilienmakler (Schwerpunkt auf die Städte München, Nürnberg und Würzburg)

Ergebnis

Als Fazit der Prüfung haben wir erkannt, dass, auch aufgrund von anhaltenden Beschwerden, die Verantwortlichen in der Wohnungswirtschaft weiter für den Datenschutz sensibilisiert werden müssen. Bei fast allen geprüften Maklern bestand erheblicher Handlungsbedarf bezüglich des Umfangs der erhobenen personenbezogenen Daten. Insbesondere wurden die ausgefüllten Selbstauskunftsformulare oft bereits vor einem Besichtigungstermin (meistens zusammen mit einer Ausweiskopie) angefordert und dabei eigentlich nicht benötigte Daten, wie z. B. die Personalausweisnummer oder das Geburtsdatum der miteinziehenden Personen, verlangt.



3.2 Internationaler Datenverkehr

Anlass und Ziel der Prüfung

Grenzüberschreitende Übermittlungen von personenbezogenen Daten in der Privatwirtschaft haben auch in den letzten Jahren weiter zugenommen. Zu den Ursachen dieser Entwicklung zählt auch die stetige Ausbreitung von Dienstleistungen und Produkten des sog. Cloud Computing. Selbst viele kleinere und mittlere Unternehmen in Deutschland verarbeiten inzwischen zahlreiche personenbezogene Daten, häufig auf Servern externer Dienstleister außerhalb der Europäischen Union, meistens von US-Unternehmen. In einer von uns angestoßenen und koordinierten Großprüfung mit neun anderen Aufsichtsbehörden wollten wir gerade diese Verarbeitungsprozesse bei Unternehmen genauer unter die Lupe nehmen.

Prüffragen

Nachfolgend stellen wir einen Auszug der Fragestellungen dieser Prüfung vor:

- Übermitteln Sie personenbezogene Daten in die USA?
- Handelt es sich dabei um Kundendaten und/oder Mitarbeiterdaten und/oder sonstige personenbezogene Daten?
- Auf welchen gesetzl. Grundlagen erfolgt derzeit die Übermittlung in die USA?
- Nehmen Sie Leistungen (z. B. Fernwartung, Support, Reisemanagement) aus Staaten außerhalb der EU und des EWR in Anspruch?
- Setzten Sie Cloud-Speicherlösungen externer Anbieter ein?

Zeitraum

Beginn: November 2016
Abschluss: noch offen

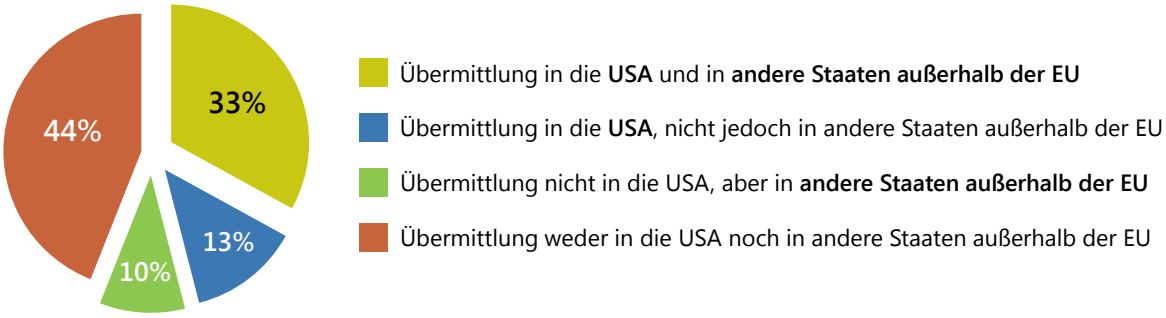
Anzahl geprüfte Stellen

150 Unternehmen (bundesweit insgesamt 500)

Ergebnis

Die Prüfung ist noch nicht abgeschlossen. Dennoch haben wir bereits jetzt anhand der eingegangen Antworten erkannt, dass bei vielen Unternehmen das Bewusstsein fehlt, dass sie Dienste ausländischer Firmen in Anspruch nehmen, bei denen zwangsläufig weitere datenschutzrechtliche Anforderungen zu berücksichtigen sind. Ein wichtiges Ziel dieser Prüfung wird daher in der Sensibilisierung der Unternehmen für Datenübermittlungen in Länder außerhalb der Europäischen Union liegen. Dort, wo wir es als notwendig erachten, werden wir auch in eine tiefere Prüfung einsteigen.

Vorläufiges Ergebnis



3.3 Bewerberdaten

Anlass und Ziel der Prüfung

Die Motivation, den Umgang mit Bewerberdaten in Unternehmen zu überprüfen, war, dass uns in der Vergangenheit immer wieder Beschwerden zu diesem Thema erreichten. Es stellte sich für uns u. a. die Frage, ob bei unternehmensinternen Weitergaben der Bewerbungsunterlagen (z. B. an die Fachstelle, in der die betreffende Stelle zu besetzen ist) die Vorgaben von Datenschutz und Datensicherheit eingehalten werden. Ziel der Großprüfung war es deshalb, die Unternehmen bei ihrem Umgang mit Bewerberdaten zu kontrollieren, aber auch noch stärker für den Datenschutz zu sensibilisieren.

Prüffragen

Der Fragebogen enthielt einerseits rechtliche Fragen, beispielsweise

- wie lange die Bewerberdaten nach Abschluss des Bewerbungsverfahrens noch vorgehalten werden,
- ob es Festlegungen für den Umgang mit Bewerberdaten bei interner Weitergabe gibt oder
- ob die Bewerbungsunterlagen an Dritte (wie Personaldienstleister) weitergegeben und in einem solchen Fall die Bewerber rechtzeitig darüber informiert werden.

Auf der anderen Seite wurden auch Fragen zum technischen Datenschutz gestellt, z. B.

- ob bei E-Mail-Bewerbungen ausreichende Verschlüsselungsmöglichkeiten (wie PGP) angeboten werden und
- ob Verfahren zur Reichweitenmessung eingesetzt werden.

Zeitraum

Beginn: März 2015
Abschluss: August 2016

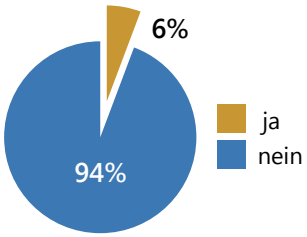
Anzahl geprüfte Stellen

70 Unternehmen

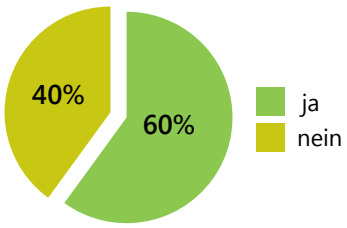
Ergebnis

Die Auswertung der Antworten ergab, dass die meisten Unternehmen im Großen und Ganzen ordentlich mit Bewerberdaten umgehen, Defizite jedoch vor allem in der technischen Absicherung von Bewerbungsplattformen bestehen. Auch ist zu erkennen, dass nach wie vor sehr wenige Unternehmen verschlüsselte E-Mail-Bewerbungen ermöglichen.

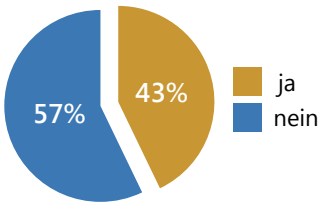
Verschlüsselte E-Mail-Bewerbung möglich?



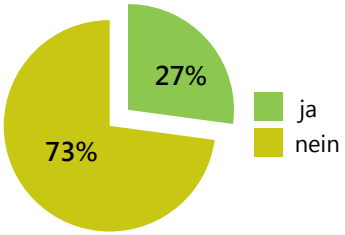
Unterstützt der E-Mail-Server STARTTLS mit PFS?



Sind Bewerbungen über die Webseite möglich?



Ist die Webseite ausreichend sicher (https+PFS)?



3.4 Selbstauskunft

Anlass und Ziel der Prüfung

Wir haben uns im September 2015 dazu entschieden, eine für uns völlig neue Form der Prüfung auszuprobieren. Dazu haben wir über eine Annonce in einer Tageszeitung nach freiwilligen Teilnehmern gesucht, d. h. Privatpersonen, die uns bei der Prüfung unterstützen. Diese Freiwilligen sollten mit einem von uns zur Verfügung gestellten Muster jeweils fünf beliebige verantwortliche Stellen, mit denen sie in irgendeiner Weise in Kontakt standen oder stehen, anschreiben und ihr Auskunftsrecht geltend machen. Ziel war es zum einen, die Öffentlichkeit über ein datenschutzrechtliches Thema zu informieren und Betroffenen aufzuzeigen, welche Möglichkeiten man als Bürger gegenüber Unternehmen hat. Wir wollten aber durch die Auswertung der Antworten der verantwortlichen Stellen vorallem prüfen, wie das Auskunftsrecht in der Praxis tatsächlich vollzogen wird.

Prüffragen

Die freiwilligen Teilnehmer haben mit unsrem Muster die verantwortlichen Stellen angeschrieben und um Auskunft nach § 34 BDSG über die dort von ihnen bzw. über sie gespeicherten Daten gebeten.

Zeitraum

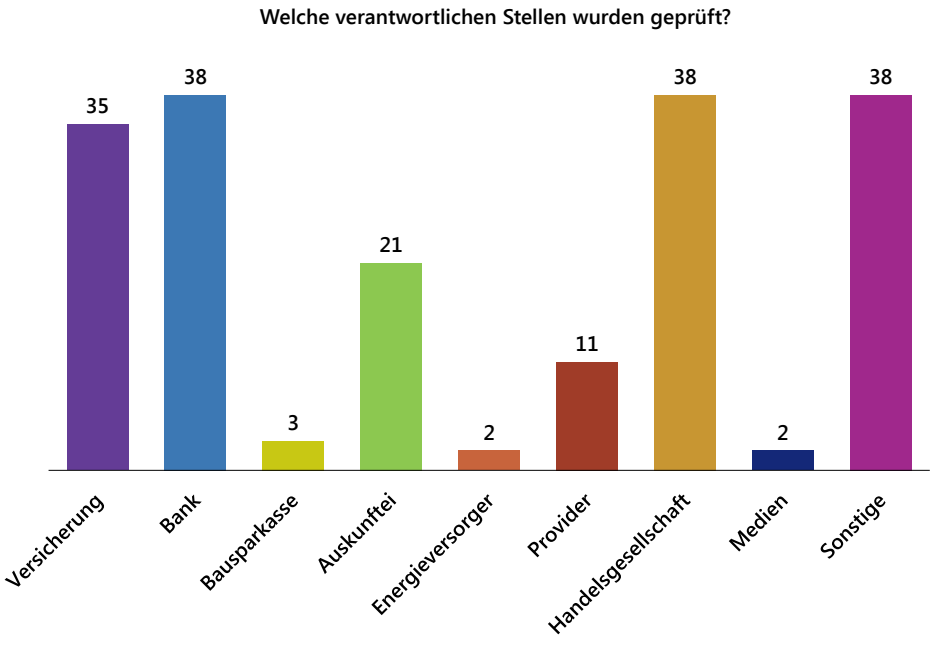
Beginn: September 2015
Abschluss: Januar 2016

Anzahl geprüfte Stellen

188 verantwortliche Stellen wurden – dank 31 aktiven freiwilligen Teilnehmern – geprüft.

Ergebnis

Die Auswertung ergab, dass lediglich in 8% der Fälle gar keine Auskunft erteilt wurde. Die Antworten, die die freiwilligen Teilnehmer erreichten, waren zu 70% zur Zufriedenheit der Betroffenen. Wir haben die gewonnenen Erkenntnisse – gerade zu den mangelhaften oder nicht vollständigen Auskünften – genutzt und Hinweise für Unternehmen in einem neuen Infoblatt zusammengestellt, so dass Unternehmen erfahren, wie richtig Auskunft zu erteilen ist.



3.5 Datenschutzorganisation

Anlass und Ziel der Prüfung

In den vorangegangenen Jahren hat es sich als ein äußerst positives Prüfinstrument erwiesen, regelmäßig durch schriftliche Großprüfungen die Umsetzung von zentralen datenschutzrechtlichen Anforderungen zu kontrollieren. Aus diesem Grund haben wir auch 2015 und 2016 solche allgemeinen Prüfungen zur Datenschutzorganisation durchgeführt. Ziel war es, insbesondere die Themenfelder rund um den Datenschutzbeauftragten, das Verfahrensverzeichnis, die Regelungen zur Auftragsdatenverarbeitung, das IT-Sicherheitskonzept usw. zu durchleuchten. Im Berichtszeitraum haben wir drei dieser Datenschutzorganisationsprüfungen durchgeführt. Im Anschluss an das schriftliche Prüfverfahren kontrollierten wir durch Vor-Ort-Kontrollen stichprobenmäßig die Einhaltung der Vorschriften bzw. der gemachten Angaben.

Prüffragen

Nachfolgend stellen wir einen Auszug der Fragestellungen dieser Prüfungen vor:

- Erstellt der Datenschutzbeauftragte Berichte über seine konkreten Tätigkeiten, Mitarbeiterschulungen etc.?
- Findet Videoüberwachung innerhalb oder außerhalb des Gebäudes statt?
- Ist die Verwendung privater Kommunikationsmittel für dienstliche Zwecke erlaubt?
- Wird Altpapier datenschutzgerecht entsorgt?
- Werden Mitarbeiter auf das Datengeheimnis gemäß § 5 BDSG verpflichtet?

Zeitraum

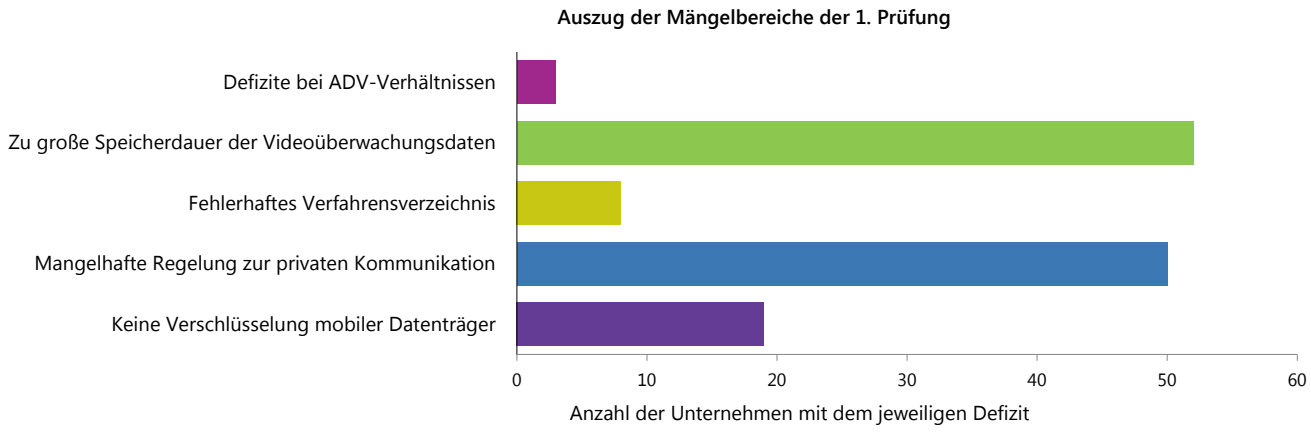
Die erste Prüfung aus 2015 ist vollständig abgeschlossen. Für die darauf folgenden Prüfungen im Jahr 2016 konnten noch nicht alle Vorgänge abgeschlossen werden.

Anzahl geprüfte Stellen

117 Unternehmen im Jahr 2015;
56 Unternehmen im Frühjahr 2016;
25 Unternehmen im Herbst 2016.

Ergebnis

Insgesamt ist festzustellen, dass bei einem Großteil der Unternehmen die grundlegenden Vorgaben aus dem BDSG erfüllt werden. Eher selten treffen wir auf Unternehmen, die gänzlich unvorbereitet sind und enormen Nachholbedarf offenbaren. In den allermeisten Fällen lassen sich die festgestellten Mängel ohne größere Probleme beheben, z. B. durch die Festlegung einer Regelung zur Nutzung von Internet und E-Mail am Arbeitsplatz oder durch eine Anpassung der Speicherdauer der Videoüberwachungsdaten.



3.6 Internet und E-Mail am Arbeitsplatz

Anlass und Ziel der Prüfung

Immer wieder erhalten wir Anfragen von Unternehmen, wie die Regelungen zur Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz aus Arbeitgebersicht zu gestalten sind, insbesondere wenn auch eine private Nutzung im geringfügigen Umgang gestattet ist. Bislang haben wir feststellen müssen, dass Unternehmen zum Teil aus Unkenntnis heraus gravierende datenschutzrechtliche Fehler unterlaufen. Aus diesem Grund untersuchen wir derzeit in einer bayernweiten Prüfaktion, inwieweit die datenschutzrechtlichen Anforderungen in der Praxis eingehalten werden. Ziel ist dabei u. a. die Sensibilisierung der Arbeitgeber dahingehend, dass bei Gestattung der Privatnutzung Nutzungsregeln zu erstellen und Einwilligungserklärungen einzuholen sind.

Prüffragen

Nachfolgend stellen wir einen Auszug der Fragestellungen dieser Prüfungen vor:

- Ist den Beschäftigten eine Nutzung des betrieblichen E-Mail-Postfachs für private Zwecke gestattet?
- Wird auf das betriebliche E-Mail-Postfach des Beschäftigten z. B. im Fall der krankheits- oder urlaubsbedingten Abwesenheit, zugegriffen?
- Hat ein Mitarbeiter beim Ausscheiden die Möglichkeit, seine E-Mails zu löschen?
- Erfolgt eine Protokollierung der Log-Daten hinsichtlich der privaten Nutzung des Internets auf betrieblichen Geräten?
- Erfolgt eine automatische Weiterleitung aller ein- und ausgehenden E-Mails an den Vorgesetzten des Beschäftigten?

Zeitraum

Beginn: Dezember 2016
Abschluss: noch offen

Anzahl geprüfte Stellen

50 Unternehmen

Ergebnis

Wir werden über das Ergebnis zur gegebenen Zeit auf unserer Webseite berichten. Auch planen wir, die neu gewonnenen Erkenntnisse in die Weiterentwicklung der Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz miteinfließen zu lassen.

3.7 International Sweep Week

Anlass und Ziel der Prüfung

Wir haben uns auch in den beiden vergangenen Jahren an den internationalen Prüfaktionen des Global Privacy Enforcement Networks (GPEN) beteiligt. So haben wir im Jahr 2015 gemeinsam mit anderen Aufsichtsbehörden Online-Dienste für Kinder untersucht. Für uns waren dabei speziell Apps bayerischer Anbieter interessant, die sich gezielt an Kinder richteten.

Im Jahr 2016 standen dagegen smarte Alltagsgeräte aus dem „Internet der Dinge" auf dem Prüfstand. Wir haben uns u. a. folgende vernetzte Gerätearten näher angesehen (d. h. alle diese Geräte waren mit smarten Funktionen ausgestattet): Spielzeugpuppe, Fitness-Tracker, Zahnbürste, Gabel, Spielkonsolen, Brettspiel, Connected Cars, Glühlampe, Spielzeugroboter.

Prüffragen

Bei den Prüfungen stand in erster Linie die Information des Nutzers über die Datenverarbeitung im Vordergrund, d. h. wird der Nutzer/Käufer verständlich und ausreichend über die Datenerhebung informiert, werden tatsächlich nur erforderliche Daten verarbeitet und kann der Nutzer überhaupt seine (Datenschutz)rechte geltend machen.

Zeitraum

Der Sweep Day 2015 fand im Mai, die etwas umfassendere Sweep Week im April 2016 statt.

Anzahl geprüfte Stellen

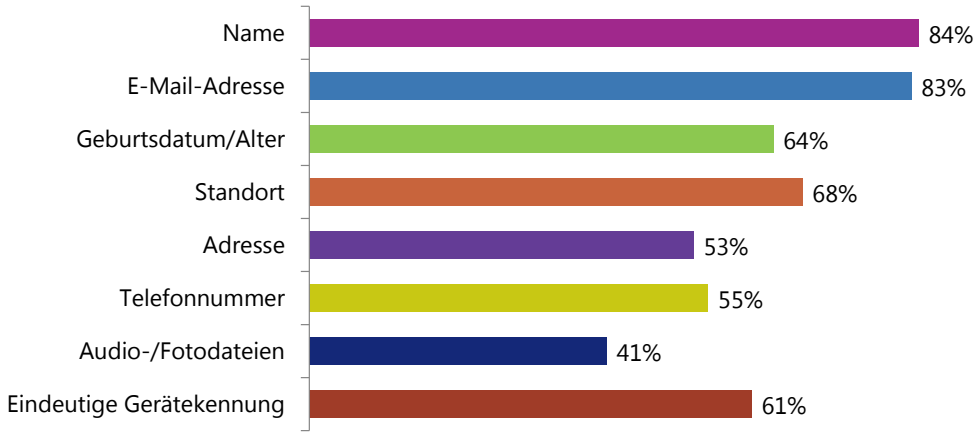
50 Apps für Kinder (2015);
14 Smart-Devices (2016).

Ergebnis

Der Sweep Day 2015 zeigte, dass Apps nach wie vor Mängel gerade hinsichtlich der Transparenz der Datenverarbeitung offenbaren. Die Kinder-Apps, die wir prüften, haben zudem oft vermissen lassen, dass Eltern Datenflüsse der Apps gezielt steuern oder unterbinden können.

Auch bei der Sweep Week 2016 war festzuhalten, dass ein Großteil der Datenschutzbestimmungen von smarten Geräten keine oder nur unzureichende Informationen über den Umgang mit den personenbezogenen Daten des Nutzers enthält. Alle geprüften Geräte hatten eine erhebliche Menge an persönlichen Daten gesammelt und diese oft auch zu gezielten Nutzerprofilen zusammengefügt. Wir werden daher künftig weiterhin das Internet of Things im Rahmen unserer Prüfmöglichkeiten berücksichtigen.

Welche Daten des Nutzers wurden durch Geräte des „Internet der Dinge" erhoben und verarbeitet?



3.8 Dating-Portale

Anlass und Ziel der Prüfung

Im Berichtszeitraum haben wir zusammen mit den Datenschutzaufsichtsbehörden von Baden-Württemberg, Berlin und Hamburg eine koordinierte datenschutzrechtliche Prüfung von Dating-Portalen im Internet vorgenommen. Dies beinhaltete die gemeinsame Entwicklung eines Prüfkatalogs, eine zeitlich abgestimmte Durchführung der Prüfungsaktion und einen gemeinsamen Austausch über die vorgefundenen Prüfungsergebnisse. Dating-Webseiten sind in unseren Prüffokus gerückt, weil durchgängig festzustellen ist, dass Nutzer nach ihrer Registrierung animiert werden, auch höchst sensible und intime Informationen preiszugeben (z. B. Rauch- und Trinkgewohnheiten, Gewicht, Religionspraxis, Fitnesslevel, erotische Vorlieben oder „Erotiktyp").

Prüffragen

Für die Prüfung wurde ein 25-seitiger Prüfkatalog verwendet. Nachfolgend stellen wir exemplarisch ausgewählte Fragen dar:

- Welche Daten werden im Rahmen des Registrierungsvorgangs von einem Nutzer erhoben?
- Welche Profildaten des Nutzers sind für andere Personen durch Benutzereinstellungen einsehbar?
- Hat der Nutzer Nachweise zur Identitätsfeststellung vorzulegen?
- Findet eine Auswertung von Öffnungs- und Klickraten des Newsletters statt?
- Mit welchen Merkmalen identifiziert sich der Nutzer beim Login?

Zeitraum

Beginn: Juni 2015
Abschluss: September 2016

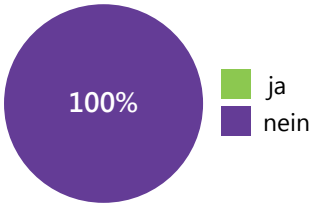
Anzahl geprüfte Stellen

10 Dating-Portale in Bayern (bundesweit 21)

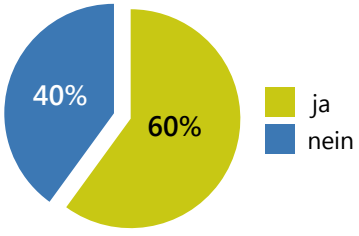
Ergebnis

Neben den positiven Feststellungen bei der Auswertung der eingegangenen Antworten – beispielsweise verfügt die überwiegende Anzahl der geprüften Portale über einen betrieblichen Datenschutzbeauftragten und ist sich der datenschutzrechtlichen Relevanz des Portals durchaus bewusst – wurde von uns in manchen Teilbereichen noch erheblicher Nachholbedarf der Portalbetreiber erkannt. So wurden z. B. Mängel in Form von unzureichenden Anmeldeverfahren, mangelnder Transparenz der vorgefundenen Datenschutzerklärungen oder auch der nicht ausreichenden Rechtsgrundlage für einen Zugriff auf Kommunikationsinhalte festgestellt. Wir haben daher den in Bayern ansässigen Portalbetreibern unser Prüfungsergebnis in schriftlicher Form mitgeteilt und diese zur Umsetzung eventuell notwendiger Überarbeitungen des Internetauftritts und der Verfahrenspraxis angehalten bzw. auch in konstruktiven persönlichen Gesprächen die Fachthemen erörtert und das weitere Vorgehen abgestimmt.

Verfügt das Portal über ein ausreichend sicheres Login-Verfahren für den Nutzer?



Findet eine Auswertung des Newsletters statt (Öffnungs- und Klickraten-Tracking)?



3.9 Facebook Custom Audience

Anlass und Ziel der Prüfung

In unserem letzten Tätigkeitsbericht hatten wir im Kapitel 22.13 darüber informiert, dass Unternehmen, die das Produkt „Custom Audience" von Facebook einsetzen, die Eröffnung eines Bußgeldverfahrens riskieren. Hintergrund war hierbei die unwirksame Anonymisierung der übertragenen personenbezogenen Daten im Rahmen des Verfahrens. Wir haben uns deshalb im Berichtszeitraum entschieden, zunächst in einer kleineren Prüfung einzelne Unternehmen stichprobenartig bezüglich des Einsatzes von Facebook Custom Audience zu kontrollieren. Hierfür haben wir zufällig Unternehmen aus ganz Bayern ausgewählt, die Webseiten mit Onlineshop-Funktion anbieten. Es handelte sich somit um eine anlasslose Prüfung, d. h. konkrete Anhaltspunkte dafür, dass im Verantwortungsbereich der verantwortlichen Stellen nicht ordnungsgemäß mit Kundendaten umgegangen wird, lagen uns bis dato nicht vor.

Prüffragen

Den geprüften Stellen wurden insb. folgende Fragen gestellt:

- Verwenden Sie Facebook Custom Audience?
- Werden von Ihnen E-Mail-Adressen oder Telefonnummern Ihrer Kunden an Facebook (gehasht) übertragen?
- Nutzen Sie für den Einsatz von Facebook Custom Audience einen „Facebook-Pixel"?

Zeitraum

Beginn: Dezember 2015
Abschluss: noch offen

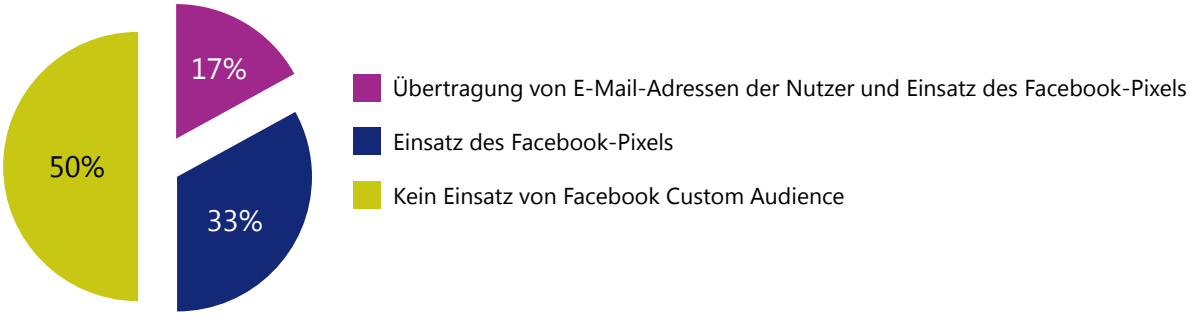
Anzahl geprüfte Stellen

12 verantwortliche Stellen

Ergebnis

Durch die Gespräche mit den verantwortlichen Stellen im Rahmen der Prüfung haben wir festgestellt, dass das Verfahren Facebook Custom Audience in der Praxis durchaus Verbreitung findet. Die Unternehmen waren sich aber in keinem Fall bewusst, dass dabei eine datenschutzrechtliche Problematik besteht. Erst auf unser Schreiben hin wurden sie auf die datenschutzrechtlichen Hintergründe und Fragestellungen aufmerksam.

Wir haben das Thema auf Grund seiner großen Reichweite im Arbeitskreis Medien der deutschen Aufsichtsbehörden platziert und im Dezember 2016 hierzu ein erstes gemeinsames Treffen in Ansbach stattfinden lassen. Der Anbieter des Verfahrens, Facebook, hat leider kurzfristig die Teilnahme an der Veranstaltung abgesagt. Wir werden nun bei den geprüften Stellen, die angaben, das Verfahren einzusetzen, für Klarheit sorgen, welche Rahmenbedingungen konkret für einen weiteren Einsatz zu berücksichtigen sind. Es kann hierbei jedoch auch wie angekündigt zur Einleitung von Ordnungswidrigkeitsverfahren kommen, deren konkretes Ausmaß noch völlig offen ist. Wir halten somit an unserer Auffassung fest, dass sowohl die Verfahren der Kundenliste als auch die des Zählpixels als datenschutzrechtlich problematisch einzustufen sind.



3.10 Offline-Tracking

Anlass und Ziel der Prüfung

Bereits im vergangenen Tätigkeitsbericht hatten wir im Kapitel 22.10 „Besucherstrommessung mit dem Smartphone" auf die Datenschutzproblematik beim sog. Offline-Tracking hingewiesen. Wir verstehen darunter Verfahren, um die Funksignale von mobilen Endgeräten (z. B. WLAN, Bluetooth, GSM) für Marketing- und Prozessoptimierungszwecke auszuwerten. Meist soll damit gerade im Einzelhandel das Bewegungs- und Besuchsverhalten von Kunden analysiert werden. Mit einer ersten Prüfung in diesem Bereich wollten wir uns primär ein Bild davon machen, ob und wenn ja welche Verfahren bei bayerischen Einzelhandelsunternehmen eingesetzt sind.

Prüffragen

Nachfolgend listen wir Fragen auf, die den Unternehmen im Rahmen der Prüfung gestellt wurden:

- Setzen Sie in Ihrem Unternehmen Verfahren zur Erhebung und Verarbeitung von Funksignalen von Smartphones von Kunden, Beschäftigten oder Passanten ein?
- Welche Funksignale werden erfasst?
- Wie viele Sensoren haben Sie zur Erfassung der Funksignale im Einsatz?
- Wo werden die Rohdaten (eindeutige Gerätenummer, Zeitstempel und Signalstärke) gespeichert?
- Werden kryptographische Verfahren zur Verarbeitung der Gerätenummern eingesetzt?

Zeitraum

Beginn: Januar 2016
Abschluss: Mai 2016

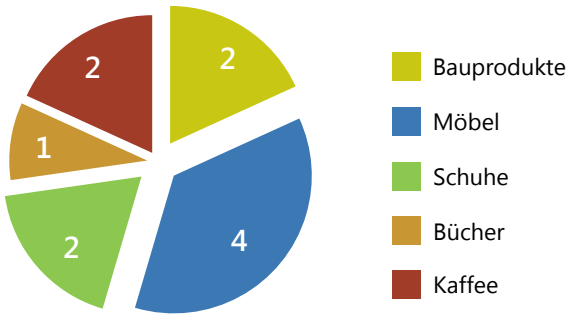
Anzahl geprüfte Stellen

11 Unternehmen

Ergebnis

Die Antworten der Unternehmen waren eindeutig: Keine einzige verantwortliche Stelle gab uns gegenüber im Rahmen der Prüfung an, ein Verfahren zum Offline-Tracking einzusetzen. Wir hinterfragen diese Antworten selbstverständlich und werden deshalb die Angaben stichprobenartig vor Ort überprüfen. Gerade weil uns bereits einige Fälle aus der Praxis bekannt sind, bei denen Offline-Tracking gezielt eingesetzt wird, haben wir Zweifel an der Richtigkeit der Antworten. Wir nehmen an, dass viele Unternehmen sich davor scheuen, den Einsatz dieser noch relativ neuen Verfahren einer Aufsichtsbehörde mitzuteilen, da eine Unsicherheit hinsichtlich ihrer datenschutzrechtlichen Zulässigkeit besteht.

Geprüfte Unternehmen im Einzelhandel nach Branche



3.11 Fitness-Armbänder

Anlass und Ziel der Prüfung

Wir initiierten eine deutschlandweite Prüfaktion, um gemeinsam mit sechs weiteren Aufsichtsbehörden sog. Wearables zu prüfen. Auf dem Prüfstand standen sowohl Fitness-Armbänder als auch Smart Watches mit Gesundheitsfunktionen. Außerdem wurden die Apps der Hersteller einer technischen Analyse unterzogen. Hierzu diente unsere Dienststelle in Ansbach als eines von drei Testcentern, in denen die Aufsichtsbehörden die technische Untersuchung gebündelt durchführen wollten. Da die Geräte in Deutschland vermehrt Einzug in den Alltag finden, war das große Ziel der Prüfung sich zunächst ein Bild davon zu machen, welche Daten der Nutzer tatsächlich durch Wearables verarbeitet und an wen diese übermittelt werden.

Prüffragen

Geprüft wurden zum einen zahlreiche rechtliche Fragestellungen, wie z. B. die ausreichende Aufklärung über den Datenumgang oder die Frage, ob Gesundheitsdaten verarbeitet werden. Im technischen Prüfumfeld wurden primär die Datenflüsse analysiert, um festzustellen, welche Daten übertragen werden und wer auf diese Zugriff bekommen kann. Außerdem war ein Blick auf die dazugehörigen Apps notwendig. Ohne die Apps sind die meisten Wearables in ihrer Funktion erheblich eingeschränkt oder sogar unbrauchbar.

Zeitraum

Beginn: Juni 2016
Abschluss: Dezember 2016

Anzahl geprüfte Stellen

16 Wearables insgesamt, drei davon federführend durch uns.

Ergebnis

Durch die Prüfung haben wir festgestellt, dass zahlreiche Datenschutzmängel bei den Fitness-Trackern bestehen. So ist einer der großen Kritikpunkte die fehlende Transparenz des Herstellers und Betreibers gegenüber den Kunden; viele Käufer können sich anhand der vorhandenen Datenschutzerklärungen kein Bild davon machen, was mit den eigenen Daten passiert. Dies ist insbesondere deshalb als heikel anzusehen, da eine große Menge an sensiblen Daten erhoben wird. Wir konnten erkennen, dass sich aus den gesammelten Daten ein präzises Bild des Tagesablaufs und Gesundheitszustands des Nutzers ergeben kann. Wir werden daher versuchen, trotz der in manchen Fällen noch offenen Zuständigkeitsfrage und den begrenzten Personalkapazitäten, im Dialog mit den Herstellern und den entsprechenden Verbänden die festgestellten Mängel abzustellen. Insgesamt hat die Prüfung aber aufgezeigt, welche Vollzugsschwierigkeiten sich bei deutschen Datenschutzaufsichtsbehörden bei Produkten dieser Art ergeben können.

3.12 Fotos im Internet

Anlass und Ziel der Prüfung

Ein für uns seit Jahren wiederkehrendes Thema ist die Veröffentlichung von Bildern im Internet. Wir hatten schon in vergangenen Tätigkeitsberichten verschiedene Praxisfälle dargestellt, die die Hintergründe hierzu durchleuchteten und die Notwendigkeit der Einholung einer Einwilligung der abgebildeten Personen beschrieben. Da es aber im Berichtszeitraum nach wie vor sowohl Anfragen als auch Beschwerden zu Fotos im Internet gab (siehe Kapitel 7.7), haben wir uns entschlossen, gezielt Sportvereine in einer schriftlichen Prüfaktion hierzu zu befragen. Ziel der Prüfung war festzustellen, ob die bekannten datenschutzrechtlichen Anforderungen berücksichtigt bzw. korrekt umgesetzt werden.

Prüffragen

Nachfolgend listen wir Fragen auf, die den Unternehmen im Rahmen der Prüfung gestellt wurden:

- Wird vor einer Veröffentlichung der Fotos eine Einwilligung eingeholt?
- In welcher Form wird die Einwilligung eingeholt?
- Legen Sie uns ein Muster Ihrer Einwilligungserklärung vor.
- Von wem wird im Fall von Fotos von Kindern die schriftliche Einwilligung eingeholt?
- Wie, wo und von wem werden die schriftlichen Einwilligungserklärungen aufbewahrt?
- Werden die veröffentlichten Fotos im Fall einer widerrufenen Einwilligung gelöscht?

Zeitraum

Beginn: November 2016
Abschluss: noch offen

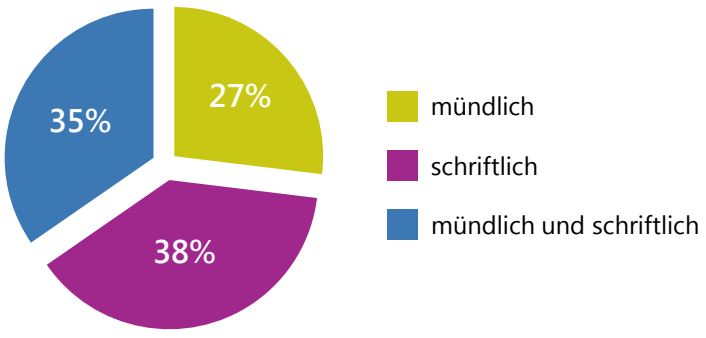
Anzahl geprüfte Stellen

26 Sportvereine aus ganz Bayern mit insgesamt über 40.000 Mitglieder, davon ca. 15.000 Mitglieder unter 18 Jahre.

Ergebnis

Die Prüfung war zum Berichtszeitraum noch nicht abgeschlossen. Durch die bisherigen Rückläufe haben wir aber jetzt schon feststellen können, dass sich die geprüften Vereine zumindest der Verantwortung und Anforderung bewusst sind, dass in vielen Fällen eine Einwilligung der betroffenen abgelichteten Personen erforderlich ist. Wir werden über das abschließende Prüfergebnis wie gewohnt auf unserer Webseite berichten.

In welcher Form wird die Einwilligung geholt?



4

Der betriebliche Datenschutzbeauftragte

4 Der betriebliche Datenschutzbeauftragte

4.1 Unvereinbarkeit mit anderen Aufgaben

Zum Datenschutzbeauftragten können nicht solche Personen bestellt werden, die im Unternehmen noch weitere Aufgaben wahrnehmen, die zu Interessenkonflikten mit den Aufgaben eines Datenschutzbeauftragten führen können.

Mehrfach wurden wir zu Sachverhalten der Vereinbarkeit der Funktion eines Datenschutzbeauftragten mit der gleichzeitigen Wahrnehmung anderer Aufgaben im oder für das Unternehmen angefragt. Grundsätze dazu hatten wir schon auf unserem Info-Blatt zum betrieblichen Datenschutzbeauftragten sowie unter Nr. 3.2 unseres 5. Tätigkeitsberichts für die Jahre 2011/2012 dargestellt.

Links:
www.lda.bayern.de/media/info_dsb.pdf
www.lda.bayern.de/media/baylda_report_05.pdf

Ob ein angestellter Unternehmensjurist als betrieblicher Datenschutzbeauftragter bestellt werden kann oder hier eine über das übliche vertretbare Maß hinausgehende Interessenkollision anzunehmen ist, hängt vom wahrzunehmenden Aufgabenbereich der Person im Unternehmen ab. Wenn bei einem Unternehmen ein für alle Rechtsbereiche zuständiger Jurist auch zum Datenschutzbeauftragten für dieses Unternehmen eingesetzt werden soll, gehen wir grundsätzlich von einer nicht vertretbaren Interessenkollision zwischen den beiden Funktionen aus, so dass eine Bestellung zum Datenschutzbeauftragten nicht möglich ist. Denn der Jurist müsste dann z. B. einerseits für betroffene Mitarbeiter und Kunden als fachlich unabhängiger Datenschutzbeauftragter Positionen vertreten, die gegenläufig mit der von der Unternehmensleitung beauftragten Rechtsvertretung sein können, insbesondere in arbeitsrechtlichen oder kundenrechtlichen Streitverfahren mit Datenschutzbezug.

Eine Interessenkollision lag nach unserer Auffassung auch im Falle eines Datenschutzbeauftragten eines bayerischen Unternehmens vor, der die Position des IT-Managers des Unternehmens bekleidete. In dem Sachverhalt hatte der IT-Manager eine derart exponierte Position im Hinblick auf die Datenverarbeitungsprozesse im Unternehmen, die aus unserer Sicht unvereinbar mit den Aufgaben eines Datenschutzbeauftragten war. Dies liefe letztlich auf eine Datenschutzkontrolle eines der maßgeblichen zu kontrollierenden Funktionsträger im Unternehmen durch sich selbst hinaus. Eine solche Selbstkontrolle widerspricht der Funktion eines Datenschutzbeauftragten, der gerade eine unabhängige Instanz sein soll, die im Unternehmen auf die Einhaltung des Datenschutzes hinwirkt. Diese Aufgabe kann der Datenschutzbeauftragte nicht erfüllen, wenn er gleichzeitig maßgebliche operative Verantwortung für Datenverarbeitungsprozesse besitzt. Wir hatten das Unternehmen auf diesen Umstand hingewiesen und zur Bestellung eines Datenschutzbeauftragten aufgefordert, der keiner derartigen Interessenkollision unterliegt. Das Unternehmen kündigte zwar wiederholt an, im Zuge von Umstrukturierungen auch die Funktion des Datenschutzbeauftragten neu zu bekleiden – versäumte es jedoch über Monate, uns den Nachweis für die Bestellung eines geeigneten Datenschutzbeauftragten vorzulegen. Vor diesem Hintergrund haben wir gegen das Unternehmen eine Geldbuße festgesetzt (siehe dazu auch unsere Pressemitteilung).

Link:
www.lda.bayern.de/media/pm2016_08.pdf

Ausblick zur DS-GVO:
Die DS-GVO fordert in Art. 38 Abs. 6 von den Verantwortlichen oder Auftragsverarbeitern sicherzustellen, dass die anderen Aufgaben und Pflichten des Datenschutzbeauftragten

nicht zu einem Interessenkonflikt führen. Es bleibt abzuwarten, welche konkreten Aussagen hierzu von der europäischen Ebene kommen. In dem Working Paper WP 243 der Art.-29-Gruppe sind unter Nr. 3.5 „Conflict of interests" bereits erste Aussagen zu finden, welche seit Dezember 2016 der Kommentierung mit weiteren Anregungen durch alle „Stakeholder" offen stehen.

Link:
http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

4.2 Übergabe von Unterlagen beim Wechsel eines Datenschutzbeauftragten

Bei einem Wechsel eines Datenschutzbeauftragten ist auf eine ordnungsgemäße Übergabe der relevanten Unterlagen zu achten.

Wir hatten in den letzten Jahren mehrere Anfragen dazu, wie mit den bisherigen Unterlagen beim Ausscheiden eines Datenschutzbeauftragten zu verfahren ist. Bei einem Wechsel eines Datenschutzbeauftragten ist auf eine ordnungsgemäße Übergabe der relevanten Unterlagen des bisherigen Datenschutzbeauftragten an den neuen Datenschutzbeauftragten zu achten, um im Interesse des Unternehmens und der von den Daten betroffenen Personen (Kunden, Mitarbeiter, Lieferanten etc.) eine möglichst reibungslose und effektive Weiterarbeit des neuen Datenschutzbeauftragten sicherzustellen sowie die Persönlichkeitsrechte der Betroffenen zu wahren.

Zu übergeben sind beispielsweise die Verfahrensverzeichnisse, Unterlagen über durchgeführte Vorabkontrollen, beim Datenschutzbeauftragten noch laufende Beschwerdefälle von Betroffenen sowie für die Zukunft noch relevante abgeschlossene Fälle. Gleiches gilt für die für das Unternehmen erstellten Tätigkeitsberichte, Materialien bzgl. Mitarbeiterschulungen und Unterlagen zu den organisatorischen Datenschutzregelungen des Datenschutzbeauftragten. Nur vertraulich an die bestimmte Person des Datenschutzbeauftragten gerichtete Betroffenen-Anfragen bzw. Datenschutzbeschwerden (siehe § 4f Abs. 4 BDSG) sind vom bisherigen Datenschutzbeauftragten bei Erledigung grundsätzlich zu löschen oder zu vernichten. Bei noch laufenden Fällen solcher vertraulicher Art ist durch Rückfrage beim Betroffenen zu klären, wie er sein Anliegen weiter behandelt haben möchte.

Für sonstige Altunterlagen ist aus unserer Sicht der Zeitraum der allgemeinen Verjährungsfrist von drei vollen Kalenderjahren ein grundsätzlich geeignetes Abgrenzungskriterium, abgeschlossene Altunterlagen noch bzw. nicht mehr zu übergeben.

4.3 Keine befristete Bestellung eines Datenschutzbeauftragten

Eine befristete Bestellung des Datenschutzbeauftragten im Unternehmen würde dessen Kündigungsschutz unterlaufen und ist daher nicht möglich.

Unternehmen fragten bei uns an, ob sie einen ihrer Beschäftigten befristet zum Datenschutzbeauftragten bestellen können. Dies ist jedoch gesetzlich nicht möglich. Denn mit der BDSG-Novelle 2009 wurde – in Ergänzung zum schon gegebenen Schutz vor Abberufung des Datenschutzbeauftragten – für den innerhalb einer verantwortlichen Stelle bestellten Datenschutzbeauftragten ein spezieller Kündigungsschutz in § 4f Abs. 3 Satz 5 BDSG eingefügt. Dieser Kündigungsschutz würde unzulässig unterlaufen werden, wenn eine befristete Bestellung eines Beschäftigten zum Datenschutzbeauftragten möglich wäre. So sieht das wohl auch das Arbeitsgericht Dortmund in dem

Urteil vom 20. Februar 2013, 10 Ca 2800/12, für den Fall der (unzulässigen) Vereinbarung einer Probezeit.

Link:
https://openjur.de/u/678169.html

Ausblick zur DS-GVO:

Wenn der bisherige Kündigungsschutz, wie im Moment im Gesetzgebungsverfahren geplant, für verpflichtend zu bestellende Datenschutzbeauftragte aufrechterhalten wird, ist auch künftig keine befristete Bestellung eines Datenschutzbeauftragten im Unternehmen möglich.

5

Auftragsdatenverarbeitung

5 Auftragsdatenverarbeitung

5.1 Abgrenzung einer Auftragsdatenverarbeitung (ADV) zu anderen Sachverhalten

Die Abgrenzung einer nach § 11 BDSG regelungsbedürftigen Auftragsdatenverarbeitung zu anderen Sachverhalten ist nicht immer offensichtlich.

Unternehmen lagern in großem Umfang Arbeiten aus, die dann im Rahmen einer auftragsgemäßen Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch andere Stellen, der sog. Auftragsdatenverarbeitung, erfüllt werden. Nach § 3 Abs. 8 Satz 3 BDSG sind diejenigen externen Stellen nicht Dritte gegenüber der verantwortlichen Stelle, die im Inland oder im Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag der verantwortlichen Stelle erheben, verarbeiten oder nutzen. Weil solche im Auftrag tätigen externe Stellen nicht als Dritte im Sinne des BDSG eingestuft werden, stellen Datenweitergaben dorthin keine nach dem BDSG (§ 4a, §§ 28 bis 32) zu prüfenden Datenübermittlungen dar, § 3 Abs. 4 Nr. 3 BDSG. Die dabei zu beachtenden Rahmenbedingungen sind vielmehr in § 11 BDSG geregelt.

In anderen Zusammenhängen werden personenbezogene Daten an dritte Stellen für die dortige fachliche Arbeit übermittelt, wenn z. B. eine Fachaufgabe dorthin ausgelagert wurde oder wenn fremde Fachleistungen extern in Anspruch genommen werden. Wann allerdings ein Auftrag (im Kern) nur die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten betrifft und ab wann eine Übermittlung von Daten an einen Dritten zur eigenständigen Verwendung vorliegt, wird zum Teil unterschiedlich diskutiert. Wir vertreten dazu die Auffassung, dass eine Übermittlung von Daten im Rahmen der Auslagerung ganzer Fachaufgaben, wie Auslagerung der Personalabteilung an die Konzernmuttergesellschaft, oder Übermittlung von Daten für die Inanspruchnahme externer Fachleistungen, wie bei der Beauftragung einer Anwaltskanzlei oder eines Gutachters, keine Auftragsdatenverarbeitung darstellt und damit nach den Vorschriften für die Zulässigkeit von Datenübermittlungen in § 4 Abs. 1 und den §§ 28 ff. BDSG zu prüfen ist.

Ferner nicht als Auftragsdatenverarbeitung, sondern als nach dem BDSG zu beurteilende Datenübermittlung (dabei insbesondere: Frage des erforderlichen Umfangs der Daten), haben wir auch eine Zurverfügungstellung personenbezogener Daten in folgenden Sachverhalten der externen Inanspruchnahme von Fachleistungen bewertet:

- externe Fachkraft für Arbeitssicherheit
- externer Krankenhausberater
- externer Geldwäschebeauftragter
- externe Reinigung von mit Namen versehener Berufskleidung
- externe Auslagerung von Bewachungs- und Pförtnerdiensten.

5.2 Website-Hosting als Auftragsdatenverarbeitung

Mit Internet-Service-Providern ist regelmäßig ein Vertrag nach § 11 Abs. 2 Satz 2 BDSG zu schließen.

Zur datenschutzgerechten Einordnung der Tätigkeit von Internet-Service-Providern werden uns immer wieder Fragen gestellt. Service-Leistungen eines Website-Hosters, wie das Entgegennehmen und Archivieren von E-Mails der Kunden oder Interessenten oder von Kontaktformulareintragungen auf der Website im Auftrag, das Tracking des Verhaltens der Website-Nutzer im Auftrag usw., betreffen den Umgang mit personenbezogenen Daten des

Unternehmens als Auftraggeber und sind als Datenverarbeitung im Auftrag nach § 11 BDSG einzuordnen. Diese Dienstleistung bedarf einer Vertragsregelung nach § 11 Abs. 2 Satz 2 BDSG. Wenn ein Service-Provider zu einer solchen Vertragsregelung nicht bereit ist, kann er im geschäftlichen Bereich nicht datenschutzkonform eingesetzt werden (im persönlich-familiären Bereich von Privatpersonen gilt das BDSG gemäß § 1 Abs. 2 Nr. 3 BDSG nicht).

Tätigkeiten von bloßen Internet-Zugangsdiensten (Zugangsvermittlung, Datentransportleistung, einschließlich Website-Hosting ohne weitere Leistungen mit personenbezogenen Daten) unterliegen dagegen (nur) dem Telekommunikations- bzw. Telemedienrecht. Man spricht dann nicht von Service-Providern, sondern von Access-Providern.

5.3 Auslagerung der Telefonanlage

Für die Auslagerung der betrieblichen Telefonanlage an einen Dienstleister ist ein Vertrag nach § 11 Abs. 2 Satz 2 BDSG zu schließen.

Lagern Unternehmen ihre gesamte Telefonanlage an einen Diensteanbieter aus (teilweise „in die Cloud"), einschließlich z. B. der Mitarbeiterdaten zu Nebenstellen und Handys, die Organisation von Telefonkonferenzen, Callcenter-Monitoring, Backup-Sicherung der entsprechenden Daten, so sind damit zusätzliche IT-Dienstleistungen außerhalb der TKG-Regelungen betroffen, die zur Sicherung einer weisungsgebundenen Dienstleistung nach § 11 Abs. 2 Satz 2 BDSG zu regeln sind.

Entscheidend ist also, ob die Leistungen nur die im TKG geregelten Sachverhalte betreffen (insbesondere die im TKG geregelte „Transportleistung", die eventuelle Lieferung von Einzelverbindungsnachweisen, die allgemeinen Abrechnungsdaten etc.) oder ob zusätzlich darüber hinausgehende Dienstleistungen unter Verwendung personenbezogener Daten des Auftraggebers erbracht werden.

5.4 Fernwartung durch Geräte-vermieter bzw. Leasinggeber

Fernwartung von Multi-Funktionsgeräten zum Drucken, Kopieren, Scannen und Faxbetrieb wird regelmäßig von § 11 Abs. 5 BDSG erfasst.

In der IT-Umgebung von Unternehmen werden meist Multi-Funktionsgeräte zum Drucken, Kopieren, Scannen sowie für aus- und eingehende Faxe eingesetzt. Wir wurden verschiedentlich dazu gefragt, wie diese Tätigkeit datenschutzrechtlich einzuordnen ist. Diese Geräte haben meist interne Dokumentenspeicher, so dass bei der Fernwartung ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Damit unterliegen solche Fernwartungssachverhalte dann der Vorschrift von § 11 Abs. 5 BDSG und bedürfen einer vertraglichen Regelung entsprechend § 11 Abs. 2 Satz 2 BDSG (in dem Umfang, wie die dort genannten Punkte auf Fernwartungssachverhalte zutreffen).

Gleiches gilt, wenn externe Wartungstechniker vor Ort kommen, dort eigenständig die Gerätewartung durchführen und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Wir weisen im Übrigen bei Anfragen dieser Art darauf hin, dass die Löschung der Gerätespeicher in Multifunktionsgeräten bei Beendigung der Miete bzw. des Leasings eine Verpflichtung des Unternehmens als verantwortliche Stelle nach § 9 BDSG ist, was nach unseren Erfahrungen in der Praxis leider manchmal übersehen wird.

5.5 Bußgeld wegen unzureichenden Vertrages nach § 11 Abs. 2 Satz 2 BDSG

Wer einen externen Dienstleister als Auftragsdatenverarbeiter mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beauftragt, muss mit diesem einen ordnungsgemäßen schriftlichen Vertrag abschließen – sonst droht ein Bußgeld.

Das BDSG schreibt in § 11 Abs. 2 Satz 2 eine Reihe von Einzelheiten vor, die zum Schutz der personenbezogenen Daten in einem Vertrag bei Auslagerung der Datenverarbeitung an einen Dienstleister ausdrücklich festgelegt werden müssen. Von besonderer Bedeutung sind dabei die technischen und organisatorischen Maßnahmen, die der Auftragsdatenverarbeiter zum Schutz der Daten treffen muss. Diese Maßnahmen müssen in dem schriftlichen Auftrag konkret und spezifisch festgelegt werden. Fehlen konkrete Festlegungen hierzu, stellt dies eine Ordnungswidrigkeit dar, die mit Geldbuße von bis zu 50.000,- € geahndet werden kann.

In einem konkreten Fall haben wir diesbezüglich gegen ein Unternehmen eine Geldbuße in fünfstelliger Höhe festgesetzt. Das Unternehmen hatte in seinen schriftlichen Aufträgen mit mehreren Auftragsdatenverarbeitern keine konkreten technisch-organisatorischen Maßnahmen zum Schutz der Daten festgelegt. Stattdessen enthielten die Aufträge nur einige wenige pauschale Aussagen und Wiederholungen des Gesetzestextes. Dies reicht keinesfalls aus. Denn die datenschutzrechtliche Verantwortung trägt auch im Falle der Einschaltung von Auftragsdatenverarbeitern nach wie vor der Auftraggeber. Dieser muss daher beurteilen können, ob der Auftragsdatenverarbeiter in der Lage ist, für die Sicherheit der Daten zu sorgen.

5.6 Gebühren für einen Vertragsabschluss zur Auftragsdatenverarbeitung

Die Preisgestaltung eines Vertrages für Dienstleistungen nach § 11 BDSG ist eine zivilrechtliche Frage und Sache der verschiedenen Anbieter.

Einige Unternehmen, die DV-Dienstleistungen nach § 11 BDSG auslagern wollten, haben bei uns nachgefragt, ob Auftragsdatenverarbeiter für die Erstellung und Pflege eines Vertrages nach § 11 BDSG ein Entgelt verlangen dürfen und in welchem Umfang das ggfls. angemessen wäre. Wir haben dazu geantwortet, dass es sich dabei um keine datenschutzrechtliche Frage handelt, sondern um eine Frage, die zivilrechtlich zu lösen ist. Insofern haben wir auch keine Stellungnahme zu einer etwaigen Höhe einer Vergütung abgegeben.

6

Auskunftsanspruch

6 Auskunftsanspruch

Betroffene Personen haben nach § 34 Abs. 1 Satz 1 BDSG einen einklagbaren Rechtsanspruch, von den verantwortlichen Unternehmen ihre dort über sie gespeicherten Daten zu erfahren. Im Streitfall unterstützen wir dazu Bürgerinnen und Bürger und verhängen Bußgelder bei Rechtsverstößen.

Eine größere Menge von Beschwerdefällen bei uns bezieht sich schon seit Jahren auf das Auskunftsrecht der betroffenen Personen zu ihren Daten gemäß § 34 Abs. 1 Satz 1 BDSG. Obwohl der Gesetzestext nach unserer Auffassung relativ eindeutig formuliert ist – Auskunft ist zu erteilen über die zur Person des Betroffenen gespeicherten Daten (einschließlich von Daten zur Herkunft der Informationen), zu Datenempfängern und zum Zweck der Datenspeicherung – kommen immer wieder Unternehmen ihren gesetzlichen Verpflichtungen zu einer vollständigen Auskunftserteilung bei entsprechenden Anträgen nicht nach. Das hat uns veranlasst, zu den Anforderungen an die Auskunftserteilung über gespeicherte Daten nach § 34 BDSG ein Info-Blatt zu erstellen. Auch hatten wir im letzten Tätigkeitsbericht für 2013/2014 in Kapitel 6 auf verschiedene Einzelfragen zum datenschutzrechtlichen Auskunftsanspruch hingewiesen.

Links:
www.lda.bayern.de/media/info_anforderungen_auskunft.pdf
www.lda.bayern.de/media/baylda_report_05.pdf

Im Berichtszeitraum dieses Tätigkeitsberichtes haben wir in fünf Fällen von nachhaltig mangelhafter Auskunftserteilung an die betroffenen Antragsteller gegen die verantwortlichen Unternehmen Bußgelder verhängt. Wir möchten dadurch unterstreichen, dass bei Rechtsverstößen dieser Art Bußgelder drohen und verantwortliche Stellen daher Auskunftsersuchen von Betroffenen mit der notwendigen Sorgfalt und Ernsthaftigkeit begegnen sollten.

Ausblick zur DS-GVO:
In der Datenschutz-Grundverordnung hat das Auskunftsrecht der betroffenen Person zu den über sie gespeicherten Daten sowie zu den weiteren Umständen dazu eine zentrale Bedeutung im Rahmen des Katalogs der Betroffenenrechte (siehe im einzelnen Art. 15 DS-GVO). Weil die gesetzlichen Vorgaben in der DS-GVO zu Bußgeldverfahren deutlich verstärkt wurden – Bußgelder sollen wirksam, verhältnismäßig und abschreckend sein – und der den Aufsichtsbehörden hier zur Verfügung stehende Bußgeldrahmen erheblich erweitert wurde (je nach Fall bis zu 20 Mio. Euro bzw. bis zu 4% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs), sind alle Verantwortlichen gut beraten, ihre Verfahren zur Auskunftserteilung an Betroffene zu überprüfen und bei Bedarf zu verbessern.

7

Datenschutz im Internet

7 Datenschutz im Internet

7.1 Erhebung von IP-Adressen bei Abmahnungen

Die Erhebung von Nutzer-IP-Adressen kann bei berechtigtem Interesse grundsätzlich zulässig sein.

Auch in der näheren Vergangenheit haben wir mehrere Anfragen von Betroffenen erhalten, die aufgrund von Urheberrechtsverletzungen abgemahnt wurden. Gegenstand der Anfragen war in der Regel, ob die IP-Adressen der Betroffenen zum Zweck der Abmahnung rechtmäßig erhoben wurden.

Wer auf sog. Filesharing-Plattformen unterwegs ist und urheberrechtlich geschützte Werke herunterlädt, stellt oft automatisch das heruntergeladene Werk auch zum Download für andere Nutzer bereit. Dieser Umstand ist vielen Nutzern häufig nicht bewusst. Indem sie jedoch die geschützten Werke zum Download anbieten, verstoßen sie wiederum gegen Urheberrechte.

„Abmahnkanzleien" haben sich zwischenzeitlich auf die Ermittlung der Urheberrechtsverletzer spezialisiert. Hierzu werden mittels spezieller Software die IP-Adressen der Nutzer, die zunächst Werke heruntergeladen und gleichzeitig wiederum selbst zum Download zur Verfügung gestellt haben, erhoben und gespeichert. Anschließend werden die ermittelten IP-Adressen zur Geltendmachung der zivilrechtlichen Ansprüche über den Auskunftsanspruch gem. § 101 UrhG dem Anschlussinhaber zugeordnet. Die Frage, ob die IP-Adresse in diesen Fällen zulässig erhoben wurde, ist von Bedeutung, wenn es darum geht, zu entscheiden, inwieweit ein Beweisverwertungsverbot vorliegen könnte. Wäre die IP-Adresse des Anschlussinhabers rechtswidrig erhoben, könnte u. U. der Nachweis der Urheberrechtsverletzung nicht mehr erbracht werden. Dies können jedoch nur die Zivilgerichte in einem Verfahren abschließend beurteilen.

Wir sind – unter dem Gesichtspunkt des Datenschutzes – der Auffassung, dass in den konkreten Fällen die IP-Adressen grundsätzlich zulässig erhoben wurden. Der Urheber der geschützten Werke hat ein berechtigtes Interesse an der Verfolgung von Urheberrechtsverletzungen. Dieses Interesse überwiegt denen der Betroffenen.

7.2 Personenbezug von IP-Adressen

In einer grundlegenden Entscheidung bestätigt der EuGH den Personenbezug von IP-Adressen, weist aber auf Einschränkungen bei der Bewertung hin.

Wie in den vorangegangen Jahren haben wir auch in diesem Berichtszeitraum eine Vielzahl von Anfragen zum Einsatz von Analyse- und Sicherheits-Tools für Webseiten erhalten. Dabei ging es oft um die zentrale Frage, ob es sich bei der dynamischen IP-Adresse (der Nutzer) um ein personenbezogenes Datum handelt und damit der Anwendungsbereich des Datenschutzrechts eröffnet ist. Diese Frage hat der EuGH in seiner grundlegenden Entscheidung vom 19. Oktober 2016 (C-582/14) geklärt. Nach Auffassung des EuGH handelt es sich bei der dynamischen IP-Adresse um ein personenbezogenes Datum – allerdings nur unter gewissen Voraussetzungen. Der EuGH stellte klar, dass sich die dynamische IP-Adresse zwar nicht unmittelbar auf eine „bestimmte" Person beziehe. Es handelt sich aber um eine Information über „bestimmbare Personen", da eine indirekte Identifizierung möglich ist. Dies gilt jedoch nur, soweit der Verantwortliche über „vernünftigerweise" zu berück-

sichtigende Mittel verfügt. Diese Voraussetzung ist häufig gegeben.

Zwar kann sich ein Webseitenbetreiber nicht direkt an den Internet-Provider wenden, um zu erfahren, welchem Nutzer eine bestimmte IP-Adresse zugeordnet ist. Allerdings kann sich der Diensteanbieter bei Cyber-Attacken an die Ermittlungsbehörden wenden. Diese können in der Regel mit gerichtlicher Hilfe wiederum das „Zusatzwissen" des Internet-Providers anfordern und die IP-Adresse dann einer natürlichen Person zuordnen. Damit entschied der EuGH auch den Streit zwischen dem absoluten und relativen Personenbezug zu Gunsten des relativen Personenbezugs.

Somit ist es für die Feststellung des Personenbezugs nicht erforderlich, dass der Diensteanbieter selbst über das Wissen verfügt, um eine Person hinreichend zu bestimmen. Allerdings ist nicht jedes Zusatzwissen irgendeines Dritten zu berücksichtigen, sondern nur das, welches dem Verantwortlichen vernünftigerweise zur Verfügung steht. Der EuGH spricht sich also insgesamt zwar für den relativen Personenbezug von IP-Adressen aus, lässt jedoch in der Praxis eine große Auslegungsbandbreite offen.

Ausblick zur DS-GVO:
Die zentrale Entscheidung des EuGH wird unserer Einschätzung nach auch für die kommenden Jahre relevant bleiben. Grundlage für die Entscheidung war die Definition des personenbezogenen Datums in der Datenschutz-Richtlinie (RL 95/46). Die Definition der Richtlinie entspricht dabei nahezu dem Wortlaut der DS-GVO. Daher gehen wir davon aus, dass der relative Personenbezug auch für die DS-GVO maßgeblich ist.

7.3 Medienprivileg im Internet

Inwieweit das Medienprivileg im Internet eröffnet ist, wenn es zu Veröffentlichungen von Meinungen kommt, ist abhängig vom jeweiligen Einzelfall.

Mehrfach haben sich Betroffene, über die Dritte sich im (öffentlich zugänglichen) Bereich des Internets geäußert haben, an uns gewandt und gefragt, ob dies datenschutzrechtlich zulässig und hinzunehmen sei. Mehrfach haben die Betroffenen auch unsere Unterstützung bei der Löschung der Veröffentlichungen erbeten.

Die Bandbreite an Telemediendiensten, in denen es zu solchen Veröffentlichungen gekommen ist, war dabei vielfältig. Oftmals schreiben sich Personen im Rahmen einer eigenen Homepage oder Blogs ihren Frust über Mitmenschen und negative Erfahrungen mit Behörden oder kommunalen Mandatsträgern von der Seele und wollen die ganze Welt an ihrem Schicksal teilhaben lassen. Auch möchten Bürgerinitiativen via Internet die Öffentlichkeit gezielt auf bestimmte Anliegen aufmerksam machen und prangern nicht selten in diesem Zusammenhang das Verhalten einzelner namentlich genannter Personen an.

Aus datenschutzrechtlicher Sicht stellt sich in jedem Einzelfall für uns die Frage, ob der konkrete Telemediendienst für sich das sog. „Medienprivileg" des § 41 Abs. 1 BDSG beanspruchen kann, mit der Folge, dass er dann von den Bestimmungen des BDSG weitgehend freigestellt ist, wir als Aufsichtsbehörde nicht mehr zuständig wären und betroffene Personen die Frage einer vermeintlichen Beeinträchtigung ihres Persönlichkeitsrechts zivilrechtlich klären lassen müssten. Dabei ist es nicht immer einfach, eindeutig zu erkennen, ob der für den Telemediendienst Verantwortliche als „Unternehmen und Hilfsunternehmen der Presse" anzusehen ist oder er einer „journalistisch-redaktionellen Tätigkeit" nachkommt. Wie auch eine Rückfrage beim Deutschen Presserat be-

stätigt hat – der ebenfalls in seiner täglichen Arbeit mit diesen Fragen zu kämpfen hat – ist eine pauschale Antwort hierzu nicht möglich, so dass jeder Einzelfall gesondert zu betrachten ist.

Unstrittig ist, dass ein Diensteanbieter beispielsweise nicht dadurch zu einem Presseunternehmen werden kann, indem er sich selbst ohne weiteren Nachweis als Journalist, Redakteur usw. bezeichnet. Ferner kann auch die schlichte Veröffentlichung von behördlichem Schriftverkehr nicht als journalistisch-redaktionelle Tätigkeit gesehen werden. Andernfalls könnte sich letztlich jeder Verein, jedes Unternehmen und jede Privatperson, die über eine eigene Homepage die Öffentlichkeit über die eigenen Aktivitäten und Erfahrungen informiert, auf das Medienprivileg berufen. Vielmehr müssen Indizien, wie beispielsweise der Besitz eines Presseausweises oder die Mitgliedschaft in einem Presseverband den Status eines „Journalisten" stützen und muss die Aufbereitung des Internetauftritts ein Mindestmaß an journalistisch-redaktioneller Bearbeitung aufweisen.

In einem Gerichtsverfahren, bei dem wir beteiligt waren, hat beispielsweise das Bundesverwaltungsgericht in seinem Beschluss vom 29. Oktober 2015 (Az.: 1 B 32.15) festgestellt, dass es für die Annahme eines Presseunternehmens nicht genügt,

> *„wenn der Vorstand einer Wählervereinigung seine allerdings von der Meinungsäußerungsfreiheit geschützten Beiträge zur Unterrichtung der Öffentlichkeit und zur öffentlichen Auseinandersetzung auf der Website veröffentlicht. Denn es fehlt insoweit an einer eigenständigen, vom sonstigen Handeln des Vorstandes abgegrenzten, autonomen redaktionellen Stelle innerhalb des Vereins, die diese Informationsbearbeitung zu einer Verarbeitung „allein" bzw. „ausschließlich" zu eigenen journalistischen Zwecken werden lassen könnte. Das Berufungsgericht nimmt zu Recht an, dass das sog. Medienprivileg kein allgemeines Meinungsprivileg enthält. (…) Insbesondere folgt aus dem Umstand, dass journalistische Tätigkeiten nicht Medienunternehmen vorbehalten sind, nicht, dass jegliche Verbreitung und Informationen, Meinungen oder Ideen in der Öffentlichkeit „allein zu journalistischen Zwecken" erfolgt."*

Somit wird es auch künftig nur Einzelfallentscheidungen zu Fragen der Anwendbarkeit des „Medienprivilegs" geben können.

7.4 Löschung von Suchmaschinenergebnissen

Betreiber von Suchmaschinen bieten mittlerweile Online-Formulare an, um die Auffindbarkeit von bestimmten Suchtreffern zu verhindern.

Wir erhielten Anfragen von besorgten Bürgern, die bei der Microsoft Corporation als Betreiberin der Suchmaschine Bing einen Antrag auf Löschung von Suchmaschinenergebnissen gestellt haben, dieser aber bislang ohne Reaktion geblieben ist. In diesen Fällen, in denen bereits eine Antragstellung beim Suchmaschinenbetreiber erfolgt ist, lässt sich regelmäßig durch uns der aktuelle Sachstand herausfinden und dem Bürger weiter helfen, sofern uns die notwendigen Unterlagen durch den Antragsteller, wie z. B. Antrag und Bearbeitungsnummer beim Suchmaschinenbetreiber, zur Verfügung gestellt werden können.

Sofern noch kein entsprechender Antrag durch den Betroffenen gestellt worden ist, machen wir unter Bezugnahme auf die Entscheidung des Europäischen Gerichtshofs (EuGH) vom 13. Mai 2014 (Az.: C-131/12) auf die Möglichkeit aufmerksam, im Einzelfall Suchergebnisse löschen zu lassen. Der EuGH hat den Suchmaschinenbetreiber Google verpflichtet, Suchergebnisse, die bei einer Suche mit dem Namen

einer Person angezeigt werden, dann zu löschen, wenn das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten das berechtigte Informationsinteresse von Internetnutzern überwiegt.

Die größten Suchmaschinenbetreiber stellen für Löschanträge Online-Formulare zur Verfügung. In einem „Info-Kompakt"-Blatt stellen wir für interessierte Bürger eine einseitige Übersicht zu diesem Thema mit den aktuellen Links zu den Formularen von Bing, Google und Yahoo bereit.

Link:
www.lda.bayern.de/media/info_kompakt_suchmaschine.pdf

Soweit ein Löschantrag abgelehnt oder auf einen solchen nicht reagiert wird, kann sich jeder Antragsteller an die jeweils zuständige Aufsichtsbehörde wenden. Für die Suchmaschine Google ist dies der Hamburgische Beauftragte für den Datenschutz und Informationsfreiheit, für die Suchmaschine Yahoo! der Yahoo! EMEA Limited die irische Datenschutzaufsichtsbehörde. Für Deutschland sind wir für die Suchmaschine Bing der Microsoft Corporation Ansprechpartner.

7.5 Daten von Behördenmitarbeitern im Internet

Mitarbeiter von Behörden müssen es nicht hinnehmen, dass dienstlicher Schriftverkehr mit ihren personenbezogenen Daten im Internet veröffentlicht werden.

In den vergangenen Jahren ist ein deutlicher Anstieg der Beschwerden von Behördenmitarbeitern – oder deren Dienstherren – zu Sachverhalten zu verzeichnen, in denen dienstliche Schreiben, die naturgemäß personenbezogene Daten des jeweiligen Mitarbeiters, wie beispielsweise Name, namensbezogene E-Mail-Adresse oder Telefonnummer enthalten, nicht anonymisiert im frei zugänglichen Bereich des Internets veröffentlicht werden. Dies reicht vom publizierten Bußgeldbescheid auf Facebook bis hin zur Wiedergabe des ungekürzten E-Mail-Verkehrs mit der Behörde auf einer eigenen Homepage. Teils geschieht dies – wie sich in Gesprächen herausgestellt hat – gedankenlos und ohne Unrechtsbewusstsein, teils offensichtlich aber ganz bewusst, um dem Unmut über eine Behördenentscheidung in der Person des Sachbearbeiters „Gestalt zu verleihen".

Wir haben bereits in unserem 5. Tätigkeitsbericht für die Jahre 2011/2012 unter Punkt 4.1.4 die datenschutzrechtlichen Aspekte bei diesem Thema beleuchtet. Im aktuellen Berichtszeitraum endete durch einen Beschluss des Bundesverwaltungsgerichts (BVerwG, Beschluss vom 29.10.2015, Az.: 1 B 32.15) ein Verfahren, in dem wir einem Webseitenbetreiber untersagt hatten, die E-Mail-Kommunikation mit einer Behörde unter Verwendung der Kommunikationsdaten der behördlichen Mitarbeiterin ins Internet zu stellen. Im Rahmen dieser zu beantwortenden Frage war von entscheidender Bedeutung, ob in dem konkret zu entscheidenden Fall der Webseitenbetreiber sich auf das sog. Medienprivileg berufen konnte (siehe dazu auch 7.3). Dazu hatte der Bayer. Verwaltungsgerichtshof in seinem Urteil vom 25. März 2015 (Az 5 B 14.2164) festgestellt, dass Äußerungen von Mitarbeitern einer Behörde grundsätzlich immer der entsprechenden Behörde zuzurechnen sind, weil diese im Auftrag der Behörde handeln. Für eine Veröffentlichung des Namens oder der Kontaktdaten eines Behördenmitarbeiters muss der Veröffentlichende gewichtige Gründe für geltend gemachte berechtigte Interessen anführen können, die in der vorzunehmenden Abwägung die schutzwürdigen Interessen des betroffenen Behördenmitarbeiters, seine personenbezogenen Daten nicht weltweit abrufbar im Internet zu sehen, überwiegen müssen. In aller Regel fehlt es an einem solchen (überwiegenden) berechtigten Interesse. Auch stellen die personenbe-

zogenen Daten des einzelnen Mitarbeiters ein nicht erhebliches Detail dar, das meist problemlos ohne sachlichen Informationsverlust weggelassen werden kann. Durch den o. g. Beschluss des Bundesverwaltungsgerichts wurde die Revision nicht zugelassen und das Verfahren beendet.

In vergleichbaren Fällen haben die Webseitenbetreiber eingesehen, dass sie ihr Anliegen, die Öffentlichkeit über einen bestimmten Sachverhalt zu informieren, in gleicher Weise verfolgen können, wenn sie die personenbezogenen Daten der einzelnen Behördenmitarbeiter in behördlichen Schreiben anonymisieren oder in ihren Schilderungen von der konkreten Namensnennung des Behördenmitarbeiters absehen und dafür allgemeine Behördenbezeichnungen wählen (z. B. „Das Jugendamt", „Das Landratsamt" usw.). Weitere Anordnungen waren nicht nötig.

7.6 Einsatz von Google Analytics nach der Safe Harbor-Entscheidung

Ein Abschluss neuer ADV-Verträge ist nicht zwingend erforderlich im Hinblick auf die Datenübermittlung in die USA.

Die bisherigen ADV-Verträge für den Einsatz von Google Analytics enthielten die Formulierung, dass die Kürzung der IP-Adressen, sofern die Anonymisierungsfunktion korrekt implementiert wurde, auf Servern innerhalb von Mitgliedsstaaten der EU oder des EWR erfolgt. Erst im Anschluss werden die Daten in die USA übermittelt. In Ausnahmefällen könne es jedoch zu einer Übermittlung der ungekürzten IP-Adresse kommen. Soweit ein solcher Ausnahmefall vorlag, war die Datenübermittlung rechtmäßig. Die Datenübermittlung konnte auf die Safe-Harbor-Zertifizierung von Google gestützt werden.

Nach der Safe-Harbor-Entscheidung des EuGH vom 6. Oktober 2015 (Az C-362/14) wurde die Angemessenheitsentscheidung der EU-Kommission für ungültig erklärt, sodass die Datenübermittlung in die USA nicht mehr auf Grundlage von Safe Harbor möglich war. Daraufhin stellte Google die hierfür erforderlichen ADV-Verträge um. Die neuen ADV-Verträge für den Einsatz von Google Analytics enthalten keinen Hinweis mehr, auf welche Rechtsgrundlage eine Datenübermittlung in die USA gestützt wird. Google empfiehlt den Abschluss dieser neuen ADV-Verträge.

Wir fordern keinen Neuabschluss bestehender ADV-Verträge hierzu. Seit 26. September 2016 ist Google nach dem Privacy Shield zertifiziert, sodass die materiellen Voraussetzungen für eine rechtmäßige Übermittlung in die USA vorliegen (zu Safe Harbor und Privacy Shield siehe auch 14.2).

Ausblick zur DS-GVO:
Auch künftig ist es nicht erforderlich, dass der ADV-Vertrag einen Hinweis enthält, auf welche Rechtsgrundlage die Datenübermittlung an Drittländer gestützt wird. Dies entbindet den Verantwortlichen jedoch nicht von der allgemeinen Pflicht gem. Art. 5 Abs. 2 DS-GVO nachzuweisen zu können, dass der Einsatz von Analysetools zur Reichweitenmessung die Anforderungen der DS-GVO erfüllt.

7.7 Veröffentlichung von Fotos im Internet

Die Veröffentlichung von Fotos im Internet bleibt ein datenschutzrechtlicher „Dauerbrenner".

Es ist wahrlich kein Einzelfall, dass Personen sich hilfesuchend an uns wenden, weil sie Fotos, auf denen sie erkennbar abgebildet sind, zufällig in einem Internetauftritt finden und diese Fotos gelöscht haben möchten. Die

Thematik ist seit Jahren ein „Dauerbrenner" in unserer Arbeit, so dass in nahezu jedem unserer bislang erschienenen Tätigkeitsberichte darüber berichtet wurde. Das Interesse und die Fallzahlen solcher Sachverhalte sind jedoch ungebrochen hoch, weshalb es uns wert erscheint, dieses Thema erneut aufzugreifen.

Grundsätzlich bedarf das Veröffentlichen von Fotos von Personen im Internet der Einwilligung der abgebildeten Personen. Einschlägige Rechtsvorschriften sind die §§ 22 und 23 Kunsturheberrechtsgesetz (KUG). Nach § 22 Satz 1 KUG dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Ausnahmen von diesem Grundsatz werden in § 23 KunstUrhG geregelt. Danach dürfen ohne Einwilligung verbreitet und zur Schau gestellt werden,

- Bildnisse aus dem Bereich der Zeitgeschichte,
- Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen,
- Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben oder
- Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem höheren Interesse der Kunst dient,

sofern nicht ein berechtigtes Interesse des Abgebildeten verletzt wird.

Anhand von zwei konkreten Beschwerden, die wir im Berichtszeitraum erhalten haben, möchten wir verdeutlichen, wo im Einzelfall die Schwierigkeiten bei der Anwendung dieser Vorschriften liegen können:

- Im ersten Fall wurde auf der Homepage einer Arztpraxis mit einem Foto das aus fünf Personen bestehende Praxisteam vorgestellt. Da eine Person zum Zeitpunkt der Eingabe bereits seit längerer Zeit nicht mehr in dieser Arztpraxis tätig war, wurde eine Löschung des Fotos gefordert.
- Im anderen Fall war ein Bild Gegenstand einer Beschwerde, das ebenfalls fünf Personen zeigte. Es wandte sich ein Beschwerdeführer an uns, der im Rahmen eines Jugend-Fußballturniers als Schiedsrichter fungierte. Auf der Homepage eines der teilnehmenden Vereine wurde ein Foto veröffentlicht, das neben zwei Sponsoren des stattgefundenen Fußballturniers das Schiedsrichtergespann zeigt, welches das Endspiel dieses Turniers geleitet hat. Während der Eingabeführer nicht in die Richtung des Fotografen blickt, ist es offensichtlich, dass die vier weiteren Personen in die Kamera blicken und sich zumindest des Fotografiertwerdens bewusst sind.

Der zuerst geschilderte Eingabefall erscheint in seiner rechtlichen Bewertung eindeutig. Das Team der Arztpraxis war sich offensichtlich der Tatsache bewusst, dass ein Foto angefertigt wird und wohl auch des Zwecks, nämlich einer Veröffentlichung auf der Homepage der Arztpraxis. Die Aufnahme und die Veröffentlichung des Fotos erfolgten aufgrund einer Einwilligung der fotografierten Personen, da ein Ausnahmetatbestand des § 23 KunstUrhG nicht einschlägig war. Nachdem eine der Personen nach dem Ausscheiden aus der Praxis ihre Einwilligung widerrufen hat, war das besagte Foto zu löschen bzw. zu überarbeiten. Dieser Forderung ist der Betreiber der Arztpraxis nach unserer Intervention nachgekommen und hat das Bild durch eine aktualisierte Fotografie seines Teams ersetzt.

Im zweiten Fall haben wir allerdings einen Grenzfall erkannt. Für Fotos von einer öffentlichen Sportveranstaltung kann grundsätzlich die Ausnahme des § 23 Abs. 1 Nr. 3 KUG („Bilder von Versammlungen, Aufzügen und ähnli-

chen Vorgängen, an denen die dargestellten Personen teilgenommen haben") greifen. Voraussetzung ist, dass der Vorgang in der Öffentlichkeit stattgefunden hat und die Darstellung des Ereignisses im Vordergrund steht. Liegt der Fokus eines Bildes nicht auf der Veranstaltung als solches, sondern auf einzelnen Personen der Veranstaltung, greift die Privilegierung des § 23 Abs. 1 Nr. 3 KUG dagegen regelmäßig nicht. Im konkreten Beschwerdefall haben wir die Auffassung vertreten, dass die Veröffentlichung des Fotos auf die Rechtsgrundlage des § 23 Abs. 1 Nr. 3 KUG gestützt werden kann. Das Foto zeigt zwei Sponsoren des stattgefundenen Fußballturniers und das Schiedsrichtergespann. Im Vordergrund des Bildes steht damit nicht eine Einzelperson, sondern die Gruppe der Sponsoren und die Gruppe der Schiedsrichter eines in der Öffentlichkeit stattgefundenen Fußball-Turniers. Neben den Feldspielern gehören auch diese Personengruppen zum erweiterten Umfeld eines Fußballturniers und geben den Charakter einer öffentlichen Veranstaltung wieder. Hierzu dürften neben Gruppenaufnahmen von Spielern ebenso auch Gruppenaufnahmen von Schiedsrichtern, Sponsoren, freiwilligen Helfern oder auch Zuschauern zählen. Es bleibt aber eine Einzelfallentscheidung, ob ein konkretes Bild dahingehend aufgefasst werden kann, dass es auf eine Einzelperson ausgerichtet ist oder vielmehr den Charakter einer öffentlichen Veranstaltung wiedergibt.

Um Unklarheiten und Streitigkeiten wegen unterschiedlicher Auffassung zu vermeiden, kann die Empfehlung nur lauten, sich vor einer Veröffentlichung von Fotos im Zweifelsfall der Einwilligung betroffener Personen zu versichern.

Um zu dem oben genannten Dauerbrenner konkretere Auskünfte geben und evtl. einen kurzen Leitfaden zu erstellen zu können, wie man es richtig macht, haben wir zu diesem Thema eine größere anlasslose Prüfung bei Sportvereinen durchgeführt (siehe 3.14).

7.8 Privatinsolvenzen im Internet

Im Praxisvollzug gegen unrechtmäßige Veröffentlichung von Privatinsolvenzen im Internet stößt auch die Datenschutzaufsicht an ihre Grenzen.

Betroffene, die eine Privatinsolvenz hinter sich hatten, haben sich bei uns darüber beschwert, dass man über die Suche nach ihrem Namen in gängigen Suchmaschinen auf ein spezielles Internetangebot zur Veröffentlichung von Privatinsolvenzen stößt. Auf dieser Webseite war ein Impressum zu finden, das eine Limited-Gesellschaft mit Sitz in München als verantwortliche Stelle ausgewiesen hat. Allerdings konnten unsere Schreiben nicht zugestellt werden – auch blieben Kontaktversuche über die im Impressum angegebene E-Mail-Adresse erfolglos. Die in der Anbieterkennzeichnung angegebene Telefonnummer war nicht funktionsfähig und die im Wege der Amtshilfe durch die von der Polizei vorgenommenen Ermittlungen vor Ort haben ergeben, dass unter der besagten Adresse kein solches Unternehmen zu finden ist.

Unsere weitergehenden technischen Überprüfungen haben nach kurzer Zeit ergeben, dass die Daten offenbar gelöscht wurden und auf dem vormals ermittelten Server mit Standort außerhalb Bayerns nicht mehr zugänglich sind. Weitere Anhaltspunkte für unsere örtliche Zuständigkeit konnten nicht gefunden werden, so dass den Betroffenen nur empfohlen werden konnte, bei den Suchmaschinenbetreibern eine zügigere Löschung des Cache zu beantragen, damit die Suchtreffer bei neuen Suchabfragen nicht mehr erscheinen.

Die datenschutzrechtlichen Rahmenbedingungen für eine Veröffentlichung von Privatinsolvenzdaten im Internet haben wir bereits in unserem 4. Tätigkeitsbericht 2009/2010 unter Punkt 4.1.5 vorgestellt. Danach stehen einer solchen Übermittlung personenbezogener Daten regelmäßig die schutzwürdigen Interes-

sen der betroffenen Personen entgegen. Zu einer anderen Bewertung kommen wir nur innerhalb der ersten zwei Wochen der öffentlichen Bekanntmachung der Privatinsolvenz, da innerhalb dieses Zeitraums die Privatinsolvenzdaten ungehindert online abrufbar und damit allgemein zugänglich sind. In diesem Fall ist eine Internetveröffentlichung nur dann unzulässig, wenn das entgegenstehende Interesse des Betroffenen offensichtlich überwiegt, was in aller Regel jedoch nicht der Fall ist.

In den vergangenen Monaten konnte beobachtet werden, dass das fragwürdige Internetangebot mit den veröffentlichten personenbezogenen Daten zu Privatinsolvenzen mehrfach auf anderslautende Domains umgezogen ist und sich auch die dort genannten verantwortlichen Stellen namentlich regelmäßig geändert haben. Sämtliche Informationen deuten derzeit darauf hin, dass weder die verantwortliche Stelle ihren Sitz in Deutschland hat, noch der Server, auf dem das Internetangebot gehostet wird. Somit müssen auch wir erkennen, dass die Datenschutzaufsicht mit deren Möglichkeit, in ihrem Persönlichkeitsrecht verletzte Bürger zu unterstützen, manchmal an ihre Grenzen stößt.

8

Rechtsanwälte

8 Rechtsanwälte und Rechtsstreitigkeiten

8.1 Einbringung personenbezogener Daten zur Verteidigung in einen Zivilprozess

Ein ehemaliger Lehrer, der von einem ehemaligen Schüler auf Schadensersatz verklagt wurde, darf grundsätzlich zu seiner Verteidigung Unterlagen mit personenbezogenen Daten des Schülers aus der Schülerakte in den Prozess einführen.

Ein ehemaliger Schüler beschwerte sich bei uns darüber, dass in einem zwischen ihm (als Kläger) und seinem ehemaligen Lehrer (als Beklagtem) bei einem Zivilgericht anhängigen Rechtsstreit der ehemalige Lehrer Dokumente aus der Schülerakte des Klägers zu Beweiszwecken dem Gericht vorgelegt habe.

Im Vorfeld hatte der Schüler eine Beschwerde bei dem für die öffentliche Schule zuständigen Bayerischen Landesbeauftragten für Datenschutz (BayLfD) eingelegt, mit der er die Aushändigung von Dokumenten aus der Schülerakte durch die Schule an den Lehrer moniert hatte. Nachdem der BayLfD ihm mitgeteilt hatte, dass dieser Vorgang nicht von vornherein und in jedem Falle als datenschutzrechtlich unzulässig anzusehen sei, kritisierte er in der an uns gerichteten Beschwerde nun die Einführung der Dokumente durch den Lehrer als Privatperson, für den wir als Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich zuständig sind, in den Zivilprozess.

Wir haben diese Einführung der Dokumente in den Zivilprozess als datenschutzrechtlich zulässig bewertet, weil es den berechtigten Interessen des Beklagten entspricht, sich gegen die Vorwürfe, die der Schüler im Rechtsstreit gegen ihn erhoben hatte, wehren zu können. Die Vorwürfe betrafen Vorgänge aus der Zeit, in der der Kläger Schüler in einer Klasse war, die der Beklagte unterrichtete. Es kann als berechtigtes Interesse des ehemaligen Lehrers anerkannt werden, etwaige Unterlagen, über die er (nach Aushändigung durch die Schule) verfügte, zur Untermauerung seiner Rechtsposition dem Gericht zur Verfügung zu stellen. Ohnehin hätte der Lehrer die gegenständlichen Unterlagen grundsätzlich auch durch entsprechende Beweisanträge als Beweismittel in das zivilgerichtliche Verfahren einführen können. Demgegenüber hat das – naturgemäß entgegenstehende – Interesse des Schülers am Unterbleiben einer solchen Einbringung bei der Interessenabwägung nach § 28 Abs. 1 S. 1 Nr. 2 BDSG zurückzustehen, da der Schüler keine schutzwürdige, legitime Erwartung daran haben kann, dass sein Prozessgegner auf die Vorlage derartiger Beweismittel im Prozess verzichtet. Anders wäre es allenfalls dann, wenn die in Rede stehenden Unterlagen unter keinem Gesichtspunkt in einem Zusammenhang mit dem Gegenstand des Klageverfahrens stünden, was aber vorliegend nicht ersichtlich war. Vielmehr betrafen die Unterlagen offenbar Angelegenheiten, die den Gegenstand der vom Schüler gegen den Lehrer vor Gericht erhobenen Vorwürfe bildeten.

Es entsprach daher dem legitimen Interesse des Lehrers, die bei der Schule vorhandenen Unterlagen über diese Angelegenheiten zur Klärung der gegen ihn erhobenen Vorwürfe in den Rechtsstreit einzubringen.

8.2 Fax an vermutete anwaltliche Vertreterin über zentralen Faxeingang einer Behörde

Die Versendung eines Telefaxes mit personenbezogenen Daten an eine Behörde, die unter keinem Gesichtspunkt für die betreffende Angelegenheit zuständig ist, stellt eine unzulässige Übermittlung personenbezogener Daten dar.

Ein Beschwerdeführer schilderte eine ungewöhnliche – und im Ergebnis von uns als unzulässig bewertete – Versendung eines Schriftsatzes durch einen früheren vom Beschwerdeführer mandatierten Rechtsanwalt. Vorausgegangen war ein Streit zwischen dem Beschwerdeführer und seinem Rechtsanwalt über das anwaltliche Honorar aus einem Mandat.

Der Anwalt verfasste einen Schriftsatz, in dem er den Mandanten zur Zahlung einer bestimmten Summe aufforderte, die ihm nach seiner Auffassung als Honorar zustand. Diesen Schriftsatz versandte er als Fax an die Lebensgefährtin seines früheren Mandanten, eine Rechtsanwältin, die den Mandanten – wie der Anwalt wusste – früher gelegentlich in anderen Angelegenheiten anwaltlich vertreten hatte. Der Anwalt teilte in dem Schreiben mit, dass er vor diesem Hintergrund annehme, dass die Anwältin auch hinsichtlich der Streitigkeit über das Honorar ihren Lebensgefährten anwaltlich vertrete. Das Fax versandte der Rechtsanwalt an die zentrale Faxnummer einer Behörde, bei der die Lebensgefährtin – wie der Anwalt ebenfalls wusste – inzwischen arbeitete. Der Mandant beschwerte sich darüber bei uns.

Nach unserer Bewertung hatte der Anwalt vorliegend in zweierlei Hinsicht datenschutzrechtlich unzulässig gehandelt. Zum einen durfte er nicht schlicht davon ausgehen, dass die Rechtsanwältin ihren Lebensgefährten ohne weiteres auch in der vorliegenden Honorarrechtsstreitigkeit vertritt. Weder der Mandant noch seine Lebensgefährtin hatten dem Rechtsanwalt eine solche anwaltliche Vertretung angezeigt. Schon aus diesem Grund stellte daher die vom Rechtsanwalt veranlasste Übermittlung des Schriftsatzes an die Lebensgefährtin des früheren Mandanten eine datenschutzrechtlich unzulässige Übermittlung personenbezogener Daten dar.

Darüber hinaus war aber auch die Versendung des Schriftsatzes per Fax an die zentrale Faxnummer der Behörde, in der die Lebensgefährtin inzwischen arbeitete, eine unzulässige Übermittlung personenbezogener Daten. Bei einem zentralen Faxeingang einer Behörde kann – wie auch vorliegend – ein mehr oder weniger großer Kreis von dort beschäftigten Personen Kenntnis von dem Inhalt des Faxschreibens erhalten. Das vom Anwalt dorthin versandte Fax betraf aber ausschließlich die Honorarrechtstreitigkeit und damit eine Angelegenheit, die nicht mit den gesetzlich festgelegten Aufgaben der betreffenden Behörde im Zusammenhang stand. Der Anwalt hätte die in seinem Schreiben enthaltenen personenbezogenen Daten zu seinem Mandanten, d. h. die Angaben zum Sachverhalt, der dem Honorarrechtsstreit zu Grunde lagen, daher nicht an den Faxeingang der Behörde versenden dürfen. Dass der Anwalt davon ausging bzw. sogar sicher wusste, dass die Rechtsanwältin inzwischen bei der Behörde beschäftigt war, rechtfertigt es nicht, dieses in keinem Zusammenhang mit der Zuständigkeit der Behörde stehende Anwaltsschreiben den bei der Behörde beschäftigten Personen zur Kenntnis zu bringen. Die Faxnummer der Behörde wird bestimmungsgemäß nur für die Entgegennahme von Informationen im Rahmen solcher Angelegenheiten zur Verfügung gestellt, die mit den gesetzlich festgelegten Zuständigkeiten und Aufgaben der Behörde zusammenhängen.

Im Übrigen stellte sich – datenschutzrechtlich irrelevant – heraus, dass die Anwältin seit Aufnahme ihrer Beschäftigung bei der Behörde über keine anwaltliche Zulassung mehr verfügte und schon aus diesem Grunde ihren Lebensgefährten in der Honorarsache nicht anwaltlich vertreten konnte. Wir haben die unzulässige Übermittlung personenbezogener Daten im Rahmen eines Bußgeldverfahrens geahndet.

8.3 Unzulässige Kfz-Halterabfrage durch Rechtsanwältin

Die Beschaffung von Fahrzeug- und Halterdaten per Registerauskunft nach § 39 StVG ist nur zu den im Gesetz genannten Zwecken zulässig. Die gesetzlich abschließend geregelten Zwecke setzen auch einer „Beweisbeschaffung" für mögliche Rechtsstreitigkeiten Grenzen und müssen daher auch von Rechtsanwälten beachtet werden.

Eine Rechtsanwältin holte bei der Kfz-Zulassungsstelle eine sog. einfache Registerauskunft nach § 39 Abs. 1 StVG (Halterabfrage) zu einem amtlichen Fahrzeugkennzeichen ein, obwohl die Voraussetzungen für die Einholung einer solchen Auskunft nicht erfüllt waren. Das Fahrzeug wurde regelmäßig von der geschiedenen Ehefrau eines Mandanten der Rechtsanwältin gefahren; dies hatte der Mandant beobachtet. Die Registerauskunft ergab, dass Fahrzeughalter der neue Lebensgefährte der geschiedenen Ehefrau des Mandanten war. Die Rechtsanwältin verwendete die erlangte Information über die Person des Halters in einem anhängigen familiengerichtlichen Unterhaltsrechtsstreit, in dem sie als anwaltliche Vertreterin des geschiedenen Ehemannes mandatiert war. Darüber beschwerte sich der Fahrzeughalter, dem seine Lebensgefährtin über die Einbringung dieser Information in den Unterhaltsrechtsstreit berichtet hatte, bei uns.

Im Rahmen der von uns zunächst unternommenen datenschutzaufsichtlichen Prüfung gab die Rechtsanwältin an, sie habe die Halterauskunft eingeholt, weil das Fahrzeug wiederholt im Halteverbot gestanden habe; dies habe ihr Mandant fotografisch festgehalten. Die Registerauskunft sei daher „zum Zwecke der Verfolgung von Parkverstößen" eingeholt worden.

Die Einholung der Registerauskunft war dennoch rechtswidrig, da keiner der in § 39 Abs. 1 bis 3 StVG abschließend geregelten Gründe für die Einholung einer Registerauskunft durch Privatpersonen vorlag. § 39 Abs. 1 und Abs. 2 StVG erlauben die Übermittlung der dort bezeichneten Fahrzeug- bzw. Halterdaten nur, wenn der Empfänger darlegt, dass er die Daten „zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt". Der von der Rechtsanwältin gegenüber uns als Abfragegrund genannte „Parkverstoß" ist zwar ein Lebenssachverhalt, der mit dem Straßenverkehr im Zusammenhang steht. Allerdings machte die Anwältin nicht geltend und es war auch sonst nicht erkennbar, dass die Abfrage – wie in § 39 Abs. 1 StVG vorausgesetzt – erfolgt war, um mit der Teilnahme am Straßenverkehr im Zusammenhang stehende Rechtsansprüche geltend zu machen, zu sichern, zu vollstrecken, zu befriedigen oder abzuwehren oder um wegen im Straßenverkehr begangener Verstöße eine Privatklage zu erheben.

Da keiner der in § 39 Abs. 3 StVG geregelten Abfragegründe vorlag, war die Abfrage als unbefugte Erhebung personenbezogener Daten, die nicht allgemein zugänglich sind, einzustufen und erfüllte damit den Tatbestand einer Ordnungswidrigkeit nach § 43 Abs. 2 Nr. 1 BDSG. Es bestand nach Lage der Dinge der – unausgeräumte – Verdacht, dass die Rechtsanwältin die Auskunft von vornherein eingeholt hatte, um die dadurch erlangte Information über die Identität des Fahrzeughalters in den anhängigen familiengerichtlichen Unterhaltsrechtsstreit einzubringen, bei dem sie als anwaltliche Vertreterin des geschiedenen Ehemannes agierte.

Wir haben den Verstoß mit einer Geldbuße geahndet, die nach Einlegung eines Einspruchs durch das Amtsgericht dem Grunde nach bestätigt wurde und inzwischen rechtskräftig ist.

9

Versicherungswirtschaft

9 Versicherungswirtschaft

9.1 Telematik-Tarife in der Kfz-Versicherung

Wir haben uns mit Ausgestaltungen von Kfz-Versicherungen beschäftigt, bei denen der Versicherte Daten über sein Fahrverhalten zur Berechnung eines Bonus preisgibt, und mitgewirkt, Kriterien zu entwickelt, wann dies zulässig ist.

Mehrere Versicherer bieten inzwischen unterschiedliche Tarifoptionen in der Kfz-Versicherung an, die es vor allem jungen Fahrern ermöglichen sollen, durch den Nachweis eines „guten" Fahrstils Geld zu sparen. Je nach Versicherung und Tarif werden die Daten zum Fahrstil auf unterschiedliche Weise erhoben. Dazu werden entweder entsprechende Boxen im Auto fest verbaut, Messgeräte an die OBD-Schnittstelle angeschlossen oder das Smartphone des Fahrers zur Aufzeichnung eingesetzt.

Wir haben mit unterschiedlichen Versicherern in unserem Zuständigkeitsbereich die neuen Modelle besprochen und begutachtet. Rechtsgrundlage für die jeweiligen Datenerhebungen kann ein Vertrag oder eine gesonderte datenschutzrechtliche Einwilligung sein. Wichtig für die konkrete Ausgestaltung der Datenerhebung ist, dass die Versicherungsnehmer sehr transparent informiert werden. Es muss verständlich werden, in welchem Umfang und wie lange die Daten über das persönliche Fahrverhalten erhoben, verarbeitet und genutzt werden.

Typische Themen, die neben der Ausgestaltung von Einwilligung und Information immer wieder geklärt und diskutiert werden müssen, sind:

- Trennung der Versichertendaten von den Fahrdaten durch unterschiedliche Datenkreise aus Gründen der Datensparsamkeit
- Löschung und Löschfrist der Rohdaten
- Anonymisierung der Daten, falls mit ihnen die Algorithmen zur Risikobewertung weiterentwickelt werden sollen (da Bewegungsprofile sehr schwer zu anonymisieren sind)
- Technische Ausgestaltungen
- Information von Dritten, die nicht Versicherungsnehmer sind, über die stattfindende Aufzeichnung

Wir haben diese als „pay as you drive" oder „pay how you drive" bezeichneten Tarifmodelle nicht als grundsätzlich unzulässig bewertet, sondern darauf hingewiesen, dass die o.g. Punkte berücksichtigt werden müssen.

Ausblick zur DS-GVO:
Nach der DS-GVO werden die genannten Grundanforderungen an die Ausgestaltung bestehen bleiben. Im Detail wird zu klären sein, wie sich die Regelungen zu Privacy by Design und zur automatisierten Verarbeitung auswirken. Derzeit werden die Daten bei den bekannten Verfahren nicht lokal auf dem Gerät analysiert, wodurch nicht nur das Ergebnis der Bewertung an die Versicherer übermittelt wird – dies könnte dem Grundsatz von Privacy by Design widersprechen. Weiterhin erfolgt die Bewertung des Fahrverhaltens und die Berechnung des Bonus oder des Tarifs in der Regel automatisiert, sodass sich im Hinblick auf Art. 22 DS-GVO Modifikationen ergeben können

9.2 Gemeinsame Nutzung von Kontaktdaten durch Vermittler und Versicherer

Die gemeinsame Nutzung und Aktualisierung von Kontaktdaten der Versicherungsnehmer durch die betreuenden Vermittler und die Versicherer in einer Datenbank ist grundsätzlich zulässig.

Wir haben von einer Versicherungsvermittlerin den Hinweis erhalten, dass nach ihrer Auffassung die gemeinsame Datenbank zur Nutzung der Kontaktdaten bei der Versicherung, an die sie angeschlossen sei, unzulässig ausgestaltet sei.

Wir haben die Datenbank untersucht und insbesondere hinsichtlich der rechtlichen Ausgestaltung geprüft. Die Datenbank ermöglicht es der Versicherung und unterschiedlichen Vermittlern, immer mit den jeweils gemeinsam aktuell gehaltenen Kontaktdaten des Versicherten zu arbeiten. Dadurch soll eine schnelle und unkomplizierte Abwicklung der Verträge mit dem Kunden, was in vielen Fällen in dessen Interesse ist, erreicht bzw. vorangetrieben werden.

Die Einrichtung der gemeinsamen Datenbank mit Kontaktdaten hat jedoch automatisch zur Folge, dass Vermittler und Versicherer Kontaktdaten der Versicherten an den jeweils anderen übermitteln – dies lässt sich auf § 28 Abs. 1 Satz 1 Nr. 1 und 2 sowie Abs. 2 Nr. 2 a) BDSG stützen. Dennoch müssen entgegenstehende Wünsche eines Versicherten berücksichtigt werden. Wünscht ein Versicherter keine Werbung oder möchte er seine dienstliche Nummer nur einem bestimmten Vermittler zur Verfügung stellen, so ist dementsprechend dafür zu sorgen, dass diese Anforderungen umgesetzt werden können. Weiterhin muss sichergestellt sein, dass nur diejenigen Personen – insbesondere Vermittler – Zugriff auf die aktuellen Daten haben, die diese auch tatsächlich benötigen. So muss nach einem Wechsel des Vermittlers sichergestellt sein, dass der bisherige Vermittler nicht weiterhin eine Aktualisierung der Kontaktdaten erhält oder im Hintergrund pflegt.

Ausblick zur DS-GVO:
Künftig könnte es sich um sog. „gemeinsame Verantwortliche" nach Art. 26 DS-GVO handeln. Es wären danach entsprechende Vereinbarungen etwa dazu zu treffen, wer die Verpflichtungen zur Wahrnehmung der Betroffenenrechte übernimmt.

9.3 Kontaktaufnahme nach Kündigung von Versicherungsverträgen

Die sogenannte Stornobearbeitung, bei der versucht wird, den Kündigenden von seiner Kündigung abzubringen, ist grundsätzlich zulässig.

Versicherer schicken Kündigungsbestätigungen an ihre Außendienstmitarbeiter. Dies lässt sich datenschutzrechtlich auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG stützen. Die Versicherer haben ein Interesse daran, dass ihre Handelsvertreter über das Bestehen und Nichtbestehen der von vermittelten Verträge informiert sind. Ein entgegenstehendes Interesse des Betroffenen, das eine solche Übermittlung ausschließen würde, ist nicht ersichtlich.

Versicherer haben weiterhin aufgrund der handelsrechtlichen Nachbearbeitungspflichten nach § 87 a Abs. 3 HGB ein schutzwürdiges Interesse daran, den Versicherungsnehmer selbst dazu zu bewegen, an dem Vertrag festzuhalten oder dem Handelsvertreter die Möglichkeit hierzu zu geben, indem sie ihn über die bevorstehende Vertragsbeendigung informieren. Diese Datennutzung zur Nachbearbeitung durch die Versicherung selbst oder die Übermittlung an den Handelsvertreter kann eben-

falls auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG gestützt werden. Dem Interesse der Versicherung an der Nachbearbeitung wird das Interesse des Betroffenen regelmäßig nicht entgegenstehen. Anders kann dies in den Fällen sein, in denen der Betroffene ausdrücklich keinen weiteren Kontakt mit dem Außendienstmitarbeiter wünscht. Entsprechende Nachbearbeitungen von gekündigten Verträgen fallen auch nicht unter den Begriff der Werbung, sondern können unter die normale Vertragsbearbeitung gefasst werden.

9.4 Mietausfallversicherung

Bei einer Mietausfallversicherung ist die Meldung einzelner Mieter an die Versicherung sowie die Einholung von Bonitätsauskünften durch die Versicherung unzulässig.

Eine Vermietervereinigung hat sich an uns gewandt, um uns auf ein konkretes Produkt zur Mietausfallversicherung aufmerksam zu machen. Wir wurden dabei gefragt, ob dieses Produkt, durch das sich ein Vermieter gegen das Risiko des Ausfalls von Mietzahlungen versichern kann, in der vorliegenden Form datenschutzrechtlich zulässig sei.

Wir haben das Modell näher begutachtet und festgestellt, dass dabei vom Vermieter alle Mieter an die Versicherung gemeldet werden. Die Versicherung holt daraufhin für jeden Mieter eine Bonitätsauskunft ein. Ist diese Auskunft unauffällig, so entscheidet die Versicherung über die Übernahme des Mietausfallrisikos positiv. Der Mieter soll bei dieser Ausgestaltung jedoch weder darüber informiert werden, dass seine Daten an die Versicherung gemeldet werden, noch, dass dort Bonitätsauskünfte eingeholt werden. Beides halten wir für datenschutzrechtlich unzulässig. Insbesondere § 28 Abs. 1 Satz 1 Nr. 2 BDSG kann nicht als Rechtsgrundlage herangezogen werden. Dies würde voraussetzen, dass der Vermieter ein die Interessen des Mieters überwiegendes Interesse an der Datenübermittlung an die Versicherung zum Zwecke der Mietausfallversicherung hat. Die Mietausfallversicherung soll dem Vermieter den potentiellen Schaden aus nicht geleisteten Mietzahlungen ersetzen. Zur Absicherung dieses Risikos hat der Gesetzgeber zum Ausgleich der Interessen jedoch zivilrechtlich andere Instrumente vorgesehen: Es kann eine Kaution vereinbart werden (§ 551 BGB), dem Vermieter steht ein Pfandrecht an den in der Wohnung eingebrachten Gegenständen zu (§ 562 BGB) und er kann bei mehrfach nicht bezahlter Miete kündigen (§ 543 BGB).

Daraus ergibt sich nach unserer Bewertung, dass das Interesse des Mieters, nicht an unbeteiligte Dritte als Mieter gemeldet und einer Bonitätsprüfung bei einer Wirtschaftsauskunftei mit unbekannten Auswirkungen auf seinen Bonitätsscore unterzogen zu werden, die Interessen des Vermieters, die Daten der Mieter an eine Versicherung zur Vorbereitung eines Vertrages über ein Mietausfallversicherung zu melden, überwiegt. Der Vermieter hat nach der Vorstellung des Gesetzgebers bereits Sicherungsinstrumente an die Hand bekommen, die seine wirtschaftlichen Interessen gegenüber den Interessen des Mieters ausgleichen. Ein darüber hinausgehendes Sicherungsbedürfnis überwiegt zumindest nicht die Interessen des Mieters am Ausschluss einer Datenübermittlung an Dritte einschließlich einer externen Bonitätsprüfung bei Auskunfteien.

Im Rahmen der Anbahnung eines Mietverhältnisses halten wir es für denkbar, dass der Mieter freiwillig in die Datenübermittlung zum Zwecke der Mietausfallversicherung einwilligt. Zu diesem Zeitpunkt entscheiden Mieter und Vermieter noch über den Abschluss des Vertrages – es gilt die Vertragsfreiheit, beide können ihre Bedingungen für den Vertrag offen legen und sich dann jeweils frei für oder gegen den Vertragsabschluss entscheiden.

Wir haben der anfragenden Vermietervereinigung entsprechend geantwortet, die Versicherung auf unsere Auffassung hingewiesen und diese dann aufgefordert, das Produkt entsprechend anzupassen.

Ausblick zur DS-GVO:
Im Rahmen von Art. 6 Abs. 1 f) DS-GVO wäre im genannten Sachverhalt eine Interessenabwägung vorzunehmen. Deren Ergebnis würde voraussichtlich genauso ausfallen wie nach heutiger Rechtslage.

9.5 Umfang der Auskunftsobliegenheit in der Krankentagegeldversicherung

Zum Nachweis über das Einkommen vor einer Krankheit kann es sein, dass Steuerbescheide nicht ausreichen.

Im Rahmen einer Beschwerde wurde uns geschildert, eine Krankentagegeldversicherung würde über die Vorlage des Steuerbescheides hinaus weitere umfassende Auskünfte als Nachweis über das erzielte Einkommen zu der vor der Krankheit ausgeübten Tätigkeit und den einzelnen Einnahmequellen sowie eine betriebswirtschaftliche Auswertung fordern.

Bei der anschließenden Prüfung hat sich herausgestellt, dass die Einkommenssteuerbescheide tatsächlich nicht ausreichend waren, um die Leistungspflicht des Versicherers der Höhe nach ausreichend nachzuweisen. Bei der Krankentagegeldversicherung ist der Versicherer nach § 192 Abs. 5 VVG verpflichtet, den als Folge von Krankheit oder Unfall durch Arbeitsunfähigkeit verursachten Verdienstausfall durch das vereinbarte Krankentagegeld zu ersetzen. Für die Berechnung des Krankentagegeldes ist es notwendig, den Verdienstausfall, also diejenigen Einnahmen, die wegen der Krankheit nicht mehr erzielt werden können, zu ermitteln. Zum Verdienstausfall wegen Krankheit können damit beispielsweise keine weiterhin laufenden Einnahmen, wie etwa fortlaufend gezahlte Bestandsprovisionen, gehören. Aus dem Steuerbescheid ergibt sich in der Regel nur eine Zahl hinsichtlich der einzelnen Einkommensarten der Einkommenssteuer. Bei einigen Tätigkeiten können Einnahmen aus Gewerbebetrieb auch bei Krankheit weiterhin fließen. Nachdem mit dem Krankentagegeld aber lediglich der Einkommensausfall kompensiert werden soll, halten wir es für zulässig, nach der konkret ausgeübten Tätigkeit zu fragen. Dadurch kann herausgefunden werden, ob eine Tätigkeit ausgeübt wird, bei der auch bei Krankheit noch Einnahmen erzielt werden. Als nicht erforderlich sehen wir es jedoch an, eine gesamte betriebswirtschaftliche Auswertung an die Versicherung zu geben. Hier räumte die Versicherung auch einen Fehler ein. Wir haben deshalb darauf hingewiesen in der täglichen Verfahrenspraxis darauf zu achten, tatsächlich nur die erforderlichen Daten abzufragen.

9.6 Anspruch der Versicherten auf Kommunikation per E-Mail

Manche Betroffene wünschen sich Kommunikation mit ihrer Versicherung ausschließlich per (unverschlüsselter) E-Mail.

Ein Betroffener wandte sich an uns und schilderte, dass er mit seiner privaten Krankenversicherung ausschließlich per E-Mail kommunizieren wolle. Die Versicherung würde dies aber mit dem Verweis auf datenschutzrechtliche Vorgaben verweigern.

Die Frage, ob der Betroffene einen Anspruch auf eine Kommunikation über einen bestimmten Übertragungskanal (nur E-Mail, nur Post o.ä.) hat, ist zivilrechtlicher Natur und nicht Gegenstand des Datenschutzes.

Wir haben uns mit der Frage beschäftigt, unter welchen Voraussetzungen eine Kommunikation mit einer Versicherung via E-Mail datenschutzrechtlichen Anforderungen genügt. Nach § 9 BDSG hat eine Versicherung diejenigen technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Anforderungen des BDSG zu gewährleisten. Darunter fällt hinsichtlich des genannten Sachverhalts insbesondere § 9 Satz 1 BDSG i. V. m. Nr. 4 der Anlage zu § 9 Satz 1 BDSG, wonach die verantwortliche Stelle Maßnahmen treffen muss, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind, zu gewährleisten, 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. Hierzu gehört auch der Versand von Daten per E-Mail.

Klassische (inhaltlich) unverschlüsselte E-Mails können viele Gewährleistungsziele wie Vertraulichkeit, Authentifizierung, Verbindlichkeit und Integrität nicht erfüllen. Die konkret zu treffenden Maßnahmen richten sich nach dem Stand der Technik und dem Schutzbedarf der Daten. In diesem Fall sind im Zweifel Daten mit hohem Schutzbedarf betroffen. Gerade bei der Krankenversicherung können Daten zur Gesundheit anfallen, die auch vom Gesetz als besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) besonders geschützt sind. Weiterhin unterliegen die Mitarbeiter von privaten Kranken-, Unfall- und Lebensversicherungen auch der strafrechtlich geschützten Schweigepflicht nach § 203 Strafgesetzbuch (StGB).

Wir sehen es beim E-Mail-Verkehr mit Daten mit erhöhtem Schutzbedarf als Stand der Technik an, sowohl eine Transport- als auch eine Inhaltsverschlüsselung vorzunehmen.

Zusätzlich müsste seitens der verantwortlichen Stelle, also der Versicherung, noch sichergestellt sein, dass die E-Mail-Adresse des Empfängers (Versicherter) auch tatsächlich von demjenigen stammt, mit dem kommuniziert werden soll: Es ist durchaus denkbar, dass sich Unbefugte eine E-Mail-Adresse mit dem Namen des Betroffenen generieren und von dort aus versuchen Informationen über diesen von der Versicherung anzufordern und zu erhalten. Solche Attacken sind mittlerweile keine Seltenheit mehr und werden oft unter den Begriffen Social Engineering und Identitätsdiebstahl behandelt. Diesem Risiko muss durch eine vorherige Verifikation der Adresse begegnet werden.

Von dem aufgeführten Verfahren der transport- und inhaltsverschlüsselten Übertragung nach dem Stand der Technik kann nach unserer Auffassung abgewichen werden, wenn dies dem Wunsch des informierten Betroffenen entspricht. Ein völliges Absenken des Sicherheitsniveaus ist unser Meinung nach nicht möglich: Es gibt einen Mindeststandard (derzeit Transportverschlüsselung), der eingehalten werden muss.

Zusammenfasend ist festzuhalten, dass Versicherungen (oder vergleichbare verantwortliche Stellen) den Kanal der Kommunikation per unverschlüsselter E-Mail nur anbieten dürfen, wenn sie gleichzeitig auch die Möglichkeit von transport- und inhaltsverschlüsselte E-Mails oder ausreichend sicherem Onlineportal anbieten. Ein Verweis auf die „gelbe Post" als einzige Alternative neben unverschlüsselter E-Mail-kommunikation wäre als unzulässiger Medienbruch nicht ausreichend. Ein Absenken des Sicherheitsniveaus ist zudem nur in der Kommunikation zwischen dem Betroffenen und der verantwortlichen Stelle möglich, nicht jedoch zwischen zwei verantwortlichen Stellen (wie z. B. zwischen Arzt und Labor oder Versicherung und Gutachter). Diese haben, da sie nicht über das Recht auf informationelle Selbstbestimmung Dritter verfügen können, den Stand der Technik auf jeden Fall einzuhalten.

10

Banken

10 Banken

10.1 Fraud Prevention Pools in der Kreditwirtschaft

Bankenübergreifende Fraud Prevention Pools sind unserer Auffassung nach datenschutzrechtlich gestaltbar.

Banken sehen sich in der letzten Zeit vermehrt betrügerischen Aktivitäten ausgesetzt, z. B. durch Vorlage gefälschter Personalausweise oder Lohnbescheinigungen, wobei die Täter immer wieder die Bankinstitute wechseln. Auf Bankenseite besteht ein gewichtiges Interesse daran, sich gegenseitig vor solchen Personen zu warnen. Im Kreditwesengesetz (KWG) wurde in § 25h Abs. 3 Sätze 3 und 4 dazu folgendes geregelt:

> *„Institute dürfen im Einzelfall einander Informationen im Rahmen der Erfüllung ihrer Untersuchungspflicht nach Satz 1 übermitteln, wenn es sich um einen in Bezug auf Geldwäsche, Terrorismusfinanzierung oder einer sonstigen Straftat auffälligen oder ungewöhnlichen Sachverhalt handelt und tatsächliche Anhaltspunkte dafür vorliegen, dass der Empfänger der Informationen diese für die Beurteilung der Frage benötigt, ob der Sachverhalt gemäß § 11 des Geldwäschegesetzes anzuzeigen oder eine Strafanzeige gemäß § 158 der Strafprozessordnung zu erstatten ist. Der Empfänger darf die Informationen ausschließlich zum Zweck der Verhinderung der Geldwäsche, der Terrorismusfinanzierung oder sonstiger strafbarer Handlungen und nur unter den durch das übermittelnde Institut vorgegebenen Bedingungen verwenden."*

Die Mehrheit der Datenschutzaufsichtsbehörden hält bankenübergreifende Fraud Prevention Pools unter bestimmten Rahmenbedingungen nach dem BDSG für grundsätzlich zulässig. Auch wir vertreten diese Auffassung. Um soweit wie möglich sicherzustellen, dass in bankenübergreifenden Fraud Prevention Pools nur konkret betrugsrelevante Sachverhalte erfasst und schutzwürdige Belange betroffener Personen angemessen berücksichtigt werden, haben sich diese Datenschutzaufsichtsbehörden auf Mindeststandards für Warndateien zur Betrugsprävention bei Banken – vorbehaltlich fallspezifischer Besonderheiten – geeinigt. Besonders zu beachten ist dabei aus datenschutzrechtlicher Sicht:

- Der Sachverhalt inkl. Identität des Täters muss eindeutig festgestellt sein, um Personenverwechslungen zu vermeiden.
- Der Vorwurf muss signifikant sein.
- Eine umfassende Dokumentationspflicht zwecks nachträglicher Überprüfbarkeit muss festgelegt werden.
- Die Betroffenen sind über ihre konkrete Einmeldung in den Pool zu unterrichten.

Ausblick zur DS-GVO:
Wir gehen davon aus, dass solche bankenübergreifende Fraud Prevention Pools unter den vorgenannten Grundsätzen auch unter Geltung der DS-GVO nach der Interessenabwägungsvorschrift von Art. 6 Abs. 1 f) zulässig sind, denn nach Nr. 47 ErwGr kann die Verarbeitung personenbezogener Daten im für die Verhinderung von Betrug unbedingt erforderlichen Umfang ein berechtigtes Interesse des jeweiligen Verantwortlichen darstellen.

10.2 Kreditverkäufe

Wer als natürliche Person seine finanziellen Pflichten aus Kreditverträgen ordnungsgemäß erfüllt, muss es nicht hinnehmen, dass die Daten aus seinem Kreditvertrag ohne seine Einwilligung anläss-

lich von Kreditverkäufen durch Banken an Dritte übermittelt werden.

Beim Verkauf von ungekündigten und nicht notleidenden Krediten von natürlichen Personen durch Banken an Dritte sind unseres Erachtens die allgemeinen Regelungen in § 398 ff. BGB zu Forderungsübertragungen im Hinblick auf die damit verbundenen Übermittlungen personenbezogener Daten durch das Datenschutzrecht eingeschränkt. Aufgrund der gesetzgeberischen Maßnahmen wegen der anfangs des Jahrhunderts zunehmenden Kreditverkaufssachverhalte, insbesondere durch das sog. Risikobegrenzungsgesetz aus 2008, der Ergänzung von § 309 Nr. 10 BGB (Wechsel des Vertragspartners) mit Aufnahme der Darlehensverträge und der Regelung in Art. 247 § 9 Abs. 1 Satz 2 EGBGB zu den Pflichthinweisen bei Immobiliendarlehensverträgen, gehen wir davon aus, dass der Übermittlung von personenbezogenen Daten bei Kreditverkäufen zu Kreditnehmern, die ihren vertraglichen Verpflichtungen bisher nachgekommen sind, regelmäßig schutzwürdige Belange der Kreditnehmer bei der Interessenabwägung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG entgegenstehen. Das schutzwürdige Interesse der Betroffenen nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG in diesem Sachverhalt wird unseres Erachtens auch gestärkt durch das besondere Vertrauensverhältnis, das die Banken ihren Kunden durch die AGB-Regelungen zusichern, insbesondere zur Wahrung des Bankgeheimnisses. Damit ist die mit einem Verkauf von ungekündigten und nicht notleidenden Krediten von natürlichen Personen durch Banken an Dritte verbundene Übermittlung personenbezogener Daten aus unserer Sicht nur mit einer Einwilligung der Betroffenen zulässig.

Ausblick zur DS-GVO:
Künftig ist davon auszugehen, dass bei solchen Kreditverkäufen unter Geltung der DS-GVO die dann nach Art. 6 Abs. 1 f) zu erfolgende Interessenabwägung im Hinblick auf die DS-GVO-Regelungen zur Zweckbindung (Art. 6 Abs. 4) und zu einer fairen Verfahrensweise nach den Grundsätzen von Treu und Glauben (Art. 5 Abs. 1 a)) in gleicher Weise ausfällt.

10.3 Finanzaufsichtliche Prüfungen in Banken

Behörden der Finanzaufsicht können nicht unbegrenzt Einblick in Personalakten erhalten.

Weil bei der Prüfung einer Bank durch die Finanzaufsicht ein intensiver Einblick in Personalakten von Bankmitarbeitern gewünscht wurde, sind wir um eine datenschutzrechtliche Bewertung gebeten worden. Bei Prüfungshandlungen der Finanzaufsicht, die personenbezogene Daten von Kunden oder Mitarbeitern betreffen, sind neben den KWG-Vorschriften auch die Vorschriften des BDSG zu berücksichtigen. Nur soweit das KWG selbst auch die datenschutzrechtliche Seite spezialgesetzlich konkret regelt, wie z. B. in § 10 Abs. 2 oder § 25h Abs. 2 Satz 2 KWG, findet das BDSG gemäß § 1 Abs. 3 Satz 1 BDSG keine Anwendung. Während das KWG insbesondere die finanzielle Situation der Bankinstitute im Fokus hat, schützt das BDSG das Persönlichkeitsrecht und die informationelle Selbstbestimmung der betroffenen Kunden und Mitarbeiter.

Bei Prüfungen der Finanzaufsicht, die Personaldaten von Mitarbeitern betreffen, ist im Hinblick auf die BDSG-Regelungen die Erforderlichkeit der Einsichtnahme in die Personaldaten für den Zweck der Prüfungshandlung im Auge zu behalten sowie zur Berücksichtigung der zentralen Grundsätze der Datenvermeidung und Datensparsamkeit (§ 3a BDSG) der Datenumfang einzugrenzen und soweit wie möglich mit anonymisierten oder pseudonymisierten Daten zu arbeiten. Dementsprechend dürfen Banken auch nur im erforderlichen Maße Personaldaten ihrer Mitarbeiter an die Finanzaufsicht übermitteln oder zur Einsicht be-

reithalten, um ihrer Arbeitgeberverantwortung für die Beschäftigtendaten gerecht zu werden. Im Zweifel müssen sie sich von der Finanzaufsicht konkret belegen lassen, warum es zur Erfüllung der gesetzlichen Aufgaben der Finanzaufsicht erforderlich ist, in einzelne konkrete Personalunterlagen Einsicht zu nehmen.

Ausblick zur DS-GVO:
Wir denken, dass künftig die nach Art. 6 Abs. 1 f) zu erfolgende Interessenabwägung im Hinblick auf die DS-GVO-Regelungen zur Zweckbindung (Art. 6 Abs. 4) und zu den Grundsätzen nach Art. 5 Abs. 1 c) (dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt) in gleicher Weise ausfällt.

10.4 Unzulässige Übermittlung von Kontoständen an Dritte

Bank-Mitarbeiter müssen vor der Nennung von Kontoständen sorgfältig die Identität des Gesprächspartners prüfen.

In einer Beschwerde wurde uns vorgetragen, dass der Beschwerdeführer einen Anruf einer Bankmitarbeiterin erhalten habe, die ihn wegen seiner Kontostände über Geldanlagen beraten wollte. Die Telefonnummer des Beschwerdeführers habe die Bankmitarbeiterin von seinem Bruder erhalten, den sie irrtümlicherweise als vermeintlichen Kontoinhaber angerufen und im Gespräch personenbezogene Bankdaten des Beschwerdeführer einschließlich seiner Kontoständen bekannt gegeben habe. Der Beschwerdeführer meinte ferner, dass er der Bank gar keine Einwilligung zur werblichen Ansprache per Telefon erteilt habe.

Unsere Ermittlungen ergaben, dass infolge unzureichender Identitätsprüfung bei dem Telefongespräch Kontostände des Beschwerdeführers von der Bankmitarbeiterin dem Bruder des Beschwerdeführers mitgeteilt worden sind. Diese unzulässige Datenübermittlung der Bankmitarbeiterin, die aufgrund ihrer Ausbildung und Tätigkeit die besondere Sensibilität von Bankdaten hätte kennen und auf eine sichere Identitätsprüfung achten müssen, haben wir mit einem Bußgeld geahndet.

11

Auskunfteien

11 Auskunfteien

11.1 Betrugsbekämpfung

Bei der Einrichtung von Datenbanken zur Betrugsabwehr (sog. Fraud Prevention Pools) ist wegen der Sensibilität dieser Daten und der möglichen Auswirkungen für betroffene Personen besondere Sorgfalt anzulegen.

Mehrfach wurden wir von Unternehmen um datenschutzrechtliche Beratung zur Verarbeitung personenbezogener Daten für die Betrugsbekämpfung gebeten. Der Anstieg von betrügerischen Aktionen im Handel und im Internet, z. B. mittels Identitäts- oder Kreditbetrug, führt bei den Leistungsanbietern zu Überlegungen, mit welchen Maßnahmen die zunehmenden finanziellen Ausfälle eingedämmt werden können. Entstanden sind dabei auch firmenübergreifende Fraud Prevention Pools in Unternehmensgruppen sowie Fraud-Datenbanken bei Auskunfteien, z. B. mit Daten zu gefälschten Ausweisen und Lohnbescheinigungen (siehe auch 10.1).

Nachfolgende Grundsätze sind bei der Gestaltung von Fraud Prevention Pools in der Wirtschaft aus datenschutzrechtlicher Sicht besonders zu beachten:

- Der Betrugssachverhalt inkl. Identität des Täters muss eindeutig festgestellt sein, um Falschverdächtigungen und Personenverwechslungen zu vermeiden.
- Der Vorwurf muss signifikant sein.
- Eine umfassende Dokumentationspflicht zwecks nachträglicher Überprüfbarkeit muss festgelegt werden.

Ausblick zur DS-GVO:
Es ist anzunehmen, dass Fraud Prevention Pools unter den vorher genannten Grundsätzen auch unter Geltung der DS-GVO nach der Interessenabwägungsvorschrift von Art. 6 Abs. 1 f) als zulässig angesehen werden können. Nach Nr. 47 ErwGr kann die Verarbeitung personenbezogener Daten im für die Verhinderung von Betrug unbedingt erforderlichen Umfang ein berechtigtes Interesse des jeweiligen Verantwortlichen darstellen.

11.2 Speicherung von Voranschriften

Gespeicherte Voranschriften von betroffenen Personen bei Auskunfteien sind im Regelfall spätestens nach sechs Jahren zu löschen.

Wir werden immer wieder von Verbrauchern zur datenschutzrechtlichen Zulässigkeit bzw. zu den Löschfristen gefragt, wenn bei einer Auskunftei in ihren Datensätzen noch frühere Anschriften enthalten sind. Die Auskunfteien begründen die Notwendigkeit der Speicherung sogenannter Voranschriften damit, dass dies zur Identitätsklärung bei namensgleichen Personen oder wegen der notwendigen Zuordnung von früheren Negativmerkmalen (Alt-Zahlungstiteln usw.) noch erforderlich sei. Dies ist grundsätzlich nachvollziehbar.

Zur Zeitdauer der Speicherung einer Voranschrift haben die Datenschutzaufsichtsbehörden aufgrund der Regelungen in § 35 Abs. 2 Nr. 4 BDSG und der Praxiserfahrungen mehrheitlich eine Prüfungsverpflichtung in zwei Drei-Jahres-Zeiträumen der Prüffrist aus § 35 Abs. 2 Nr. 4 BDSG als sachgerecht für den Zweck angesehen, ob die Voranschrift wegen fehlender weiterer Relevanz zu löschen ist. Das bedeutet, dass überholte Voranschriften re-

gelmäßig spätestens nach sechs Kalenderjahren zu löschen sind. Für überholte Voranschriften, die schon länger zurückliegen, müssen für eine fortdauernde Speicherung bei einer Auskunftei besondere Gründe geltend gemacht werden können, z. B. vorliegende gerichtliche Zahlungstitel, zu denen ein Schuldner immer noch keine Zahlungen geleistet hat. Andernfalls sind solche überholten Altanschriften zu löschen.

Ausblick zur DS-GVO:

Die DS-GVO nennt in Art. 17 zum Recht auf Löschung personenbezogener Daten zwar keine konkreten Zeiträume. Bei der Beurteilung nach Art. 17 Abs. 1 a) DS-GVO, ob personenbezogene Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, noch als notwendig angesehen werden können, erscheinen uns die vorgenannten Maßstäbe aus dem BDSG weiterhin als geeignete Orientierung.

12

Werbung und Adressenhandel

12 Werbung und Adressenhandel

12.1 Datenschutzverstöße bei Werbung

Unternehmen sind gut beraten, die datenschutzrechtlichen Vorgaben für die Nutzung von Kontaktdaten für Werbung zu beachten, sonst drohen Bußgelder.

Beschwerden von Verbrauchern über belästigende Werbung werden nicht wirklich weniger. Besonders die unerwünschte Telefon- und E-Mail-Werbung sowie die Nichtbeachtung von Werbewidersprüchen sind bei den Datenschutzaufsichtsbehörden ein Dauerthema. Darauf haben wir nochmals im Juli 2015 mittels einer Pressemitteilung hingewiesen.

Link:
www.lda.bayern.de/de/pressemitteilungen.html

Zur Aufklärung über die Rechtslage haben wir zudem in einem kurzen Papier für Unternehmen, Vereine und selbständige Gewerbetreibende, aber auch Bürgerinnen und Bürger, die wesentlichen Rahmenbedingungen für eine zulässige Nutzung von Kontaktdaten zu Werbezwecken zusammengestellt.

Link:
www.lda.bayern.de/media/info_werbung_buerger.pdf

Ausführlichere Erläuterungen zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für werbliche Zwecke finden sich in den Anwendungshinweisen der Datenschutzaufsichtsbehörden.

Link:
www.lda.bayern.de/media/ah_werbung.pdf

Wer sich als Unternehmen nicht an die mehrfach kommunizierten und altbekannten Regeln hält, muss nicht nur mit kostenpflichtigen Abmahnverfahren, sondern auch mit Bußgeldbescheiden der Aufsichtsbehörden rechnen. So haben wir in den letzten beiden Jahren unter anderem vier Bußgeldbescheide wegen Nichtbeachtung der von Verbrauchern erklärten Werbewidersprüche erlassen.

Ausblick zur DS-GVO:
Zur Zulässigkeit der Nutzung von Kontaktdaten für Werbung gibt es durch die DS-GVO keine wesentlichen Änderungen.

12.2 Gewinnspielangebote

Bei einer Erhebung personenbezogener Daten anlässlich von Gewinnspielen ist auf eine korrekte Datenschutzinformation der Teilnehmer zu achten.

Unklare Informationen zu Gewinnspielangeboten führen zur Verwirrung bei Verbrauchern und zu Nachfragen und Beschwerden bei uns. Für die Durchführung von Gewinnspielen weisen wir auf die Vorschriften von § 4 Abs. 3 BDSG und bei Online-Gewinnspielen auf § 13 Abs. 1 TMG hin, wonach die von einer Datenerhebung betroffenen Personen, hier die Gewinnspielteilnehmer, möglichst transparent über den Zweck und den beabsichtigten Umgang mit ihren Daten sowie über die verantwortlichen Stellen zu informieren sind. Soweit Daten nur auf freiwilliger Basis erhoben werden, sind die entsprechenden Datenfelder deutlich zu kennzeichnen. Eine hinreichende Information nach § 4 Abs. 3 BDSG und § 13 Abs. 1 TMG erfüllt nicht nur die datenschutzrechtlichen Rahmenbedingungen, sondern fördert auch das notwendige Vertrauen der Personen, deren Teilnahme an dem Gewinnspiel erwünscht ist, in einen ihren Interessen entsprechenden datenschutzkonformen Umgang mit ihren Daten.

12.3 Werbe-E-Mails aus dem Ausland

Unerwünschte Werbe-Mails aus dem Ausland werden von den E-Mail-Providern je nach Vertrag unterschiedlich gut ausgefiltert – die Datenschutzaufsichtsbehörden können selten wirksam dagegen vorgehen.

Zu manchen uns zugeleiteten unerwünschten Werbe-E-Mails konnten wir bei unserer Prüfung keine Verbindung zu einer in Deutschland ansässigen verantwortlichen Stelle oder Person feststellen. Oft ist es in solchen Fällen für uns auch technisch nicht möglich, den tatsächlichen Versender von unerwünschten Werbe-E-Mails ausfindig zu machen und solche Mails zu stoppen, wenn die Absender aus dem Ausland agieren und die Absenderdaten bewusst fälschen oder verschleiern. Meist verbergen sich dahinter dubiose bzw. betrügerische Werbeangebote oder es wird versucht, unvorsichtigen Nutzern auf deren IT-Geräten Schadsoftware zu installieren oder deren Daten auszuspähen („Trojaner-Mail", „Phishing-Mail", siehe Beitrag in Kapitel 22 zum Thema Spam und Phishing).

Die E-Mail-Provider bieten ihren Nutzern mittlerweile jedoch – je nach gebuchtem Tarif – unterschiedlich gut wirkende Spam- und Schadsoftware-Filter an, um solche unerwünschten Nachrichten von der eigentlichen E-Mail-Post zu separieren.

Wir empfehlen deshalb, die angebotenen Schutzmöglichkeiten der Anbieter auch zu nutzen. Ein kostenloser Tarif sieht oft nur wenige Schutzvorkehrungen vor, was Verbraucher dann bei ihrem Verhalten im Umgang mit ihrem Postfach berücksichtigen sollten.

13

Handel und Dienstleistung

13 Handel und Dienstleistung

13.1 Kundendaten beim Asset Deal

Bei Unternehmensverkäufen in der Form des sog. Asset Deals ist häufig auch der Verkauf von Kundendaten gewünscht. Eine Übermittlung von Nicht-Listendaten kann unter Umständen bei Einräumung eines Widerspruchsrechts an die Kunden zulässig sein.

Im Berichtszeitraum beschwerten sich immer wieder im Rahmen unterschiedlicher Sachverhalte Eingabeführer darüber, dass sie von einem ihnen bis dahin unbekannten Unternehmen Werbung – meist per E-Mail – erhalten hätten, und dass ihnen auf Nachfrage mitgeteilt worden sei, das Unternehmen sei „Rechtsnachfolger" eines anderen Unternehmens und habe daher dessen Kundendatei „übernommen". Wir sind den Eingaben nachgegangen und dabei auf eine offenbar recht weit verbreitete Problematik gestoßen – die Veräußerung von Kundendaten im Rahmen der Veräußerung ganzer Geschäftsbereiche oder gar der wesentlichen Teile des operativen Geschäfts von Unternehmen.

Personenbezogene Kundendaten haben für Unternehmen häufig erheblichen wirtschaftlichen Wert, vor allem, weil sie die Möglichkeit der werblichen Ansprache der Kunden beinhalten. Unternehmen, die ihre Tätigkeit einstellen, versuchen daher oft, Kundendaten als werthaltiges Gut („Asset") entgeltlich an andere Unternehmen zu veräußern. Wie sich im Zuge unserer Überprüfungen zeigte, wird dies besonders auch in Insolvenzfällen seitens der Insolvenzverwalter versucht; mehrere der von uns überprüften Beschwerden betrafen Unternehmen in der Insolvenz. Zudem erreichten uns im Berichtszeitraum auch Beratungsanfragen von in der Insolvenz befindlichen Unternehmen, die eine Veräußerung von Kundendaten wünschten.

Datenschutzrechtlich verhältnismäßig unproblematisch ist in solchen Fällen die Übermittlung von Namen und Postanschriften. Diese sog. Listendaten dürfen gemäß § 28 Abs. 3 Satz 2 BDSG, jedenfalls bei Einhaltung bestimmter Dokumentationspflichten, auch ohne Einwilligung der Betroffenen für werbliche Zwecke übermittelt werden. Bei den uns bekannt gewordenen Asset Deals wurden auch weitere Datenkategorien übermittelt, etwa – insbesondere bei Veräußerungen von Webshops – E-Mail-Adressen und Telefonnummern. Sofern solche „Nicht-Listendaten" (u. U. auch Bank- und Kreditkartendaten, Kaufhistorien, Kundenprofile etc.) übermittelt werden sollen, ist das gemäß § 28 Abs. 3 Satz 1 BDSG grundsätzlich nur mit Einwilligung der Betroffenen möglich.

In der Praxis sehen wir allerdings, dass in Asset-Deal-Fällen „der Sache nach" häufig eine Weiterführung des Geschäftsbetriebs des abgewickelten Unternehmens oder zumindest von signifikanten Teilen hiervon durch ein anderes Unternehmen, den Käufer der Assets, stattfindet. Oft werden dabei auch mehr oder weniger große Teile der Belegschaft des abgebenden Unternehmens durch das erwerbende Unternehmen übernommen. Die wirtschaftliche Einheit bleibt in derartigen Fällen somit – zumindest hinsichtlich einzelner Geschäftsbereiche – erhalten und wird durch einen neuen Rechtsträger fortgeführt. Wenn es sich um eine solche faktische (Teil-)Fortführung des Geschäftsbetriebs handelt, beschränkt sich der Zweck der Kundendatenübermittlung nicht allein auf die werbliche Verwendung, sondern dient vielmehr der Fortsetzung von (zum Teil langjährigen) Kundenbeziehungen und mittelbar der (Teil-)Fortführung des Geschäftsbetriebs. Bei derartigen Fällen faktischer Geschäfts(teil)fortführung können neben § 28 Abs. 3 BDSG grundsätzlich auch noch die Erlaubnistatbestände des § 28 Abs. 2 BDSG Anwendung finden. Eine Übermittlung von Kundendaten kann daher unter bestimmten Um-

ständen mit dem berechtigten Interesse der Geschäfts(teil)fortführung des abgebenden und des erwerbenden Unternehmens nach § 28 Abs. 2 Nr. 1 bzw. Nr. 2a BDSG gerechtfertigt werden.

Voraussetzung für die Zulässigkeit der Übermittlung ist allerdings, dass die Kunden im Vorfeld auf die geplante Übermittlung hingewiesen werden und ihnen eine – zeitlich ausreichend bemessene – Frist zum Widerspruch gegen die Übermittlung eingeräumt wird. Bei Kunden, die trotz ausdrücklicher Einräumung der Widerspruchsmöglichkeit der Übermittlung nicht widersprochen haben, darf nach Ablauf der Widerspruchsfrist grundsätzlich davon ausgegangen werden, dass sie keine schutzwürdigen Interessen am Unterbleiben der Übermittlung im Sinne der nach § 28 Abs. 2 Nr. 1 bzw. Nr. 2a BDSG haben.

In einem der von uns bearbeiteten Fälle hatte das erwerbende Unternehmen – ein Autohaus – mit dem veräußernden insolventen Unternehmen vereinbart, für die kaufrechtlichen Gewährleistungsansprüche der Kunden einzustehen, wodurch die Kunden besser gestellt wurden, als wenn ihre Gewährleistungsansprüche nur als Insolvenzforderungen zur Insolvenztabelle angemeldet worden wären. Dieses Beispiel zeigt, dass die Bandbreite der denkbaren Fallgestaltungen und Interessenlagen bei Asset Deals beträchtlich ist, so dass stets der jeweilige Einzelfall betrachtet werden muss und sich allzu schematische datenschutzrechtliche Bewertungen verbieten.

Die „Widerspruchslösung" bietet aber jedenfalls einen angemessenen und interessengerechten Ausgleich für Fälle, in denen das erwerbende Unternehmen Teile des Geschäftsbetriebs fortführt.

Soll hingegen nur isoliert die „Kundendatenbank" im Wege eines Asset Deal verkauft werden, spricht das gegen eine Anwendbarkeit der „Widerspruchslösung", da in solchen Fällen in der Regel die werbliche Verwendung der Daten den vorrangigen Zweck der Übermittlung darstellen wird, so dass allein § 28 Abs. 3 BDSG als Spezialvorschrift anwendbar ist.

Selbst wenn auf der Basis der Widerspruchslösung Kundendaten übermittelt wurden, ist darauf hinzuweisen, dass das erwerbende Unternehmen damit noch nicht die Möglichkeit hat, die erworbenen E-Mail-Adressen bzw. Telefonnummern der Kunden zu eigenen werblichen Zwecken zu verwenden. Denn hierfür wäre wegen § 7 Abs. 2 Nr. 2 bzw. Nr. 3 UWG eine ausdrückliche Einwilligung des Kunden erforderlich; ein bloßes Nicht-Widersprechen stellt aber nicht gleichzeitig auch eine ausdrückliche Einwilligung im Sinne von § 7 Abs. 2 UWG dar. Schließlich ist auch § 7 Abs. 3 UWG, der jedenfalls für das Medium E-Mail die Werbeansprache erlaubt, auf das erwerbende Unternehmen nicht anwendbar, da diese Vorschrift voraussetzt, dass das „Unternehmen" – also das erwerbende Unternehmen (d. h. der neue Rechtsträger) selbst – die E-Mail-Adresse des Kunden vom Kunden im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung erhalten haben müsste. Das erwerbende Unternehmen ist aber bei einem solchen Asset Deal nicht identisch mit dem veräußernden Unternehmen, dem der Kunde ggf. seine E-Mail-Adresse im Rahmen eines Kaufs zur Verfügung gestellt hat; daher ist § 7 Abs. 3 UWG nur auf das veräußernde, nicht jedoch auch auf das erwerbende Unternehmen anwendbar. Wenn bei einem Asset Deal daher gewollt ist, dass das erwerbende Unternehmen E-Mail-Adressen von Kunden für eigene werbliche Zwecke verwenden können soll, genügt die Widerspruchslösung alleine nicht. Vielmehr müsste dann vor der Übermittlung eine ausdrückliche Einwilligung der Betroffenen in die Übermittlung und die werbliche Nutzung der E-Mail-Adressen durch das erwerbende Unternehmen eingeholt werden.

Wir haben im Berichtzeitraum über diese Problematik intensiv mit Unternehmen und Insol-

venzverwaltern diskutiert und entsprechende Informationen über die hier geschilderten Anforderungen bereitgestellt. Wir werden unsere Informationen fortsetzen, da es sich nach unserer Beobachtung um ein sehr praxisrelevantes Thema handelt, und gerade in Insolvenzfällen den Anforderungen des Datenschutzrechts nach unserer Beobachtung nicht immer die notwendige Aufmerksamkeit eingeräumt wird.

13.2 Rückgabe eines defekten USB-Sticks

Bei Rückgabe von defekten Datenträgern im Rahmen der Gewährleistung muss das betroffene Unternehmen für eine Datenlöschung sorgen.

Eine Bürgerin beschwerte sich bei uns, weil ihr bei der Rückgabe eines defekten USB-Sticks an ein Handelsgeschäft im Rahmen der Gewährleistung keine sachgerechte Lösung für die Löschung ihrer inzwischen auf dem USB-Stick gespeicherten persönlichen Daten angeboten werden konnte. Sie selbst konnte wegen des Defekts nicht mehr auf den Datenspeicher zugreifen und die Daten nicht selbst löschen. Ein mechanisches Zerstören des USB-Sticks durch die Bürgerin selbst hätte aber den Gewährleistungsanspruch gefährdet.

Wir setzten uns mit dem betroffenen Unternehmen in Verbindung, um hier eine datenschutzkonforme Lösung zu erreichen. Der Kundin wurde daraufhin ein neuer USB-Stick ausgehändigt. Der alte USB-Stick mit den Daten der Kundin wurde im Beisein der Kundin datenschutzgerecht zerstört und entsorgt. Der Vorfall wurde bei dem Unternehmen zum Anlass genommen, den Prozess der Rückgabe von USB-Sticks im Rahmen der Gewährleistung neu zu regeln.

13.3 Aufzeichnung von Aufzugs- und Alarmanlagen-Notrufen

Die Aufzeichnung von Sprachkommunikation kann bei sog. Notrufen ggf. auch ohne Einwilligung des Betroffenen zulässig sein. Hinsichtlich der Länge der Speicherdauer kommt es darauf an, innerhalb welcher Zeiträume in aller Regel ein Rückgriff auf die Sprachaufzeichnung notwendig werden kann, um sich gegen Vorwürfe nicht ordnungsgemäßer Notrufbearbeitung zu verteidigen.

Ein Unternehmen, das sog. Notruf- und Serviceleitstellen betreibt, wollte wissen, inwieweit Sprach-Notrufe aus Aufzügen sowie Sprachverbindungen zur Leitstelle, die infolge eines Alarms einer Alarmmeldeanlage (z. B. Einbruchmeldeanlage) automatisch aufgebaut werden, aufgezeichnet und wie lange die Aufzeichnungen aufbewahrt werden dürfen.

Sowohl bei den Aufzugsnotrufen als auch bei den Sprachverbindungen zu den Alarmmeldeanlagen wird mit der Aufzeichnung zum einen der Zweck verfolgt, den Gesprächsverlauf zu dokumentieren, um bei Bedarf ein wiederholtes Abspielen des Notrufs durch die Leitstellenmitarbeiter zu ermöglichen. Dies könne nach Angaben des Unternehmens erforderlich werden, um schlecht verstandene Passagen noch einmal nachzuhören oder Angaben zu verifizieren (etwa wenn die betroffene Person später nicht mehr ansprechbar ist) und so die Lage korrekt einschätzen und die bestmögliche Hilfeleistung in die Wege leiten zu können.

Wir halten es in den vom Unternehmen geschilderten Fällen für grundsätzlich vertretbar, die Sprachkommunikation auch ohne vorherige Einwilligung der betroffenen Gesprächspartner aufzuzeichnen, da es nach – grundsätzlich plausibler – Darstellung des Unternehmens in den geschilderten typischen Notrufsituationen mit Blick auf den Zeitdruck, umgehend

handeln zu müssen, zumindest häufig nicht möglich ist, eine Einwilligung des Gesprächspartners einzuholen. Die Aufzeichnung lässt sich unter diesen Voraussetzungen nach unserer Bewertung datenschutzrechtlich mit berechtigten Interessen des die Leitstelle betreibenden Unternehmens auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG stützen, da es nachvollziehbar ist, dass der Leitstellenmitarbeiter in einigen Fällen die Aufzeichnung benötigt, um schlecht verstandene Angaben noch einmal nachzuhören. Schutzwürdige Interessen der Betroffenen am Unterbleiben der Aufzeichnung überwiegen in den geschilderten Notfällen demgegenüber nicht, da die Betroffenen auch selbst ein Interesse daran haben, dass die von ihnen gemachten Angaben bei Bedarf noch einmal abgespielt werden können, um die Situation korrekt einzuschätzen und so sachgerechte Hilfe zu ermöglichen.

Im Zusammenhang mit der weiteren aufgeworfenen Frage nach der zulässigen Speicherdauer teilte uns das die Leitstelle betreibende Unternehmen mit, dass eine Speicherung auch nach Abarbeitung der unmittelbaren Notrufsituation für eine gewisse Zeitdauer noch notwendig sei, da es immer wieder Fälle gebe, in denen die Kunden (etwa Unternehmen, bei denen eine Einbruchmeldeanlage betrieben wird) nach einer gewissen Zeit dem Leitstellenbetreiber ein unrichtiges bzw. nicht vertragsgemäßes Handeln vorhalten, indem sie beispielsweise behaupten, der Leitstellenbetreiber habe die mit dem Kunden für den Alarmfall vereinbarten Maßnahmepläne nicht eingehalten. Derartige Reklamationen würden erfahrungsgemäß häufig auch noch einige Wochen nach dem Vorfall erhoben. Wir haben vor diesem Hintergrund eine Speicherung der Sprachaufzeichnungen von bis zu 100 Tage als vertretbar angesehen, haben jedoch dem Unternehmen mitgeteilt, dass hierzu eine zu dokumentierende Evaluation dahingehend erfolgen müsse, innerhalb welcher Zeiträume Reklamationen tatsächlich erhoben werden. Sollte die Praxis ergeben, dass der weitaus größte Teil von Reklamationen binnen eines kürzeren Zeitraums erhoben wird, muss die Speicherdauer entsprechend korrigiert werden.

13.4 Einwilligungserklärungen zur Datenverwendung in Formularen

Die Aufsichtsbehörden geben Hinweise dazu, welche gesetzlichen Anforderungen datenschutzrechtliche Einwilligungen in Bezug auf Form und Inhalt erfüllen müssen.

Weil wir immer wieder zur datenschutzgerechten Formulierung und Gestaltung von Einwilligungserklärungen für den beabsichtigten Umgang mit personenbezogenen Daten von Kunden, Interessenten, Gewinnspielteilnehmern usw. angefragt wurden, haben wir im „Düsseldorfer Kreis" die Erarbeitung einer Orientierungshilfe zu diesem Thema vorgeschlagen. Das dann im März 2016 beschlossene Papier enthält in elf Unterpunkten Ausführungen zu verschiedenen Aspekten einer datenschutzkonformen Einwilligung – vom eindeutigen Inhalt über die Klarstellung der Freiwilligkeit bis zur notwendigen Hervorhebung.

Link:
www.lda.bayern.de/media/oh_einwilligung.pdf

Ausblick zur DS-GVO:
Die DS-GVO regelt in Art. 4 Nr. 11 und in Art. 7 sowie in den ErwGr. 32 und 42 ähnliche Grundsätze für Datenschutz-Einwilligungen, allerdings werden durch die DS-GVO (insbesondere Art. 13) die dabei gegebenen Informationspflichten gegenüber den betroffenen Personen erweitert. Die möglichen Auswirkungen haben wir in einem kurzen Papier zur DS-GVO auf unserer Webseite veröffentlicht.

Link:
www.lda.bayern.de/de/datenschutz_eu.html

13.5 Datenumgang im Schornsteinfegerwesen

Die Übermittlung personenbezogener Daten eines Hauseigentümers und eines Schornsteinfegers an den Bezirksschornsteinfeger zum Zweck der Überprüfung der Arbeiten nach einem Feuerstättenbescheid ist datenschutzrechtlich zulässig.

Ein Schornsteinfeger (Beschwerdeführer) beschwerte sich bei uns darüber, dass er dem sog. bevollmächtigten Bezirksschornsteinfeger personenbezogene Daten zu Kunden des Beschwerdeführers melden müsse, die der bevollmächtigte Bezirksschornsteinfeger nutze, um ihm, dem Beschwerdeführer, unfaire Konkurrenz zu machen.

Um diese Beschwerde einschätzen und bewerten zu können, haben wir die gesetzlichen Regelungen zu den Aufgaben der sog. bevollmächtigten Bezirksschornsteinfeger untersucht. Im Zuge der erfolgten Abschaffung des Monopols im Schornsteinfegerwesen wurden per Gesetz den sog. bevollmächtigten Bezirksschornsteinfegern einige Aufgaben als beliehene Unternehmer zur Durchführung innerhalb ihres Bezirks übertragen, darunter die Führung des Kehrbuchs, die Durchführung der Feuerstättenschau und der Erlass des Feuerstättenbescheids, in dem auch zu beseitigende Mängel sowie der späteste Termin zur Beseitigung genannt werden.

Zur Durchführung dieser Mängelbeseitigung können sich die Hauseigentümer selbst einen Schornsteinfegerbetrieb aussuchen. Dieser hat nach Ausführung der Arbeiten ein Formblatt auszufüllen und es dem bevollmächtigten Bezirksschornsteinfeger vorzulegen. Dadurch werden dem Bezirksschornsteinfeger die Daten der verschiedenen Schornsteinfegerbetriebe einschließlich der jeweiligen Kunden mitgeteilt.

Die bevollmächtigten Bezirksschornsteinfeger haben nach § 19 SchfHwG das sog. Kehrbuch zu führen, in das bestimmte Daten, die in Absatz 1 Satz 1 der Vorschrift aufgelistet sind, einzutragen sind. Die Formblätter sind gem. § 5 und der Anlage 2 zu § 5 der Kehr- und Überprüfungsverordnung (KÜO) im Aussehen und den zu übermittelnden Daten vorgegeben. Die Datenübermittlung erfolgt also aufgrund einer Rechtsvorschrift als Rechtsgrundlage (§ 4 Abs. 1 SchfHwG, § 5 KÜO) und ist damit datenschutzrechtlich nach § 4 Abs. 1 BDSG zulässig.

Der bevollmächtigte Bezirksschornsteinfeger ist einerseits gemäß § 8 SchfHwG beliehener Unternehmer, der die ihm staatlich zugewiesenen Maßnahmen in seinem Bezirk durchzuführen hat; andererseits ist er hinsichtlich sonstiger Leistungen „normaler" Handwerker, der mit den übrigen Schornsteinfegern im Wettbewerb steht.

Es mag sein, dass der bevollmächtigte Bezirksschornsteinfeger – was der Beschwerdeführer monierte – durch seine Tätigkeit als beliehener Unternehmer faktisch einen „Wissensvorsprung" gegenüber seinen Mitstreitern hat. Jedoch darf der bevollmächtigte Bezirksschornsteinfeger die Daten aus dem Kehrbuch bzw. aus seiner Tätigkeit als beliehener Unternehmer gemäß § 19 Abs. 5 Satz 1 SchfHwG nur nutzen, soweit dies zur Erfüllung seiner Aufgaben nach dem Gesetz erforderlich ist, d. h. nicht für Zwecke, hinsichtlich derer er „normaler Handwerker" ist.

Anhaltspunkte für einen Verstoß konnten wir im konkreten Fall nicht erkennen.

13.6 Sperrvermerke in behördlichen Registern

Sperrvermerke in Melderegistern, Fahrzeugregistern o.ä. verpflichten grundsätzlich nur die jeweils davon betroffenen Behörden. Unternehmen sind von diesen Regelungen nur insoweit betroffen, als sie ggf. keine Auskunft erteilt bekommen, wenn sie bei diesen Registern Anfragen stellen.

Der Kunde eines Unternehmens, für den ein Sperrvermerk im Melderegister eingetragen war, beschwerte sich bei uns darüber, dass das Unternehmen sich trotz entsprechender Aufforderung geweigert habe, dem Umstand unternehmensintern Rechnung zu tragen, dass seine Daten im Melderegister mit einem Sperrvermerk versehen seien. Der Kunde war der Meinung, dass er es in dieser besonderen Situation – von der er das Unternehmen informiert habe – nicht hinnehmen müsse, dass „normale" Mitarbeiter des Unternehmens Zugriff auf seine beim Unternehmen gespeicherten Daten nähmen. Es sei vielmehr geboten, dass nur ein enger, besonders ausgewählter Kreis von Mitarbeitern auf seine Daten zugreifen dürfe, etwa der Datenschutzbeauftragte. Dieser Sichtweise konnten wir uns nicht anschließen.

Unternehmen dürfen nach § 28 Abs. 1 Satz 1 BDSG für eigene Geschäftszwecke personenbezogene Daten erheben, speichern, verändern, übermitteln oder nutzen, wenn dies für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Vertragsverhältnisses mit dem Betroffenen erforderlich ist (Nr. 1) oder 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 (Nr. 2).

Ein Zugriff der Mitarbeiter innerhalb des Unternehmens, die gemäß ihren Arbeitsbereichen mit der Verarbeitung und Nutzung der personenbezogenen Daten der Kunden betraut sind, stellt keine Übermittlung, sondern nur eine sog. Datennutzung dar (§ 3 Abs. 5 BDSG). Je nach Größe des Unternehmens sind Zugriffsregelungen mit dem Ziel einzurichten, dass nur diejenigen Mitarbeiter Zugang zu den Kundendaten erhalten, die die Daten für die Erfüllung ihrer Tätigkeit benötigen. Sofern jedoch – wie vorliegend – ein Kunde eine darüber noch hinausgehende Einschränkung der Zugriffsrechte auf ganz bestimmte Mitarbeiter fordert, lässt sich ein entsprechender Anspruch aus dem Datenschutzrecht nicht herleiten.

Durch den Sperrvermerk im Melderegister wird lediglich die Meldebehörde gebunden, mit den Meldedaten des betroffenen Bürgers in gesetzlich beschränkter Art und Weise umzugehen. Auswirkungen auf die Privatwirtschaft hat dieser Sperrvermerk nicht.

Sonderregelungen, die sich aus dem auch für nicht-öffentliche Stellen relevanten Zeugenschutz-Harmonisierungsgesetz (ZSHG) ergeben könnten, waren hier nicht einschlägig.

13.7 Weitergabe der privaten Telefonnummer eines ehemaligen Ladenbesitzers

Wenn ein ehemaliger Ladenbesitzer der Kundschaft – etwa im Zusammenhang mit ausgegebenen Gutscheinen – eine Kontaktmöglichkeit eröffnet hat, um sich um Anfragen und Beschwerden zu kümmern, ist die Weitergabe dessen privater Kontaktdaten an die Kunden durch den Nachmieter zunächst nicht erforderlich und damit unzulässig.

Ein ehemaliger Ladeninhaber hatte für Nachfragen seiner Kunden zu ausgegebenen und

nicht eingelösten Gutscheinen auf der Internetseite zwei E-Mail-Adressen sowie eine geschäftliche Telefonnummer angegeben, über die ihn Kunden kontaktieren konnten. Der Nachmieter dieses Ladengeschäftes hat Kunden, die Beschwerden zu Gutscheinen des ehemaligen Ladenbesitzers hatten, die private Telefonnummer des ehemaligen Inhabers gegeben.

Durch die Weitergabe der Telefonnummer wurden personenbezogene Daten des ehemaligen Ladeninhabers an Dritte übermittelt. Dies stellt eine Datenverarbeitung gemäß § 3 Abs. 4 Nr. 3 BDSG dar. Eine Rechtsgrundlage für die Weitergabe haben wir nicht gesehen. Sie wäre auch nicht erforderlich, da der frühere Ladenbesitzer ausreichende Kommunikationsmöglichkeiten angeboten hatte und keine Anhaltspunkte dafür vorlagen, dass er auf Anfragen über die angebotenen Kommunikationswege nicht reagieren würde.

13.8 Meldescheine im Hotel

Im neuen Bundesmeldegesetz sind die im Hotel für den Meldeschein zu erhebenden Daten abschließend festgelegt – eine Personalausweiskopie ist bei der Anmeldung nicht gefordert und damit nicht zulässig.

Im Berichtszeitraum erreichten uns einige Beschwerden von Hotelkunden über den Umfang personenbezogener Daten, die Hotels von ihnen erhoben haben oder erheben wollten. Nach dem neuen Bundesmeldegesetz (BMG) ist nun auch offiziell das in vielen Hotels bereits übliche Vorausfüllen des Meldescheines zulässig. Der Gast hat den Meldeschein nach § 29 BMG lediglich handschriftlich zu unterschreiben.

Die für den Meldeschein zu erhebenden Daten sind abschließend in § 30 Abs. 2 BMG festgehalten. Danach sind das Datum der Ankunft und der voraussichtlichen Abreise, Familienname, Vorname, Geburtsdatum, Staatsangehörigkeit, Anschrift, Zahl der Mitreisenden und ihre Staatsangehörigkeit sowie bei ausländischen Personen die Seriennummer des anerkannten und gültigen Passes oder Passersatzpapiers zu erheben. Bei ausländischen Personen hat der Leiter der Beherbergungsstätte die Angaben im Meldeschein mit denen des Identitätsdokuments zu vergleichen.

Das Kopieren von Personalausweisen oder sonstigen Ausweisdokumenten von Hotelgästen durch Hotels ist auch im neuen Gesetz weder bei In- noch bei Ausländern vorgesehen und daher unzulässig. Nach § 30 Abs. 4 BMG sind die ausgefüllten Meldescheine ein Jahr aufzubewahren und innerhalb von drei Monaten nach Ablauf der Aufbewahrungsfrist zu vernichten. Die Meldescheine sind den nach Landesrecht bestimmten Behörden und den in § 34 Abs. 4 Satz 1 Nr. 1 bis 5 und 9 bis 11 genannten Behörden zur Erfüllung ihrer Aufgaben auf Verlangen zur Einsichtnahme vorzulegen. In Bayern sind die Meldescheine gem. Art 4 Abs. 2 des Gesetzes zur Ausführung des Bundesmeldegesetzes (BayAGMBG) auf Verlangen den Meldebehörden vorzulegen, Meldebehörden sind die Gemeinden (Art. 1 Abs. 1 Satz 1 BayAGMBG).

14

Internationaler Datenverkehr

14 Internationaler Datenverkehr

14.1 Binding Corporate Rules

Immer mehr Unternehmensgruppen entdecken Binding Corporate Rules (BCR) als Instrument zur Erfüllung der Anforderungen an (konzerninterne) Übermittlungen personenbezogener Daten in Nicht-EU-Staaten. Wir waren auch im Berichtszeitraum wieder mit mehreren BCR-Anerkennungsverfahren befasst und sind auch auf europäischer Ebene an der Fortschreibung und weiteren Präzisierung der Anforderungen an BCR beteiligt.

Rund 90 Unternehmensgruppen haben inzwischen Binding Corporate Rules eingeführt, die von den Datenschutzaufsichtsbehörden der jeweils zuständigen EU-Mitgliedstaaten „genehmigt" (besser: anerkannt) worden sind. Die Unternehmensgruppen, die erfolgreich ein BCR-Anerkennungsverfahren abgeschlossen haben, sind auf einer Liste online veröffentlicht.

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

Das unter den Datenschutzaufsichtsbehörden der EU-Mitglieds- und EWR-Vertragsstaaten bereits seit mehreren Jahren praktizierte Kooperations- und Mutual-Recognition-Verfahren (Verfahren zur gegenseitigen Anerkennung) hat sich bewährt. Durch zunehmende Erfahrung der Aufsichtsbehörden, aber auch der beratenden Praxis und der Unternehmen konnten die Anerkennungsverfahren beschleunigt und die Anforderungen an BCR, jedenfalls in der Praxis, weiter geklärt und präzisiert werden.

Wir waren im Berichtzeitraum als federführende Aufsichtsbehörde (lead authority) für mehrere BCR-Anerkennungsverfahren zuständig, von denen eines im Berichtszeitraum abgeschlossen werden konnte (Fa. Giesecke & Devrient). Daneben haben wir als sog. Co-Prüfer in mehreren Verfahren mitgewirkt, die von Datenschutzaufsichtsbehörden anderer EU-Mitgliedstaaten federführend geführt wurden. Von den in Deutschland insgesamt bisher acht BCR-Verfahren unter Federführung einer deutschen Aufsichtsbehörde abgeschlossenen Verfahren haben wir vier Verfahren betreut (Giesecke & Devrient, Siemens, Osram und BMW).

Weitere Verfahren, darunter auch solche, bei denen es um „BCR für Auftragsdatenverarbeiter" (BCR-Processors) geht, d. h. um BCR, die spezifisch für Unternehmensgruppen geeignet sind, die in erheblichem Umfang Dienste der Auftragsdatenverarbeitung für eine große Anzahl konzernfremder Auftraggeber anbieten, sind momentan noch anhängig und nicht abgeschlossen.

Auch ist festzustellen, dass manche große Konzerne für Datenübermittlungen innerhalb des Konzerns inzwischen den Einsatz von BCR gegenüber anderen Instrumenten wie etwa Standardvertragsklauseln bevorzugen. Möglicherweise erhoffen sich Konzerne durch die Prüfung und Anerkennung ihrer BCR seitens der Aufsichtsbehörden eine irgendwie „verbindliche" Anerkennung ihrer (konzerninternen) Datentransfers als insgesamt datenschutzkonform (1). Zum anderen mag es sein, dass sich Unternehmensgruppen von dem Abschluss des BCR-Verfahrens einen „Werbeeffekt" nach außen versprechen, zumal gerade große Unternehmen erfahrungsgemäß darauf bedacht sind, in möglichst vielen Regulierungsbereichen am Markt „Compliance" zu demonstrieren (2).

Bezüglich der ersten Vermutung ist darauf hinzuweisen, dass BCR lediglich die Anforderungen der sog. Zweiten Stufe an den Datentransfer abdecken, also die in §§ 4b, 4c BDSG

geregelten spezifischen, zusätzlichen Anforderungen an den Transfer personenbezogener Daten in Nicht-EU-Staaten. Die Erfüllung dieser Anforderungen wird durch den erfolgreichen Abschluss des Anerkennungsverfahrens behördlich bestätigt. Daneben müssen die Unternehmen aber bei jeder Datenübermittlung stets auch die – nicht von den BCR erfassten – Anforderungen an die „Erste Stufe" erfüllen, d. h. die Anforderungen nach § 4 Abs. 1, §§ 28 ff. BDSG, die bei jeder Übermittlung personenbezogener Daten (d. h. auch innerhalb Deutschlands) gelten.

Bezüglich der zweiten Vermutung ist festzuhalten, dass Berufung auf ein erfolgreich abgeschlossenes BCR-Anerkennungsverfahren durch eine Unternehmensgruppe am Markt sicher legitim ist. Andererseits sehen wir, dass manche Unternehmen BCR offenbar gar nicht so sehr aus ihrer eigentlichen datenschutzrechtlichen Funktion heraus begreifen – nämlich als eine Möglichkeit zur Erfüllung der Anforderungen an die „Zweite Stufe" von Datenübermittlungen (§§ 4b, 4c BDSG) –, sondern z. T. etwas vereinfachend als umfassende Demonstration einer „Datenschutz-Compliance". Wir schließen das daraus, dass wiederholt Unternehmen mit dem Wunsch nach Einführung von BCR auf uns zukommen, für die sich das Instrument bei näherer Betrachtung nur wenig eignet – etwa weil die Unternehmensgruppe nur aus wenigen einzelnen Gesellschaften besteht oder nur wenige konzerninterne Übermittlungen aus der Europäischen Union in Nicht-EU-Staaten stattfinden.

Im Dialog mit den entsprechenden Unternehmen haben wir bei solchen Anfragen auf die Funktion und die möglichen Einsatzbereiche von BCR einerseits sowie auf die Anforderungen an BCR und auf den Aufwand hingewiesen, der mit der Erstellung von BCR für das Unternehmen regelmäßig einhergeht. Auf diese Weise wollten wir den Unternehmen eine realistische Einschätzung ermöglichen, ob die Einführung von BCR in ihrem konkreten Fall wirklich sinnvoll ist.

Ausblick zur DS-GVO:

BCR-Verfahren, die ihre Grundlage bisher nur aus einem gemeinsamen Verständnis der in der Artikel-29-Gruppe vertretenen Datenschutzaufsichtsbehörden, das u. a. in den Arbeitspapieren (Working Papers) 153, 154 und 155 zum Ausdruck kommt, herleiten, sind nunmehr in der DS-GVO ausdrücklich gesetzlich geregelt (Art. 47 DS-GVO). Die Aufsichtsbehörden werden in der Zeit bis zur Anwendbarkeit der DS-GVO nähere Hinweise dazu geben, inwieweit Konzerne mit bereits behördlich anerkannten BCR etwas unternehmen müssen, um auch nach dem Mai 2018 Übermittlungen weiter auf ihre BCR stützen zu können. Mit Blick auf Art. 46 Abs. 2 DS-GVO ist davon auszugehen, dass der Gesetzgeber für die in Art. 46 Abs. 2 DS-GVO (bzw. Art. 26 Abs. 2 Richtlinie 95/46/EG) aufgezählten Instrumente und somit auch für bereits anerkannte BCR von „Bestandsschutz" ausgegangen ist, was dafür spricht, dass bereits anerkannte BCR auch nach Anwendbarkeit der DS-GVO als Rechtsgrundlage für Übermittlungen grundsätzlich tragfähig bleiben.

14.2 Safe Harbor / EU-U.S. Privacy Shield

Die aus dem Jahr 2000 stammende Safe-Harbor-Entscheidung der Europäischen Kommission wurde vom Europäischen Gerichtshof aufgehoben. Das Nachfolgeinstrument EU-U.S. Privacy Shield ist seit 1. August 2016 in Kraft und kann grundsätzlich für Datenübermittlungen an US-Unternehmen verwendet werden, die eine Privacy-Shield-Zertifizierung erworben haben.

Einem Paukenschlag gleich kam die Schrems-Entscheidung des Europäischen Gerichtshofs

vom 6. Oktober 2015 (Rechtssache C-362/14), mit der die Entscheidung der Europäischen Kommission aus dem Jahr 2000 zum sog. Safe Harbor für unwirksam erklärt wurde.

Die Kommissionsentscheidung wurde vom EuGH zum einen aufgehoben, weil der EuGH befand, dass die Kommission u. a. darin die Befugnisse der Datenschutzaufsichtsbehörden eingeschränkt hatte, ohne dafür nach der EG-Datenschutzrichtlinie befugt zu sein. Der zweite Grund zur Aufhebung von Safe Harbor lag darin, dass die Kommission es vor Erlass ihrer Safe-Harbor-Entscheidung versäumt hatte, die Rechtslage und Rechtspraxis in den USA tatsächlich umfassend im Hinblick auf den darin gewährleisteten Schutz personenbezogener Daten zu überprüfen. Dazu wäre die Kommission aber vor Erlass einer Angemessenheitsentscheidung wie im Falle von Safe Harbor verpflichtet gewesen. Die Kommission hätte überprüfen müssen, ob die Rechtslage und Rechtspraxis zum Schutz personenbezogener Daten einen Schutz gewährleisten, der demjenigen in der Europäischen Union im Wesentlichen gleichwertig ist und daher als „angemessenes Datenschutzniveau" anerkannt werden kann.

Durch die Entscheidung des EuGH vom 6. Oktober 2015 ist Safe Harbor ohne jegliche Übergangsfrist als mögliche Grundlage zur Erfüllung der Anforderungen der §§ 4b, 4c BDSG für Übermittlungen personenbezogener Daten in die USA weggefallen. Dieser Umstand stellte Unternehmen, die ihre Übermittlungen personenbezogener Daten an US-Unternehmen auf Safe Harbor gestützt hatten, vor erhebliche Probleme. Sie mussten kurzfristig die Übermittlungen auf eine andere valide Rechtsgrundlage stellen oder andernfalls die Übermittlungen beenden. Es war zu beobachten, dass gerade große US-Unternehmen, die (in der Regel als Auftragsdatenverarbeiter) Cloud-Computing-Leistungen anbieten und den Datenempfang aus der EU vorher auf Safe Harbor gestützt hatten, sehr kurzfristig nach dem 6. Oktober 2015 ihren Auftraggeber als Ersatz für Safe Harbor angeboten haben, einen Standardvertrag abzuschließen; dies ist verständlich angesichts dessen, dass aufgrund des Wegfalls von Safe Harbor die Gefahr bestand, dass die Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten Datentransfers aus der EU mangels einer Rechtsgrundlage auf der „zweiten Stufe" (Art. 25, 26 EG-Datenschutzrichtlinie) untersagen würden.

Auch die Europäische Kommission hat auf das Urteil des EuGH kurzfristig reagiert und ihre bereits seit 2013 laufenden Verhandlungen mit den US-Behörden zu einer Verbesserung von Safe Harbor noch einmal deutlich intensiviert, um rasch ein Nachfolgeinstrument für Safe Harbor vorzulegen. Am 29. Februar 2016 erklärte die Kommission, eine Einigung mit den USA erzielt zu haben und veröffentlichte unter dem Namen „EU-U.S. Privacy Shield" den Entwurf einer Angemessenheitsentscheidung nach Art. 25 Abs. 6 der EG-Datenschutzrichtlinie, die als Nachfolgeinstrument für Safe Harbor vorgesehen war. Die Kommission bat die Artikel-29-Gruppe um eine Stellungnahme zu dem Entwurf der Privacy-Shield-Entscheidung. Die Art. 29-Gruppe veröffentlichte am 29. April 2016 eine Stellungnahme, in der sie zwar im Privacy-Shield-Entwurf eine Reihe von Verbesserungen gegenüber der aufgehobenen Safe-Harbor-Entscheidung anerkannte, gleichzeitig aber noch signifikante Bedenken insbesondere im Hinblick auf den Umfang und die Verhältnismäßigkeit möglicher Datenzugriffe durch US-Nachrichtendienste und US-Sicherheitsbehörden auf aus der EU übermittelte personenbezogene Daten äußerte; es sei nicht hinreichend klar, ob ein massiver und unterschiedsloser Zugang der Behörden zu personenbezogenen Daten ausgeschlossen ist. Als fraglich bezeichnete die Art. 29-Gruppe daneben auch, ob die vom Privacy Shield als Rechtsschutzmöglichkeit für Betroffene vorgesehene Ombudsperson über hinreichende Befugnisse und ausreichende funktionelle Unabhängigkeit verfügt, wie dies in der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte

im Hinblick auf den Rechtsschutz Betroffener im Bereich nachrichtendienstlicher Maßnahmen gefordert wird.

Nach dieser kritischen Stellungnahme der Art. 29-Gruppe trat die Europäische Kommission in Nachverhandlungen mit der US-Seite ein, im Rahmen derer noch einige Änderungen erzielt wurden. Schließlich verabschiedete die Kommission am 12. Juli 2016 die neue Angemessenheitsentscheidung zum EU-U.S. Privacy Shield, die ab 1. August 2016 anwendbar wurde. Die Art. 29-Gruppe nahm am 26. Juli 2016 noch einmal in einer Pressemitteilung Stellung zur Endfassung des Privacy Shield, in der sie gewisse Restzweifel insbesondere im Hinblick auf die Stellung der Ombudsperson und auf die Frage massenhafter Datenzugriffe durch US-Behörden äußerte. Ungeachtet dessen ist durch die Angemessenheitsentscheidung der Kommission vom 12. Juli 2016 zunächst einmal verbindlich anerkannt, dass bei US-Unternehmen, die sich nach den Anforderungen des Privacy Shield zertifizieren, von einem angemessenen Datenschutzniveau ausgegangen werden kann. Damit ist es Unternehmen aus der EU grundsätzlich möglich, an zertifizierte US-Unternehmen personenbezogene Daten aus der EU zu übermitteln. Bis Ende 2016 hatte sich bereits eine mittlere dreistellige Anzahl von US-Unternehmen gemäß dem Privacy Shield zertifiziert. Der Privacy Shield basiert – wie zuvor Safe Harbor – auf einem System der Selbstzertifizierung. US-Unternehmen erklären gegenüber dem US-Handelsministerium verbindlich, die im Privacy Shield festgelegten Grundsätze zum Schutz personenbezogener Daten, die aus der EU übermittelt wurden, zu befolgen. Unternehmen müssen mit ihrer Selbsterklärung, die sie an das US-Handelsministerium zuleiten, eine Reihe von Nachweisen vorlegen, etwa dahingehend, dass sie eine Datenschutz-Policy besitzen und sich darin auf die Befolgung der Privacy-Shield-Grundsätze verpflichten. Enthält die Selbsterklärung alle erforderlichen Angaben – was vom US-Handelsministerium überprüft wird –, wird das US-Unternehmen auf die Privacy-Shield-Liste des US-Handelsministeriums gesetzt.

Link:
www.privacyshield.gov/list

Die Dauer der Gültigkeit der Zertifizierung beträgt 1 Jahr. Unternehmen, die ihre Zertifizierung nicht erneuern, werden von der Liste entfernt. Das US-Handelsministerium hat sich u. a. auch dazu verpflichtet, proaktiv zu überprüfen, ob Unternehmen möglicherweise auf ihren Internet-Präsenzen fälschlicherweise angeben, (noch) zertifiziert zu sein.

Ein wichtiges Element zum Gelingen des Privacy Shield wird die Bearbeitung von Beschwerden Betroffener sein, deren personenbezogene Daten an US-Unternehmen übermittelt wurden. Der Privacy Shield bietet mit der neu geschaffenen Funktion einer sog. Ombudsperson im US-Außenministerium nun erstmalig auch ein Instrument, um Beschwerden Betroffener zu bearbeiten, die einen rechtswidrigen Datenzugriff durch US-Nachrichtendienste befürchten. Betroffene aus der EU haben die Möglichkeit, derartige Beschwerden an eine neu zu schaffende zentrale Stelle, die bei der Art. 29-Gruppe angesiedelt sein wird, einzureichen, von wo aus die Beschwerden an die US-Ombudsperson weitergeleitet werden. Daneben haben Betroffene auch die Möglichkeit, Beschwerden einzulegen, wenn sie befürchten, dass ein zertifiziertes US-Unternehmen beim Umgang mit ihren Daten gegen die Privacy-Shield-Grundsätze verstoßen hat. Ein so genanntes Informelles Gremium, bestehend aus Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten, ist in bestimmten Fällen (insb. soweit es sich um Daten von Beschäftigten handelt) dafür zuständig, Beschwerden zu überprüfen und kann gegenüber den zertifizierten US-Unternehmen aus Anlass der Prüfung einer Beschwerde auch verbindliche Anweisungen über den Umgang mit personenbezogenen Daten im konkreten Fall erteilen. In anderen Fällen (insbesondere soweit es nicht

um Beschäftigtendaten geht) können die Datenschutzbehörden der EU-Mitgliedstaaten bei etwaigen Beschwerden Betroffener US-Behörden (US-Handelsministerium, Federal Trade Commission) um Überprüfung der Angelegenheit bitten.

Die Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten arbeiten derzeit an den noch notwendigen Schritten zur vollständigen Umsetzung der vom Privacy Shield geforderten Mechanismen. Insbesondere werden derzeit die Verfahrensregelungen des sog. Informellen Gremiums für die Bearbeitung von Beschwerden Betroffener erarbeitet. Geplant ist, auf den Webseiten der Datenschutzbehörden der Mitgliedstaaten ein Beschwerdeformular und Informationsmaterialien sowohl für Betroffene, d. h. für natürliche Personen, als auch Informationsmaterialien für europäische Unternehmen zum Privacy Shield bereitzustellen. Erste Informationen in der Gestalt von FAQ für Betroffene sowie für EU-Unternehmen wurden von der Art. 29-Gruppe bereits als Arbeitspapiere 245 und 246 verabschiedet und auf ihrer Website bereitgestellt.

Link:
http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Ungeachtet dieser praktischen Umsetzungsfragen dürfte zu erwarten sein, dass die Angemessenheitsentscheidung der EU-Kommission zum EU-U.S. Privacy Shield ebenso wie das Vorgängerinstrument Safe Harbor mittelfristig dem Europäischen Gerichtshof zur Überprüfung vorgelegt werden wird. Der EuGH hat im Schrems-Urteil vom 6. Oktober 2015 hohe Anforderungen an Angemessenheitsentscheidungen der Kommission formuliert. Besonders betont hat der EuGH dabei, dass die Datenschutzaufsichtsbehörden auch bei Bestehen einer Angemessenheitsentscheidung dennoch umfassend zur Prüfung von Beschwerden Betroffener zuständig bleiben und grundsätzlich auch in diesem Fall über ihre Befugnisse aus Art. 28 Abs. 3 EG-Datenschutzrichtlinie verfügen, mithin unter gewissen Umständen sogar in der Lage sein müssen, eine Datenübermittlung auszusetzen, um Verletzungen des Grundrechts auf informationelle Selbstbestimmung zu verhindern bzw. zu beenden.

Auch die Frage der Verhältnismäßigkeit von Datenzugriffen ausländischer Sicherheitsbehörden und Nachrichtendienste spielt ferner im Rahmen von Angemessenheitsentscheidungen eine wichtige Rolle. Der EuGH hat im Schrems-Urteil erneut betont, dass massenhafte und unterschiedslose Datenzugriffe unter bestimmten Umständen eine Verletzung des Grundrechts auf Achtung des Privatlebens (Art. 7 EU-Grundrechtecharta) darstellen kann. Allerdings hat er im Fall von Safe Harbor nicht entscheiden müssen, ob die Rechtslage und -praxis in den USA einen solchen Verstoß darstellen, vielmehr hat er die Safe-Harbor-Entscheidung der Kommission (unter anderem) schon deshalb für unwirksam erklärt, weil die Kommission es entgegen ihrer Verpflichtung versäumt hatte, zu überprüfen, ob die Rechtslage und Rechtspraxis in den USA tatsächlich einen Schutz personenbezogener Daten gewährleisten, der als „angemessenes Datenschutzniveau" angesehen werden kann. Es könnte aber durchaus sein, dass im Falle einer Überprüfung des Privacy Shield durch den EuGH die Frage des Schutzniveaus für personenbezogene Daten in den USA vom EuGH geprüft werden wird. Ob dabei – insbesondere mit Blick auf die Verhältnismäßigkeit von Datenzugriffen durch Nachrichtendienste – die Anforderungen an einen der EU-Schutzniveau im Wesentlichen vergleichbaren Schutz vom EuGH als erfüllt bewertet werden würden, bleibt abzuwarten.

14.3 Standardvertrag

Unternehmen versuchen oft, die EU-Standardverträge mit weiteren Regelungen zu ergänzen, um zusätzliche Fragen im Zusammenhang mit Datenübermitt-

lungen zu regeln oder die Standardvertragsklauseln spezifisch an ihre Bedürfnisse anzupassen. Hierbei ist aber Vorsicht angesagt, da Änderungen zum Nachteil der Betroffenen zur Genehmigungsbedürftigkeit der Übermittlung führen.

Im Berichtszeitraum erhielten wir immer wieder Kenntnis von Fällen, in denen Unternehmen für ihre Übermittlungen personenbezogener Daten in Drittstaaten zwar im Ausgangspunkt einen der drei zur Verfügung stehenden EU-Standardverträge (vgl. Kommissionsbeschlüsse Nr. 2001/497/EC vom 15.06.2001, Nr. 2004/915/EG vom 27.12.2004 sowie Nr. 2010/87/EU vom 05.02.2010) verwendeten, den Vertrag jedoch um zusätzliche datenschutzrechtliche Klauseln ergänzten. Eine solche Vorgehensweise kann unterschiedlichen Motiven entspringen. Eine typische Motivation hierfür ist, dass Konzerne bzw. Unternehmensgruppen für ihre konzerninternen Datenflüsse oft eine „One-fits-all"-Lösung anstreben, indem ein datenschutzrechtliches sog. Intra Group Agreement – d. h. ein Mehrparteienvertrag – aufgesetzt wird, an dem möglichst alle Konzerngesellschaften von inner- und außerhalb der EU als Datenexporteure und Datenimporteure beteiligt werden sollen. Je nachdem, ob die einzelne Übermittlung aus einem EU-Mitgliedstaat oder aber aus einem Nicht-EU-Staat stattfindet, wird der inkorporierte Standardvertrag für anwendbar erklärt (und oft um bestimmte Zusatzklauseln ergänzt) oder es werden (für Übermittlungen aus Nicht-EU-Staaten) andere Vertragsklauseln als der inkorporierte Standardvertrag für anwendbar erklärt. Häufig werden zu diesem Zweck die eigentlichen Standardvertragsklauseln in eine Anlage genommen, während in einem „Vorblatt" (das häufig erheblichen Umfang haben kann) zusätzliche Klauseln aufgestellt werden.

In mehreren von uns geprüften Vertragswerken dieser Art war bei Durchsicht der Zusatzklauseln zu den Standardvertragsklauseln festzustellen, dass darin Regelungen enthalten waren, die in inhaltlichem Widerspruch zu den Klauseln des angehängten Standardvertrags standen. Besonders häufig fanden sich Abweichungen in Vertragsklauseln großer international tätiger Auftragsdatenverarbeiter (insbesondere etwa bei einigen Anbietern von Cloud Computing). Ein typisches von uns festgestelltes Problem betrifft die Erteilung von Unteraufträgen. Gemäß Klausel 5h des Standardvertrags ist die Erteilung von Unteraufträgen durch den Datenimporteur nur mit vorheriger schriftlicher Zustimmung des Datenexporteurs möglich. Die Art. 29-Gruppe hat in ihrem Arbeitspapier 196 („Cloud Computing", dort Ziffer. 3.3.2) hierzu eine Vereinfachung nur insoweit als akzeptabel angesehen, dass der Auftragnehmer (Datenimporteur) den Auftraggeber (Datenexporteur) vor Erteilung des Unterauftrags über die Identität des avisierten (neuen) Unterauftragnehmers informiert und dem Auftraggeber ein Recht zum Widerspruch oder zur Vertragsbeendigung eingeräumt wird („Widerspruchslösung").

In mehreren von uns geprüften Vertragsklauseln war demgegenüber – unter Abweichung von Klauseln 5h des Standardvertrags sowie zur „Widerspruchslösung" – vorgesehen, dass der Datenimporteur Unterauftragnehmer nach eigener Entscheidung einschalten kann, d. h. ohne dass dem Auftraggeber insoweit ein Widerspruchsrecht zusteht. Eine derartige Klausel verschlechtert signifikant die Rechtsposition des Auftraggebers gegenüber dem EU-Standardvertrag. Ein solcher Vertrag kann nicht mehr als EU-Standardvertrag angesehen werden, sondern stellt einen sog. Ad-hoc-Datenexportvertrag dar, der gemäß § 4c Abs. 2 Satz 1 BDSG der Genehmigung der Datenschutzaufsichtsbehörde bedarf. Die Erteilung einer Genehmigung sähen wir in so einem Fall zudem als ausgeschlossen an, da es mit den Grundgedanken der Auftragsdatenverarbeitung nicht vereinbar ist, wenn die Einschaltung von Unterauftragnehmern im Belieben des Auftragnehmers stünde und der Auftraggeber

der Einschaltung des jeweiligen Unterauftragnehmers nicht verhindern könnte.

Eine weitere in mehreren von uns geprüften „ergänzten Standardverträgen" aufgefundene Klausel änderte das Auftragskontrollrecht des Auftraggebers und Datenexporteurs aus Klausel 5f des EU-Standardvertrags zur Auftragsdatenverarbeitung (Kommissionsentscheidung 2010/87/EU vom 05.02.2010) zum Nachteil des Datenexporteurs und Auftraggebers ab. Während Klausel 5f des EU-Standardvertrags vorsieht, dass der Datenexporteur die Datenverarbeitungseinrichtungen des Datenimporteurs entweder selbst prüfen oder durch einen von ihm ausgewählten externen Dritten prüfen lassen kann, sahen die von uns beanstandeten Zusatzklauseln vor, dass eine Auftragskontrolle ausschließlich durch Zertifikate, die Aussagen über die technisch-organisatorischen Maßnahmen beinhalten, erfolgt. In anderen Fällen sahen die Verträge vor, dass eine Auftragskontrolle ausschließlich durch einen externen Dritten möglich ist, der durch den Datenimporteur – d. h. nicht durch den Datenexporteur – benannt wird. Auch solche Klauseln führen zu einer signifikanten Verschlechterung der Position des Datenexporteurs gegenüber dem EU-Standardvertrag zur Auftragsdatenverarbeitung (Klausel 5f), so dass ein um derartige Klauseln „ergänzter" Standardvertrag nicht als EU-Standardvertrag, sondern auch als (nicht genehmigungsfähiger) Ad-hoc-Datenexportvertrag anzusehen ist.

In den Fällen, in denen wir derartige signifikante Abweichungen von den Klauseln der EU-Standardverträge festgestellt haben, haben wir den Unternehmen, die derartige Klauseln verwenden wollten, unsere rechtliche Bewertung mitgeteilt und erklärt, dass ein Datenexport auf dieser Grundlage genehmigungsbedürftig nach § 4c Abs. 2 S. 1 BDSG ist, wir jedoch eine Genehmigungserteilung aus den genannten Gründen nicht für möglich halten. In geeigneten Fällen haben wir zudem auch direkt Kontakt mit Deutschland-Niederlassungen der Datenimporteure (meist Anbieter von Cloud-Computing-Diensten) aufgenommen, die die entsprechenden Verträge vorformuliert hatten, und haben ihnen unsere Bewertung mitgeteilt. Unsere Anmerkungen wurden akzeptiert. Die Unternehmen sagten zu, die entsprechenden Klauseln abzuändern und haben uns bereits in mehreren Fällen geänderte Fassungen vorgelegt. Wichtig erscheint es uns zudem, gerade Cloud-Computing-Anbieter, die ihre Dienste in mehreren (meist: in allen) EU-Mitgliedstaaten anbieten, darauf hinzuweisen, dass sie bei Verwendung von abgewandelten bzw. „ergänzten" Standardverträgen die Gefahr eingehen, dass zumindest einige der Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten den entsprechenden Vertrag als Abweichung von den EU-Standardvertragsklauseln qualifizieren und die entsprechenden Datenexporte aus den betreffenden Mitgliedstaaten somit u. U. zumindest nicht genehmigungsfrei (und u. U. auch nicht genehmigungsfähig) sind.

Da Cloud-Computing-Konzerne typischerweise denselben Vertragstext für Kunden (Auftraggeber) aus allen EU-Mitgliedstaaten anbieten möchten (oft bieten sie potentiellen Kunden den Datenschutzvertrag zum Download auf ihrer Homepage an), besteht für sie in solchen Fällen die Möglichkeit, eine koordinierte Beurteilung des Vertragstexts durch die Aufsichtsbehörden aller betroffenen EU-Mitgliedstaaten vornehmen zu lassen.

Diese Möglichkeit der koordinierten behördlichen Prüfung wird im Arbeitspapier 226 der Art. 29-Gruppe aufgezeigt und angeboten. Die Aufsichtsbehörden haben allerdings erklärt, nur solche Datenexportvertrags-Entwürfe der koordinierten Prüfung zu unterziehen, bei denen als Kern des Vertrags einer der EU-Standardverträge verwendet wird und allenfalls in begrenztem Umfang gewisse Zusatzklauseln zum Standardvertrag vorgesehen sind. Gegenstand der Prüfung ist bei dieser koordinierten Prüfung die Frage, ob die Zusätze bzw. Abweichungen von den EU-Standardvertragsklauseln

noch als so geringfügig angesehen werden können, dass der Vertrag als noch im Einklang mit den EU-Standardvertragsklauseln stehend eingestuft werden kann.

Durch die von den Aufsichtsbehörden im Arbeitspapier 226 angebotene koordinierte Bewertung des Vertragstextes erhält der Konzern eine verbindliche Aussage aller Datenschutzbehörden der Mitgliedstaaten, in denen er den Vertrag als Grundlage für Datenexporte in Drittstaaten zum Einsatz bringen möchte. Es ist allerdings festzustellen, dass bislang nur verhältnismäßig wenige Konzerne auf freiwilliger Basis eine solche koordinierte Überprüfung ihrer Datenexportverträge durch die Aufsichtsbehörden in Anspruch genommen haben. Konzerne, die diese Möglichkeit nicht in Anspruch nehmen, nehmen somit in Kauf, dass ein etwaiger von ihnen verwendeter „abgewandelter Standardvertrag" von den Datenschutzaufsichtsbehörden unterschiedlicher Mitgliedstaaten unterschiedlich bewertet wird und sie somit möglicherweise nicht EU-weit denselben Vertragstext zum Einsatz bringen können.

15

Beschäftigtendatenschutz

15 Beschäftigtendatenschutz

15.1 Veröffentlichung von Mitarbeiter-Krankheitstagen

Das Aushängen von Krankheitszeiten der Mitarbeiter in personenbezogener Form durch den Arbeitgeber ist unzulässig.

Ein Mitarbeiter eines Unternehmens beschwerte sich bei uns darüber, dass sich im dortigen Büro eine Pin-Wand befinde, die für jedermann einsehbar sei. Auf dieser Pin-Wand befänden sich die Urlaubs- und Fehltage mit Personalnummer und Namen der jeweiligen Mitarbeiter.

Nach § 4 Abs. 1 BDSG ist das Erheben, Verarbeiten und Nutzen personenbezogener Daten nur zulässig, wenn eine Vorschrift des BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder wenn der Betroffene eingewilligt hat. Die Mitarbeiter waren hier mit dem Aushängen der Krankheitstage weder einverstanden noch existierte eine gesetzliche Vorschrift, die eine solche Bekanntgabe erlaubt. Somit war das Aushängen unzulässig. Wir haben das Unternehmen auf den Datenschutzverstoß hingewiesen. Das Unternehmen war einsichtig und teilte mit, die „Übersichtswand" umgehend zu entfernen. Wir haben uns dennoch auf Grund des nicht unerheblichen Vorfalls dazu entschieden, den Verstoß mit einem Bußgeld zu ahnden. Der Bußgeldbescheid hierzu wurde rechtskräftig.

15.2 Weitergabe von Mitarbeiter-Krankheitstage durch Personalstelle an Vorgesetzte

Wenn die Personalstelle eines Unternehmens die Zahl der Krankheitstage von Mitarbeitern an deren Vorgesetzten weitergibt, kann dies datenschutzrechtlich zulässig sein.

Ein Unternehmen fragte an, ob die Personalstelle die krankheitsbedingten Fehlzeiten von Mitarbeitern an deren Vorgesetzten weitergeben und wie dieser die Daten verwenden dürfe. Bei den krankheitsbedingten Fehlzeiten handelt es sich um besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG. Die Zulässigkeit der beabsichtigten Datennutzung bemisst sich deshalb nach § 28 Abs. 6 Nr. 3 BDSG. Für die zu treffende Entscheidung ist zu berücksichtigen, dass die Daten nicht allzu sensibel sind und es sich um eine innerbetriebliche Weitergabe handelt. Notwendig ist allerdings auch, dass die Weitergabe der betreffenden Daten für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. Das ist z. B. dann anzunehmen, wenn der Vorgesetzte diesen Aspekt bei der Personalplanung berücksichtigen oder in einem Mitarbeitergespräch im Hinblick auf eine mögliche Arbeitsüberlastung ansprechen möchte. Nicht zulässig wäre es, wenn der Vorgesetzte die krankheitsbedingten Fehlzeiten seiner Mitarbeiter bspw. bei einer Besprechung anderen Abteilungsleitern mitteilen würde, weil dies nicht erforderlich wäre (andere Abteilungsleiter haben mit den betreffenden Mitarbeitern nichts zu tun).

15.3 GPS-Überwachung der Mitarbeiter in Dienstfahrzeugen zur Einsatzsteuerung

Der GPS-Einsatz in Geschäftsfahrzeugen ist nur für wenige bestimmte Zwecke wie Einsatzsteuerung und ggf. Arbeitszeitfeststellung zulässig.

Ein Mitarbeiter eines Unternehmens hatte sich darüber beschwert, dass in den Dienstfahrzeu-

gen seines Unternehmens neuerdings eine GPS-Überwachung stattfinde. Um den Zweck des Einsatzes von GPS zu erfahren, haben wir die verantwortliche Stelle kontaktiert. Das Unternehmen teilte mit, die Ortung erfolge zur Koordination von Eilaufträgen und zur Arbeitszeitfeststellung, ggf. auch zur Klärung von Unstimmigkeiten mit Kunden. Die Daten der Fahrzeuge würden bei Stillstand alle 30 Minuten und während der Fahrt im Abstand von 600 Metern aufgezeichnet. Außerdem würde auch die gefahrene Geschwindigkeit erfasst.

Der Arbeitgeber darf Mitarbeiterdaten u. a. dann erheben, verarbeiten oder nutzen, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist (§ 32 Abs. 1 Satz 1 BDSG). Dies bejahen wir bei einem GPS-Einsatz im bestimmten Umfang zur Koordinierung von Aufträgen (z. B. in der Logistik). Auch zur Zeiterfassung für die im Außendienst Beschäftigten kann es zulässig sein, wenn Beginn und Ende der Arbeitszeit mit Beginn und Ende der Fahrt mit dem Dienstfahrzeug zusammenfallen und gleichzeitig keine weiterführende Überwachung (z. B. nach Dienstschluss) möglich ist. Wir hielten im konkreten Fall die punktuellen Aufzeichnungen für noch vertretbar, weil hier die Abstände angemessen sind, eine lückenlose Totalkontrolle der Mitarbeiter aber nicht erfolgt. Die Aufzeichnungen können so auch für die Fälle von Unstimmigkeiten mit Kunden herangezogen werden. Wir weisen darauf hin, dass die Intervalle zur Erfassung von Standortdaten auf Grund der möglichen Rückschlüsse auf das Verhalten einzelner Personen durch deren Bewegungsmuster auch in solchen Anwendungsfällen nicht zu klein sein dürfen.

Für zu weitgehend und damit unzulässig hielten wir im vorliegenden Beschwerdefall das Nutzen der erfassten gefahrenen Geschwindigkeit, weil die verantwortliche Stelle die Erforderlichkeit dieser Datenerhebung nicht belegen konnte. Wir forderten das Unternehmen deshalb auf, es zu unterlassen, die gefahrene Geschwindigkeit zu erfassen.

15.4 Bewerbungen über Externe

Erweckt ein Unternehmen im Rahmen einer Stellenanzeige den Eindruck, die Person, an die die Bewerbungen gesendet werden sollen, gehöre zum Unternehmen, obwohl es sich um einen Externen handelt, der eine Vorauswahl für das Unternehmen trifft, ist dies unzulässig.

In einem uns vorgetragenen Beschwerdefall hatte sich eine Person auf eine Stellenanzeige eines Unternehmens beworben, wobei dieses darum bat, die Bewerbungsunterlagen zu Händen eines bestimmten Herren zu schicken, dessen E-Mail Adresse aus Vor- und Nachnamen sowie im zweiten Teil aus dem Namen des Unternehmens bestand. Es wurde somit der Eindruck erweckt, es handle sich dabei um einen Mitarbeiter des Unternehmens. Tatsächlich war es aber der Geschäftsführer eines Personalberatungsunternehmens, das unter den eingegangenen Bewerbungen eine Vorauswahl treffen sollte.

Das Verhalten des Unternehmens war nicht korrekt. Es hätte auf die Tatsache, dass eine andere verantwortliche Stelle die Bewerbungen erhält und eine Vorauswahl, also eine eigene Entscheidung trifft, gemäß § 4 Abs. 3 Nr. 3 BDSG in der Stellenanzeige hinweisen müssen, da die Bewerber aufgrund der Gesamtumstände mit einer solchen Weitergabe nicht rechnen konnten bzw. mussten. Nur dann ist es eine freie Entscheidung jedes Einzelnen, ob er diesen Umstand akzeptiert und sich in Kenntnis dessen bewirbt oder ob er dann von einer Bewerbung Abstand nimmt.

Wir haben daher auf das Defizit hingewiesen und für eine Anpassung des Bewerbungsprozesses gesorgt.

15.5 Gesprächsaufzeichnung in Call Centern

Das Aufzeichnen von Telefonaten in Call Centern zum Zweck des Supports von Kunden ist nur mit Einwilligung des jeweiligen Mitarbeiters und dessen Gesprächspartners möglich.

Ein Unternehmen fragte bei uns an, ob es zulässig sei, Telefongespräche der Mitarbeiter im unternehmenseigenen Call Center aufzuzeichnen. Der Zweck der Gesprächsaufzeichnung sei es, die von den Kunden geschilderten Probleme mit den beim Unternehmen gekauften Geräten auf diese Weise besser lösen zu können. Außerdem könne der Arbeitgeber auf diese Weise überprüfen, ob bei dem jeweiligen Mitarbeiter ein gewisser Schulungsbedarf bestehe.

Für die Aufzeichnung der Telefongespräche ist im Hinblick auf § 201 StGB (Verletzung der Vertraulichkeit des gesprochenen Wortes) die Einwilligung der Mitarbeiter und die des Kunden zwingend erforderlich. Der Kunde muss dazu zu Beginn des Telefongesprächs über die Absicht der Aufzeichnung informiert werden, um frei entscheiden zu können, ob er damit einverstanden ist oder die Aufzeichnung ablehnt. Der Mitarbeiter des Unternehmens kann im Gegensatz dazu bereits zu Beginn seiner Tätigkeit pauschal für die Aufzeichnung von Telefongesprächen einwilligen. Sollte ein Mitarbeiter mit dem Aufzeichnen der Telefongespräche jedoch nicht einverstanden sein, ist ein Einsatz im Bereich des Call Center sicherlich erschwert, jedoch nicht unmöglich.

Bei Telefonaufzeichnungen in Call Centern weisen wir darauf hin, dass ein Arbeitgeber nicht auf jedes Gespräch zugreifen, sondern die Auswertung auf bestimmte Anwendungsfälle eingrenzen sollte (z. B. bei neuen Mitarbeitern). Auch ein Durchführen von Stichproben oder die Beschränkung auf Fälle von Meinungsverschiedenheiten mit Kunden sind mögliche Umsetzungsszenarien.

Eine anlasslose und permanente Aufzeichnung aller Gespräche der Mitarbeiter eines Call Centers ist nicht zulässig.

15.6 Weiterleitung von E-Mails an einen Kollegen nach Ausscheiden des Mitarbeiters

Die Weiterleitung dienstlicher E-Mails an einen Kollegen nach Ausscheiden eines Mitarbeiters kann im Einzelfall vertretbar sein.

Ein Unternehmen wandte sich mit der Frage an uns, ob es erlaubt sei, nach Ausscheiden eines Mitarbeiters eine Weiterleitung der in seinem E-Mail-Postfach eingehenden E-Mails vorzunehmen. Wir wiesen zunächst darauf hin, dass es vertretbar ist, wenn der E-Mail Account eines ausgeschiedenen Mitarbeiters noch für eine gewisse Zeit vorgehalten wird, weil erfahrungsgemäß noch eine gewisse Zeit E-Mails, die an den ausgeschiedenen Mitarbeiter gerichtet sind, dort eingehen. Nach etwa drei Monaten sollte dieser aber dann geschlossen werden.

Bei der Frage, ob die Weiterleitung möglich ist, ist zu unterscheiden, ob die private E-Mail-Nutzung erlaubt ist oder nicht. Wenn die Privatnutzung verboten ist, kann der Arbeitgeber einseitig Regelungen treffen, wie beim Ausscheiden eines Mitarbeiters mit den auf dessen E-Mail-Account eingehenden E-Mails zu verfahren ist. Zwar ist das Setzen einer Abwesenheitsnotiz die datenschutzfreundlichere Lösung, doch kann auch eine Weiterleitung vertretbar sein. Falls private E-Mails eingehen sollten, was sich auch bei einem Verbot der Privatnutzung nicht verhindern lässt, würden diese auch weitergeleitet werden. Diese dürften von dem Kollegen, an den sie weitergelei-

tet werden, jedoch nicht gelesen werden. Je nach Festlegung wären private E-Mails zu löschen oder, sofern vereinbart, an den ausgeschiedenen Mitarbeiter weiterzusenden.

Ist die Privatnutzung erlaubt, ist die Schutzwürdigkeit des Mitarbeiters entsprechend höher, weil der Arbeitgeber als Diensteanbieter im Sinne des Telekommunikationsgesetzes anzusehen und infolgedessen das Fernmeldegeheimnis zu beachten ist. Hier wäre – wie auch in der Orientierungshilfe des Düsseldorfer Kreises zur E-Mail- und Internet-Nutzung vorgesehen – eine Einwilligungslösung geboten.

Link:
www.lda.bayern.de/media/oh_email_internet.pdf

Es handelt sich um eine freiwillige Leistung des Arbeitgebers, wenn er die private E-Mail-Nutzung gestattet, so dass er dann auch die Bedingungen vorgeben kann, zu denen er zur Gestattung bereit ist. Neben der Einräumung gewisser Zugriffsmöglichkeiten könnte in diesem Zusammenhang auch die Weiterleitung der eingehenden E-Mails an einen Kollegen und die Behandlung eingehender privater E-Mails in den Fällen vorübergehender Abwesenheit und bei Ausscheiden geregelt werden. Ist der Mitarbeiter dann mit den Bedingungen einverstanden, sind die entsprechenden Datenumgänge durch den Arbeitgeber zulässig, weil sie von der Einwilligung gedeckt sind. Akzeptiert der Mitarbeiter die Bedingungen des Arbeitgebers nicht, ist für ihn die private Nutzung verboten und nur die dienstliche erlaubt, mit der Folge, dass in der weiter oben beschriebenen Weise zu verfahren ist.

15.7 Erneuerung der Verpflichtung auf das Datengeheimnis

Die Verpflichtung auf das Datengeheimnis sollte in regelmäßigen Abständen wiederholt werden.

Jede verantwortliche Stelle ist gemäß § 5 Satz 2 verpflichtet, seine Mitarbeiter auf das Datengeheimnis nach 5 Satz 1 BDSG zu verpflichten. In vielen Unternehmen erfolgt dies mit der Aufnahme der Tätigkeit, sei es durch eine Zusatzregelung zum Arbeitsvertrag oder durch eine Handlung kurz nach Arbeitsaufnahme. Es ist anzuraten, diese Verpflichtung oder eine Sensibilisierungsmaßnahme hierzu regelmäßig zu wiederholen, wenn diese Verpflichtung längere Zeit zurückliegt. Dies gilt insbesondere, wenn der Mitarbeiter mit einer Aufgabe betraut ist, die Zugang zu besonderen Arten von Daten hat oder er eine Administratorentätigkeit ausübt, die den Zugang zu einer umfangreichen Menge an personenbezogenen Daten ermöglicht.

Ausblick zur DS-GVO:
Eine dem § 5 BDSG vergleichbare Regelung ist in der DS-GVO nicht direkt enthalten. Jedoch hat der Verantwortliche nach Art. 24 Abs. 1 DS-GVO und der Auftragsverarbeiter nach Art. 28 Abs. 1 DS-GVO geeignete (technische und organisatorische) Maßnahmen zu treffen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Hinsichtlich einer Wiederholung bzw. „Auffrischung" dieser Verpflichtungen werden die Anforderungen aufgrund der Nachweisverpflichtung sogar eher steigen.

16

Gesundheit und Soziales

16 Gesundheit und Soziales

16.1 Verlassenes Krankenhaus

Wenn eine verantwortliche Stelle ihren Geschäftsbetrieb ungeordnet einstellt, kann dies zu gravierenden datenschutzrechtlichen Problemen führen.

Durch Medienberichte haben wir erfahren, dass in einem ehemaligen Krankenhaus Patientenakten offen herumliegen würden und das Gelände insgesamt in einem sehr schlechten Zustand sei, so dass der Aufwand für unbefugte Dritte, an diese Daten heranzukommen, sehr gering sei.

Unsere Recherchen ergaben, dass das Krankenhaus zunächst von einer Familie betrieben worden war. Als die Familienmitglieder sich zur Ruhe setzen wollten, übergaben sie das Krankenhaus an einen Konzern, der kurze Zeit später Insolvenz anmelden musste. Danach wurde das Gelände zwar noch kurz von einem weiteren Krankenhaus verwendet, dann aber letztendlich sich selbst überlassen und – kurz vor den Medienberichten darüber – von einem neuen Eigentümer erworben.

Bei einem Ortstermin mit dem neuen Eigentümer konnten wir feststellen, dass sich noch aus allen Nutzungszeiträumen Akten in dem weit verzweigten Gelände mit mehreren Gebäuden befanden. Inzwischen waren alle Gebäude in einem äußerst schlechten Zustand und wiesen Spuren von Vandalismus auf. Wir konnten mit dem neuen Eigentümer schon vor dem gemeinsamen Ortstermin vereinbaren, dass er unverzüglich einen Zaun um das Gelände errichtet um den Zugang etwas zu erschweren. Weiterhin wurden nach unserer Besichtigung alle Akten unter Aufsicht des Datenschutzbeauftragten des neuen Eigentümers datenschutzkonform vernichtet. Wir hielten es in diesem Fall für vertretbar, trotz eventuell in Einzelfällen möglicherweise noch laufender Aufbewahrungsfristen alle Akten der Vernichtung zuzuführen, da aufgrund der unübersichtlichen Lage und der Aktenunordnung eine manuelle Sortierung und Auswertung nicht mit verhältnismäßigen Mitteln möglich war. Vorher gab der neue Eigentümer den Vorbesitzern bzw. deren Rechtsnachfolgern aber noch Gelegenheit, sich selbst um die Akten zu kümmern.

Der Fall zeigt, dass bei der Übergabe von Datenbeständen und Geschäftsaufgaben genaue Regelungen getroffen werden sollten und auch Insolvenzverwalter ein Augenmerk auf einen sicheren und datenschutzkonformen Umgang mit den verbliebenen Akten haben sollten.

16.2 Betriebsarztwechsel

Beim Wechsel des Betriebsarztes kommt es regelmäßig zu Unsicherheiten, wie mit der ärztlichen Schweigepflicht einerseits und den Verpflichtungen des Arbeitgebers zur Dokumentation der Arbeitssicherheitsmaßnahmen andererseits umgegangen werden muss.

Nachdem die datenschutzrechtlich verantwortliche Stelle für die betriebsärztliche Tätigkeit der Arbeitgeber ist (§ 1 Abs. 1 Arbeitssicherheitsgesetz (ArbSiG)), können die Akten, wenn der Betriebsarzt aus dieser Tätigkeit ausscheidet, nicht bei diesem verbleiben. Sie müssen beim Arbeitgeber weitergeführt werden. Nachdem der Betriebsarzt aber weiterhin der Schweigepflicht unterliegt (§ 8 Abs. 1 Satz 3 ArbSiG), darf der Arbeitgeber keine Einsicht in die Akten nehmen. Dies obliegt nur dem nachfolgenden Betriebsarzt. Die Einsicht durch den neuen Betriebsarzt ist durch seine Tätigkeit und seine Aufgaben nach den Arbeitsschutzgesetzen gerechtfertigt. Die Akten aus der betriebsärztlichen Tätigkeit müssen vom ausscheidenden Arzt deshalb grundsätzlich an den

nachfolgenden Betriebsarzt übergeben werden. Etwas anderes gilt für die Aufzeichnungen, die außerhalb der betriebsärztlichen Aufgaben getätigt wurden.

Vor der Übergabe sind die noch beschäftigten Mitarbeiter vom geplanten Wechsel umfassend zu informieren. Die Information muss auch enthalten, wer der neue Betriebsarzt werden soll und ist so zu formulieren, dass den Mitarbeitern das Ausmaß der Dokumentation deutlich wird. Weiterhin muss ihnen ausreichend Zeit für einen Widerspruch gegen die Übergabe eingeräumt werden. Akten zu bereits ausgeschiedenen Mitarbeitern müssen ebenfalls übergeben werden, sind aber zu sperren. Im Fall des Widerspruchs sind die Akten ebenfalls zu sperren. Die gesperrten Akten dürfen nicht vom neuen Betriebsarzt zur Kenntnis genommen werden; sie sind besonders geschützt im Betrieb aufzubewahren bis die Löschungsfrist erreicht ist. Nachdem sich der Arbeitnehmer bei einem späteren Bedarf eher an den früheren Arbeitgeber wenden wird, ist die Verwahrung im Betrieb unter Verschluss durch den amtierenden Betriebsarzt sachgerecht. Auf die Akten kann in der Regel nur zurückgegriffen werden, wenn der betroffene Mitarbeiter dies veranlasst. Dieser kann dann ggf. auch Aussagen treffen, ob der neue Betriebsarzt von den Akten Kenntnis nehmen darf. Selbstverständlich muss der neue Betriebsarzt nach Ablauf der Aufbewahrungsfristen auch für die ordnungsgemäße Entsorgung der Akten Sorge tragen.

Ausblick zur DS-GVO:
Nach Art. 9 Abs. 2 h) DS-GVO kann die Verarbeitung personenbezogener Daten zu Zwecken der Arbeitsmedizin auf Grundlage des Rechts der Union oder eines Mitgliedstaates gerechtfertigt sein, sofern die Verarbeitung durch Personal stattfindet, das einem Berufsgeheimnis oder einer ähnlichen Geheimhaltungspflicht unterliegt. Derzeit gehen wir davon aus, dass auf Grundlage dieser Öffnungsklausel die bestehenden Regelungen hierzu auch nach dem Mai 2018 Bestand haben.

16.3 Löschung von Patientendaten vor vollständiger Auskunftserteilung

Eine Klinik löschte Patientendaten, obwohl die Betroffene noch keine vollständige Auskunft erhalten hatte.

Eine Patientin trug vor, dass sie zu ihren Klinikaufenthalten in den Jahren 2004 und 2005 keine vollständige Auskunft erhalten habe. Sie habe sich kurz vor Ablauf der 10-jährigen Aufbewahrungsfrist an die Klinik gewandt, um die zu ihren beiden Aufenthalten gespeicherten Daten zu erhalten, bevor diese gelöscht bzw. vernichtet werden. Als sie wegen fehlender Unterlagen nachfragte, wurden ihr zum Aufenthalt im Jahr 2005 weitere Unterlagen zugeschickt und ihr außerdem mitgeteilt, dass die Daten zum Aufenthalt im Jahr 2004 bereits gelöscht bzw. die dazugehörigen Unterlagen vernichtet seien.

Nach den uns hierzu vorliegenden Unterlagen erfolgte die Vernichtung allerdings zu einem Zeitpunkt, zu dem der Klinik bekannt gewesen sein musste, dass die Patientin ein weitergehendes Auskunftsrecht geltend macht. Diese weitergehenden Auskünfte wurden der Patientin zunächst verweigert, weil sie subjektive Eindrücke oder Wahrnehmungen der Ärzte enthielten und nach Ansicht der Klink deshalb vom Auskunftsrecht der Patientin nicht erfasst gewesen seien. Die Löschung bzw. Vernichtung personenbezogener Daten richtet sich nach § 35 BDSG. Gemäß § 35 Abs. 3 Nr. 2 BDSG tritt an die Stelle der Löschung eine Sperrung, wenn Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden. Diese Voraussetzungen lagen hier vor. Es war der Klinik bekannt, dass die Patientin die ihr erteilten

Auskünfte als unvollständig angesehen und deshalb weitere Auskünfte verlangt hat. Es war auch noch nicht abschließend geklärt, ob die Patientin Auskunft zu den ihr zunächst vorenthaltenen Daten verlangen kann, denn die Patientin hatte insoweit noch nicht alle rechtlichen Möglichkeiten ausgeschöpft, um eine ihrer Ansicht nach erforderliche Auskunftserteilung durchzusetzen (z. B. Einschaltung der Aufsichtsbehörde, zivilrechtliche Geltendmachung). Die Vernichtung hätte deshalb so lange zurückgestellt werden müssen, bis abschließend geklärt ist, dass der Patientin keine weitergehenden Auskünfte mehr zu erteilen sind.

Wir haben deshalb festgestellt, dass die Löschung der Unterlagen zu dem Krankenhausaufenthalt der Patientin aus dem Jahr 2004 unzulässig war.

16.4 Elektronische Erreichbarkeit von Ärzten und Apotheken

Wenn Ärzte und Apotheken für ihre Patienten bzw. Kunden elektronisch erreichbar sein wollen, müssen sie wegen der Sensibilität der eingehenden Nachrichten höhere Datensicherheitsmaßnahmen ergreifen.

Auch Ärzte und Apotheken wollen außerhalb von Sprech- und Öffnungszeiten für ihre Patienten und Kunden erreichbar sein und stellen deshalb auf ihren Internetseiten vermehrt Kontaktformulare zur Verfügung. Auch bieten sie zum Teil an, sich mit einem Anliegen per E-Mail dorthin zu wenden.

Apotheken integrieren in ihre Webseiten beispielswiese Formulare, damit online Medikamente vorbestellt werden können. Auch Ärzte stellen den Nutzern ihrer Internetseite immer öfter Kontaktmöglichkeiten zur Verfügung oder nennen mindestens eine E-Mail-Adresse mit dem Hinweis, dass sich der Patient mit seinen Wünschen auch auf diesem Weg an die Praxis wenden kann – auch wenn es sich nur um eine Terminvereinbarung für eine gewöhnliche Behandlung handeln sollte. Diese Angebote haben wir im Berichtszeitraum einzelfallbezogen einer Prüfung unterzogen. Da sich die Anfragen gerade im Bereich von Ärzten und Apotheken gehäuft haben, listen wir in den nachfolgenden Passagen die grundsätzlichen Rahmenbedingungen auf, die zumindest aus datenschutzrechtlicher Sicht dabei beachtet werden müssen.

Wenn Ärzte oder Apotheken ein Kontaktformular (oder aktiv eine E-Mail-Erreichbarkeit) anbieten, ist davon auszugehen, dass Patienten bzw. Kunden auf diesem Weg auch Angaben zur Gesundheit – besondere Arten personenbezogener Daten i. S. d. § 3 Abs. 9 BDSG – übermitteln. Der Schutzbedarf der übermittelten Daten ist deshalb sowohl für die Inhalts- als auch für die Verkehrsdaten sehr hoch. Gemäß § 9 BDSG haben nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen zu gewährleisten. Nach der Weitergabekontrolle in Nr. 4 der Anlage zu § 9 BDSG ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Zu diesem Zweck sind dem Stand der Technik entsprechende Verschlüsselungsverfahren zu verwenden (Satz 3 der Anlage zu § 9 BDSG). Daneben haben Diensteanbieter nach § 13 Abs. 7 Satz 1 Telemediengesetz (TMG), soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Ein-

richtungen möglich ist und diese gegen Verletzungen des Schutzes personenbezogener Daten und gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind, gesichert sind. Dabei ist der Stand der Technik zu berücksichtigen (§ 13 Abs. 7 Satz 2 TMG). Eine Maßnahme ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens (§ 13 Abs. 7 Satz 3 TMG).

Für den Einsatz von Kontaktformularen sind folgende Punkte zu berücksichtigen:

- Es muss eine Transportverschlüsselung des Kontaktformulars zum Webserver nach Stand der Technik und dem Schutzbedarf entsprechend eingesetzt werden. Dies setzt momentan das Protokoll TLS 1.2, den Einsatz der Verschlüsselungstechnik Perfect Forward Secrecy als auch eine Schlüssellänge von 4096-Bit RSA als (Mindest-)Anforderung voraus.
- Zusätzlich muss der Inhalt der Kommunikation mittels eines Verfahrens zur Ende-zu-Ende-Verschlüsselung abgesichert werden (z. B. PGP mit 4096-Bit). Dies kann beispielsweise durch eine Verschlüsselung innerhalb des Browsers (mittels Javascript) realisiert werden.
- Als Alternative zur Ende-zu-Ende-Verschlüsselung des Kontaktformulars kann eine Ende-zu-Ende-Verschlüsselung der E-Mail-Kommunikation angeboten werden. Hierfür muss der dazugehörende öffentliche Schlüssel hinterlegt werden. Zusätzlich muss dann noch auf die fehlende Sicherheit des Kontaktformulars hingewiesen werden, d. h. dass bei diesem übertragene Inhalte möglicherweise von Unbefugten im Klartext abgefangen bzw. mitgelesen werden können. Ein Verweis auf den (sicheren) Postweg stellt jedoch keine geeignete Alternative dar, denn wir fordern, dass es sich um eine Alternative „ohne Medienbruch" handeln muss. Wer seinen Nutzern also eine elektronische Erreichbarkeit anbieten möchte, muss auch für ausreichende Datensicherheit sorgen. Eine pauschale „Warnung" vor Sicherheitslücken oder Risiken der Internetnutzung ist nicht ausreichend. Vor allem entbindet diese den Diensteanbieter nicht von der Anforderung, eine dem Stand der Technik und dem Schutzbedarf der Daten angemessene Verschlüsselung ohne Medienbruch zumindest als Alternative anzubieten.

Für das Angebot von Ärzten und Apotheken, mit den Patienten bzw. Kunden per E-Mail zu kommunizieren, sind folgende Punkte zu berücksichtigen:

- Zur möglichen Verschlüsselung der Kommunikation zwischen Mailservern ist unabhängig vom Schutzbedarf der personenbezogenen Daten eine Transportverschlüsselung mit dem STARTTLS-Protokoll als notwendig zu betrachten. Zum wirksamen Schutz der übermittelten Daten ist zudem der Einsatz der Verschlüsselungstechnik Perfect Forward Secrecy erforderlich, um ein nachträgliches Entschlüsseln von aufgezeichneten Transportdaten massiv zu erschweren.
- Zusätzlich muss auch hier der Inhalt der Kommunikation mittels eines Verfahrens zur Ende-zu-Ende-Verschlüsselung abgesichert werden.

Ein Unterschreiten dieser Sicherheitsanforderung ist nur mit Einwilligung des Betroffenen möglich und nur zulässig, wenn den Patienten bzw. Kunden eine sichere Alternative, wie oben beschrieben, ohne Medienbruch (d. h. Verweis auf Post nicht ausreichend) angeboten wird. Der Nutzer muss zudem deutlich und verständlich darüber informiert werden, welcher Übertragungsweg dem Stand der Technik entspricht und welcher nicht – und vor der weniger sicheren Versendung aktiv (z. B. durch Setzen eines Häkchens) bestätigen, dass er trotz der Mög-

lichkeit der sicheren Versendung seine Daten lediglich per transportverschlüsselter E-Mail übertragen möchte.

Wir haben diesen Sachverhalt bereits ausführlich im Kapitel 22 unseres 6. Tätigkeitsberichts dargestellt.

Link:
www.lda.bayern.de/media/baylda_report_06.pdf

16.5 Nutzung von Rezeptdaten für Werbezwecke

Rezeptdaten dürfen nur zweckgebunden verwendet und keinesfalls dafür genutzt werden, den Patienten zu bewerben.

Der Hersteller eines orthopädischen Hilfsmittels hat die ihm vorliegenden Angaben zu den Patienten genutzt, um diese persönlich anzuschreiben und unter Bezugnahme auf die konkrete Verletzung und das genutzte Hilfsmittel weitere Tipps zur Genesung zu erteilen sowie hilfreiche Artikel seiner Partnerfirma und eine weitere telefonische Beratung anzubieten.

Die auf dem Rezept angegebenen Daten der Patienten dürfen nur für die festgelegten Zwecke (in erster Linie für die Abrechnung mit der Krankenkasse) verwendet werden. Eine werbliche Verwendung der Daten sehen die hier einschlägigen Regelungen des Sozialgesetzbuches V (SGB V) dagegen nicht vor. Auch nach den allgemeinen Regelungen des BDSG dürfen Gesundheitsdaten nicht ohne Einwilligung des Betroffenen für Zwecke der Werbung verwendet werden, denn die für Gesundheitsdaten einschlägigen Bestimmungen (§ 28 Abs. 6 bis 9 BDSG) enthalten dafür keine Rechtsgrundlage.

16.6 Fehler bei Fax- und E-Mail-Versendungen

Bei der Versendung von Telefaxen und E-Mails kommt es leider immer wieder zu Fehlern, die in Einzelfällen für die betroffenen Personen teils gravierende Folgen haben können.

Im Berichtszeitraum wurden mehrere Fälle an uns herangetragen, in denen es bei der Versendung von Nachrichten mit sensiblem Inhalt per Fax oder E-Mail zu Fehlern gekommen ist. In einem besonders gravierenden Fall landete ein mehrseitiger psychosomatischer Befundbericht am zentralen Faxeingang des Arbeitgebers und konnte dort von mehreren Kollegen der Betroffenen zur Kenntnis genommen werden. In weiteren Fällen erreichten E-Mails wegen eines Tippfehlers jeweils den falschen Empfänger. Eine Patientin trug hierbei bspw. vor, dass ihr Arzt eine Terminabsage an die allgemeine E-Mail-Adresse des Vereins gesandt hat, für den sie hin und wieder tätig ist.

All diese Vorfälle waren zwar auf individuelle Fehler zurückzuführen. Trotzdem möchten wir allgemein darauf hinweisen, dass bei Fax- und E-Mail-Versendungen nicht nur überlegt werden muss, ob dieser Transportweg ausreichend sicher und für sensible Informationen überhaupt geeignet ist, sondern dass immer besondere Vorsicht bei der Adressierung geboten ist. Gerade beim Faxversand ist insbesondere zu berücksichtigen, dass das Fax „offen" beim Empfänger ankommt. Soll nur der Empfänger persönlich den Inhalt der Nachricht zur Kenntnis nehmen und ist – aus welchen Gründen auch immer – keine andere Versendungsform möglich, muss der Faxversand vorher mit dem Empfänger abgesprochen werden, so dass er die Nachricht persönlich entgegennehmen kann, sofern er nicht über ein nur ihm zugeordnetes Faxgerät verfügt.

Auch wenn bekannt ist, dass sowohl bei Eingabe der Faxnummer (als auch beim Eintippen der E-Mail-Adresse) besondere Sorgfalt geboten ist, kommt es hier immer wieder zu Fehlern. Dagegen hilft nur eine gewissenhafte Kontrolle.

In dem Fall, in dem der Arzt eine Terminabsage an die allgemeine E-Mail-Adresse des Vereins gesandt hatte, lagen uns zur Herkunft dieser E-Mail-Adresse gegensätzliche Aussagen vor. Die Betroffene hat glaubhaft versichert, dass sie selbst diese E-Mail-Adresse nicht angegeben habe; sie habe persönliche E-Mail-Adressen, die sie bei solchen privaten Angelegenheiten angegeben hätte. Der Arzt hingegen versicherte, dass es keine andere Möglichkeit gebe, als dass die Betroffene selbst diese E-Mail-Adresse in seiner Praxis hinterlassen hat. Nachdem wir uns auf Grund unserer Recherche durchaus andere Möglichkeiten zur Herkunft der E-Mail-Adresse vorstellen konnten und daher Zweifel an der Aussage des Arztes hatten, haben wir ihn darauf hingewiesen, dass nur die vom Patienten selbst angegebenen Kontaktmöglichkeiten genutzt werden dürfen. Bei einer Kontaktaufnahme über andere (z. B. selbst recherchierte) E-Mail-Adressen besteht die Gefahr, dass diese nicht mehr aktuell sind oder Dritte von der Nachricht und der Tatsache, dass sich die angesprochene Person in ärztlicher Behandlung befindet, Kenntnis erlangen. Bei einer allgemeinen E-Mail-Adresse (wie z. B. info@...) muss in jedem Fall damit gerechnet werden, dass auf den dazugehörigen Posteingang auch andere Personen Zugriff haben.

16.7 Outsourcing im Krankenhausumfeld

Die beiden bayerischen Datenschutzaufsichtsbehörden haben einen gemeinsamen Leitfaden zur datenschutzkonformen Auslagerung von Aufgaben in bayerischen Krankenhäusern herausgegeben.

Im bayerischen Krankenhausgesetz findet sich in Art. 27 Abs. 4 eine Regelung zur Auslagerung von Datenverarbeitungen in Krankenhäusern, die, wie sich nach einer Prüfung des Bayerischen Landesbeauftragten für den Datenschutz und zahlreichen Anfragen von Dienstleistern und Krankenhäusern bei uns ergeben hatte, durchaus unterschiedlich interpretiert wurde.

Daraufhin haben wir mit unserer bayerischen „Schwesterbehörde" unser gemeinsames Verständnis der Regelung in einem Leitfaden, der auf unserer Homepage veröffentlicht ist, niedergelegt.

Link:
www.lda.bayern.de/media/info_kh_leitfaden.pdf

Nach unserem Verständnis von Art. 27 BayKrG dürfen Patientendaten, die nicht zur verwaltungsmäßigen Abwicklung der Behandlung der Patienten erforderlich sind (medizinische Patientendaten/Behandlungsdaten), nur im Wege der Auftragsdatenverarbeitung (z. B. zur Aktenvernichtung, Scannen oder Archivierung) an einen Dienstleister weitergegeben werden, wenn es sich bei dem Dienstleister um ein nach Art. 2 BayKrG i.V.m. KHG förderfähiges Krankenhaus handelt oder ein derartiges Krankenhaus weiterhin Gewahrsam an den Daten behält. Dazu genügt es nicht, wenn an eine Gesellschaft ausgelagert wird, die zu einem Krankenhauskonzern gehört oder, die zu über 50% von einem Krankenhaus bestimmt wird. Einige nicht abschließende Beispiele, wie der Gewahrsam eines Krankenhauses sichergestellt werden kann, sind in dem Leitfaden dargestellt.

Ausblick zur DS-GVO:
Nach unserem derzeitigen Kenntnisstand ist bisher keine Änderung des BayKrG im Rahmen der Umsetzungs- und Anpassungsgesetze zur DS-GVO geplant. Europarechtlich ist es vorstellbar, dass die Regelung auf die Öffnungsklausel des Art. 9 Abs. 4 gestützt werden kann und die Rechtslage in Bayern damit so bleibt, wie sie derzeit ist.

16.8 Datenübermittlung von Beratungsstellen und Suchtkliniken an Strafgerichte bei Auflagen

Gerichte bzw. Bewährungshelfer möchten im Zuge der Überwachung von Straftäter öfter Auskünfte von den Beratungsstellen über die Wahrnehmung von Terminen haben oder in Einzelfällen sogar Auskunft darüber, ob der Klient bei der Therapie mitwirkt. Eine entsprechende Übermittlung von Daten kann datenschutzrechtlich zulässig sein.

Es kommt des Öfteren vor, dass Straftätern aufgegeben wird, Beratungsstellen oder Suchtkliniken im Rahmen von gerichtlich angeordneten Bewährungsauflagen nach §§ 56b, 65c StGB oder aufgrund von Auflagen/Weisungen nach § 153a StPO aufzusuchen. Dazu stellen die Gerichte regelmäßig Schweigepflichtentbindungserklärungen zur Verfügung.

Wir wurden von einer verantwortlichen Stelle gefragt, ob auf Grundlage dieser Erklärungen eine Datenübermittlung stattfinden kann. Die verantwortliche Stelle hatte daran Zweifel. Nachdem die gerichtlichen Anordnungen nach den §§ 153a StPO oder 56b, 56c, 59a StGB nur getroffen werden, wenn sie im Hinblick auf die Schwere der Tat oder zur Verhinderung weiterer Straftaten erforderlich sind, wird man als rein datenschutzrechtliche Rechtsgrundlage für die Datenübermittlung nach dem BDSG auch § 28 Abs. 2 Nr. 2b und Abs. 8 heranziehen können. Es ist in diesen Fällen anzunehmen, dass die Überprüfung der Einhaltung der Auflagen sowie die damit einhergehende Datenübermittlung privater Stellen an das Gericht zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit erforderlich ist. Könnte keine Überprüfung stattfinden, würde das Funktionieren des Rechts- und Strafsystems in Frage gestellt.

16.9 Verdeckte Weiterleitung an anderen Diensteanbieter zur Online-Terminvergabe

Die Weiterleitung von Online-Formular-Daten an einen anderen Diensteanbieter muss dem Nutzer deutlich angezeigt werden.

Im Berichtszeitraum sind uns mehrere Internetseiten von Ärzten aufgefallen, die ihren Patienten eine Online-Terminvereinbarung anbieten. Bei diesen Angeboten handelte es sich aber tatsächlich oft um den Dienst eines anderen Unternehmens. Die Online-Terminvereinbarung war zum Teil als Frame in den Internetauftritt des Arztes eingebunden. Für den Nutzer war nicht erkennbar, dass er seine Daten – darunter auch besondere Arten personenbezogener Daten i. S. d. § 3 Abs. 9 BDSG in der Form von Gesundheitsdaten, wie z. B. der Besuchsgrund – gegenüber einer anderen verantwortlichen Stelle angibt. Insbesondere ist in den von uns untersuchten Fällen die angezeigte URL meist gleichgeblieben, so dass in der Adresszeile des Internetbrowsers dem Nutzer noch die Webseite des Arztes genannt wurde. Der Nutzer konnte dann weder an der Gestaltung der Seite noch an deren Inhalt erkennen, dass er sich eigentlich auf der Internetseite eines anderen Diensteanbieters befindet. Lediglich den Allgemeinen Geschäftsbedingungen und den Datenschutzhinweisen (die erst auf der letzten Seite der Terminvereinbarung abgerufen werden konnten) ließ sich dies entnehmen.

Wir haben von den in unserem Zuständigkeitsbereich ansässigen Ärzten gefordert, die Weiterleitung kenntlich zu machen – wie § 13 Abs. 5 TMG dies auch vorsieht.

16.10 Zugriff auf die Daten eines verstorbenen Arztes

An die Witwe eines verstorbenen Arztes haben sich einige Patienten mit Auskunftsanfragen gewandt. Nachdem sie selbst mit dem Patientenverwaltungsprogramm nicht vertraut war, fragte sie uns um Rat, ob sie einen Dienstleister zur Unterstützung beauftragen könne.

Die Witwe eines verstorbenen Arztes stand vor dem Problem, dass mehrere Patienten Auskunft verlangt haben, sie jedoch mit dem Praxisverwaltungssystem nicht vertraut war und sich deshalb nicht in der Lage sah, dem nachzukommen. Sie wollte deshalb einen Dienstleister damit beauftragen und fragte uns um Rat, welche datenschutzrechtlichen Maßstäbe hierfür gelten.

Aufgrund der Tatsache, dass sich die Praxiscomputer im Besitz der Witwe befinden (Erbenstellung), ist diese datenschutzrechtlich als verantwortliche Stelle i. S. d. § 3 Abs. 7 BDSG anzusehen. Das bedeutet, sie muss beim Umgang mit den gespeicherten Patientendaten die datenschutzrechtlichen Bestimmungen beachten. Hinzu kommt, dass sie gemäß § 203 Abs. 3 Satz 3 Strafgesetzbuch (StGB) zur Wahrung der ärztlichen Schweigepflicht verpflichtet ist. Die Beauftragung eines Dienstleisters für die Aktivierung der Praxiscomputer, die Einsichtnahme in die gespeicherten Daten und die Selektion derjenigen Daten/Dateien, die an die Betroffenen herausgegebenen werden sollen, kann in der Form einer Datenverarbeitung im Auftrag (§ 11 BDSG) erfolgen. Dabei bleibt die Witwe für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich (§ 11 Abs. 1 Satz 1 BDSG), während der Auftragnehmer mit den Daten nur weisungsgemäß umgehen darf. Hinzu kommt aber, dass mit der Beauftragung eines Dienstleisters eine Offenbarung von Patientendaten gegenüber diesem Dienstleister verbunden ist und sich deshalb Probleme wegen Geheimnisverrat nach § 203 StGB ergeben könnten.

Nachdem es nur um wenige Personen ging, deren Daten gezielt gesucht werden sollten, bestand die Möglichkeit, dass diese darüber informiert werden, dass ein Ausdruck der gespeicherten Patientendaten nur mit Hilfe eines Dienstleisters möglich sei und für die damit verbundene Offenbarung ihrer Daten gegenüber diesem Dienstleister eine Schweigepflichtentbindungserklärung eingeholt werden müsse. Da es um sehr sensible Daten geht, haben wir der Witwe empfohlen, die Arbeiten des Dienstleisters persönlich zu überwachen (um z. B. sicherzustellen, dass dieser nicht für sich selbst Kopien der Daten anfertigt oder Daten anderer Patienten einsieht). Als weitere Möglichkeit haben wir es angesehen, dass ehemalige Praxisangestellte bei der Auskunftserteilung behilflich sind. Als berufsmäßige Gehilfen i.S.d. § 203 StGB würde ihnen gegenüber keine unbefugte Offenbarung erfolgen, so dass sie datenschutz- und strafrechtlich zulässig die Auskünfte erteilen könnten.

16.11 Einsicht in Schülerunterlagen

Der Gesetzgeber hat zum Jahreswechsel 2015/16 die Einsicht in Schülerunterlagen mit der Schülerunterlagenverordnung (SchUntV) neu geregelt.

Nach § 6 SchUntV stehen nun

- Schülerinnen und Schülern ab Vollendung des 14. Lebensjahres,
- Erziehungsberechtigten
- früheren Erziehungsberechtigten bei Schülerinnen und Schülern ab Vollendung des 18. Lebensjahres bis zur Vollendung des 21. Lebensjahres, soweit Vorschriften des BayEUG oder der Schulordnungen ihre Unterrichtung vorschreiben, und

- ehemaligen Schülerinnen und Schülern

Einsicht in die nach § 2 Nr. 1 SchUntV geführten Schülerunterlagen zu.

Daneben bestehen auch die allgemeinen datenschutzrechtlichen Ansprüche auf Auskunft, etwa nach § 34 BDSG. Die SchUntV gilt auch für Ersatzschulen mit dem Charakter einer öffentlichen Schule sowie für staatlich anerkannte Ersatzschulen, soweit diese als Beliehene tätig werden.

Das Bayerische Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst empfiehlt in seinen Durchführungshinweisen insgesamt allen Schulen die Anwendung der SchUntV und der zugehörigen Hinweise. Dieser Empfehlung schließen wir uns an.

16.12 Ausschreibung von Schülerbeförderungsleistungen für ein Förderzentrum

Bei Ausschreibungen muss stets geprüft werden, inwieweit die Aufnahme personenbezogener Daten in den Ausschreibungstext tatsächlich erforderlich ist, damit Bewerber Angebote abgeben können.

Ein Beschwerdeführer monierte, dass eine gemeinnützige GmbH Leistungen der Schülerbeförderung für ein Förderzentrum mit Förderschwerpunkt „geistige Entwicklung" auf ihrer Webseite ausgeschrieben hatte und der Ausschreibungstext auch Angaben über die gesundheitliche Situation einzelner Schüler – zwar ohne Nennung der Schülernamen, jedoch unter Nennung der Wohnadressen – enthielt. Die gGmbH war Betreiberin des Förderzentrums und erbrachte in dieser Eigenschaft Leistungen der Rehabilitation und Teilhabe behinderter Menschen nach dem Sozialgesetzbuch IV. Im Rahmen der Ausschreibung forderte sie Beförderungsunternehmen auf, Angebote zur Beförderung der Schüler des Förderzentrums abzugeben. Der Ausschreibungstext enthielt eine „Haltestellen- und Fahrgastübersicht", im Rahmen derer die von dem Beförderungsunternehmen anzufahrenden Adressen aufgelistet waren. Bei einigen der Adressen waren Geburtsdaten angegeben – vermutlich der jeweiligen Schüler – sowie in einigen Fällen Abkürzungen wie etwa „Aut" oder „A"; die Bedeutung der Kürzel wurde im Ausschreibungstext erläutert; danach stand etwa „Aut" für Autismus, „A" für Aggression/Anfälle.

Wir haben diese Art und Weise der Ausschreibung bemängelt. Die in der Liste enthaltenen Adressdaten stellen personenbezogene Daten dar. Nicht ausgeschlossen ist, dass bestimmte Außenstehende ausgehend von den Adressangaben in der Lage sind, (ggf. mit Zusatzkenntnissen) die betreffenden Schüler zu identifizieren. Die verwendeten Abkürzungen waren als Angaben zur Gesundheit im Sinne von § 3 Abs. 9 BDSG einzuordnen, da sie das Krankheitsbild und/oder das krankheitsbedingte Verhalten des jeweiligen Schülers näher beschrieben. Somit waren die darin enthaltenen Angaben zu Krankheitsbildern und (krankheitsbedingtem) Verhalten von Schülern aufgrund ihrer erheblichen Sensibilität in besonderem Maße schutzwürdig. Die Aufnahme dieser Merkmale in den Ausschreibungstext sollte die an der Ausschreibung teilnehmenden Beförderungsunternehmen in die Lage versetzen, sich auf die entsprechenden Situationen einzustellen und diese Umstände bei der Kalkulation und Unterbreitung ihres Angebots berücksichtigen zu können.

Nach unserer Bewertung ist es nicht akzeptabel, derart sensible Daten – wie geschehen – in einem für jedermann abrufbaren Ausschreibungstext im Internet zu veröffentlichen. Eine solche Veröffentlichung personenbezogener Daten der Schüler ist für die Ermöglichung der Abgabe von Angeboten durch Beförderungsunternehmen aus unserer Sicht schon nicht

erforderlich, da durchaus auch Vorgehensweisen vorstellbar sind, bei der die Ausschreibungsunterlagen nur an die interessierten Beförderungsunternehmen zugeschickt werden.

Es muss daher eine Vorgehensweise gefunden werden, die ohne eine Veröffentlichung dieser Informationen im „offenen" Internet auskommt.

Die ausschreibende gGmbH hatte uns mitgeteilt, dass sie die Ausschreibung in der von uns vorgefundenen Art und Weise, d. h. mit Aufnahme der genannten Daten zur Gesundheit und zum Verhalten von Schülern sowie der Schüleradressen, so mit dem Bezirk – dem Träger der Leistungen nach dem SGB IX – abgesprochen habe. Zudem habe sie die Ausschreibung der Schülerbeförderung „auf ausdrücklichen Wunsch der Regierung" – d. h. der für Schülerbeförderung zuständigen Behörde – vorgenommen. Da es sich bei dem Bezirk sowie bei der Regierung um öffentliche Stellen handelt, die nicht unserer datenschutzrechtlichen Aufsicht unterliegen, haben wir den für die Datenschutzaufsicht über öffentliche Stellen in Bayern zuständigen Bayerischen Landesbeauftragten für Datenschutz (BayLfD) auf die Angelegenheit aufmerksam gemacht und angeregt, zu prüfen, ob Bezirk und Regierung Vorgaben für Ausschreibungstext gemacht haben und wenn ja, wie diese Vorgaben datenschutzrechtlich zu beurteilen sei.

Wir hatten die Veröffentlichung der Ausschreibung mit Angaben zur Gesundheit und zum Verhalten von Schülern sowie der Schüleradressen im offenen Internet als nicht erforderlich und damit datenschutzrechtlich unzulässig angesehen. Die gGmbH hat sehr kurzfristig auf unsere Intervention reagiert und die Ausschreibungstexte von ihrer Homepage entfernt.

16.13 Elternbefragung im Kindergarten

Bei schriftlichen Elternbefragungen muss deutlich kommuniziert werden, wer die Fragebogen auswertet und zur Kenntnis nimmt.

Kindertageseinrichtungen müssen, um die Fördervoraussetzungen nach dem Bayerischen Kinderbildungs- und -betreuungsgesetz (BayKiBiG) zu erfüllen, jährlich eine Elternbefragung oder eine sonstige, gleichermaßen geeignete Maßnahme der Qualitätssicherung durchführen (Art. 19 Nr. 2 BayKiBiG). In einem Kindergarten ist wegen der Auswertung der Fragebogen ein Streit entbrannt. Ein Vater monierte gegenüber der Einrichtung, dass die Anonymität der betroffenen Kinder nicht gewährleistet gewesen sei, weil die ausgefüllten Fragebogen der Einrichtungsleitung zugänglich waren und diese – obwohl keine Namen genannt wurden – den Fragebogen ohne weiteres dem entsprechenden Kind zuordnen konnte.

Aus datenschutzrechtlicher Sicht ist zunächst festzustellen, dass es in Bezug auf den Umfang der Fragen sowie die Auswertung schriftlicher Elternbefragungen keine besonderen Vorgaben gibt. Insbesondere wird nicht gefordert, dass Elternbefragungen anonym durchzuführen sind. Deshalb kann der Kindergarten bzw. Einrichtungsträger sowohl den Inhalt und den Umfang des Fragebogens als auch das Procedere der Auswertung und die Verwertung der Ergebnisse selbst bestimmen.

Entscheidend dabei ist es jedoch für uns, dass gegenüber den Eltern deutlich kommuniziert wird, was mit den ausgefüllten Fragebogen geschieht (insbesondere, wer die Auswertung durchführt und die einzelnen Fragebogen zur Kenntnis nehmen kann). Wenn den Eltern beim Ausfüllen des Fragebogens bewusst ist, wer die Fragebogen einsieht (Elternbeirat, Kindergartenleitung, Team, Träger, etc.) und sie ihre

Antworten so formulieren können, wie sie dies gegenüber diesen Personen/Stellen tun möchten, ist der dortige Umgang mit den Daten auch dann unproblematisch, wenn bestimmt werden kann, wer den Fragebogen ausgefüllt hat und um welches Kind es geht.

In dem von uns geprüften Fall waren die Informationen, die die Eltern zu der Elternbefragung erhalten haben, missverständlich. Einerseits wurde der Eindruck erweckt, es handele sich um eine anonyme Befragung, weshalb die Erwartungshaltung des betroffenen Vaters, dass ein Rückschluss auf das einzelne Kind nicht möglich ist, nachvollziehbar ist. Anderseits wird aber auch beschrieben, dass die Fragebogen an den Kindergarten zurückgehen sollen und der Kindergarten seine Abläufe reflektieren wird. Um solche Missverständnisse zu vermeiden, haben wir gefordert, dass in Zukunft deutlich darüber informiert wird, wer die ausgefüllten Fragebogen auswertet und zur Kenntnis nimmt.

16.14 Verstoß gegen Direkterhebungsgrundsatz

Personenbezogene Daten sind grundsätzlich beim Betroffenen zu erheben und nicht ohne seine Mitwirkung anderweitig abzufragen.

Eine Interessentin für einen Weiterbildungskurs konnte bei der Anmeldung noch nicht den Nachweis erbringen, dass sie die für die Weiterbildung notwendige Grundausbildung erfolgreich abgeschlossen hat. Trotz mehrfacher Nachfragen legte sie dem Weiterbildungsträger diesen Nachweis nicht vor. Dieser hatte dann, als er darüber entscheiden musste, ob die Interessentin an dem Kurs teilnehmen kann oder nicht, beim vorherigen Bildungsträger nachgefragt und mitgeteilt bekommen, dass die Betroffene die Ausbildung nicht erfolgreich abgeschlossen habe.

Wir sind bei unserer Überprüfung zu dem Ergebnis gekommen, dass der Weiterbildungsträger zwar aufgrund der Tatsache, dass sich die Betroffene für den Weiterbildungskurs angemeldet hat, die Information erheben durften, ob sie die Zulassungsvoraussetzungen für den Weiterbildungskurs tatsächlich, wie von ihr im Lebenslauf angegeben, erfüllt. Dies ist für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen Schuldverhältnisses mit dem Betroffenen erforderlich und die dazugehörende Datenerhebung nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG zulässig. Allerdings hätte er den erforderlichen Nachweis von der Betroffenen selbst anfordern müssen, denn personenbezogene Daten sind grundsätzlich beim Betroffenen zu erheben (§ 4 Abs. 2 Satz 1 BDSG). Ohne seine Mitwirkung dürfen sie nur unter den Voraussetzungen des § 4 Abs. 2 Satz 2 BDSG erhoben werden. Diese Voraussetzungen für eine Datenerhebung bei Dritten sahen wir hier nicht als erfüllt an. Der Weiterbildungsträger hat seiner Stellungnahme zufolge die Betroffene zwar mehrfach aufgefordert, den Nachweis selbst zu erbringen. Nachdem sie dies nicht getan hat, hätte er aber entweder die Zusage für die Teilnahme widerrufen oder die Betroffene für die geplante Rückfrage beim Ausbildungsträger um Einwilligung bitten müssen. Die Betroffene hätte dann die Möglichkeit gehabt, über das weitere Vorgehen selbst zu entscheiden.

16.15 Asylbewerberhelferkreise

Ehrenamtliche Helfer für Asylbewerber möchten gerne durch Datenbanken mit Flüchtlingsinformationen ihre Arbeit erleichtern – dabei muss jedoch auch das Datenschutzrecht beachtet werden.

Wir wurden nach dem starken Zuwachs der Asylbewerber von Mitarbeitern aus ehrenamtlichen Helferkreisen, die sich bei der Unterbringung und Betreuung von Asylbewerbern engagieren, öfter kontaktiert. Viele Helferkreise

wünschen sich für ihre Betreuung den Aufbau einer eigenen Datenbank. Die Inhalte der gewünschten Listen oder Datenbanken, sowie den konkreten Informationsaustausch stellen sich die Helferkreise unterschiedlich vor.

Der Bayerische Landesbeauftragte für den Datenschutz hat dazu zutreffend die Auffassung vertreten, dass öffentliche Stellen ohne wirksame Einwilligung der Betroffenen keine konkreten Informationen über Asylbewerber an diese Vereinigungen weitergeben dürfen. Über die Frage, ob und wie Helferkreise Daten erheben, verarbeiten und nutzen dürfen, sei unter Heranziehung der Vorschriften für den nichtöffentlichen Bereich – und damit durch uns – zu entscheiden.

Bei der rechtlichen Beurteilung war zu berücksichtigen, dass die Arbeit der ehrenamtlichen Helfer wichtig ist und nicht unnötig erschwert werden darf. Andererseits sind die Helferkreise durch lockere Strukturen gekennzeichnet, die Gefahrenpotential bergen, etwa, wenn sich Asylkritiker absichtlich unter die Helfer mischen, um Informationen für strafbare Handlungen zu gewinnen. Diesen Konflikt – einerseits die Arbeit nicht unnötig zu behindern und anderseits die Asylbewerber ausreichend zu schützen – haben wir versucht, mit praxisorientierten Empfehlungen zu lösen.

Wir haben auf die (bei Asylbewerbern nicht leicht zu verwirklichende) Möglichkeit der Einwilligung, die Anforderungen an die Datensicherheit und Notwendigkeit die Helfer nach § 5 BDSG auf das Datengeheimnis zu verpflichten, hingewiesen.

Die ehrenamtlichen Helfer legen Wert darauf, dass ihre Tätigkeit freiwillig ist und daraus im Zweifel keine Rechtsfolgen entstehen. Eine rechtliche Organisationsstruktur, die eine datenschutzrechtlich verantwortliche Stelle erkennen ließe, gab es deshalb nicht. Verantwortliche Stelle war deshalb im Ergebnis jeder Helfer selbst, der die datenschutzrechtlichen Vorgaben einhalten muss.

Wir konnten den anfragenden ehrenamtlichen Helfern deshalb nicht die klare datenschutzrechtliche Hilfestellung für ihre Arbeit geben, die sie sich gewünscht hatten, gehen aber davon aus, dass unsere Beratung dazu beigetragen hat, die schon vorhandene Sensibilität für die Belange des Datenschutzes im Umgang mit Asylbewerbern zu steigern.

17

Vereine und Verbände

17 Vereine und Verbände

17.1 Mitteilung der Kontaktdaten von Delegierten eines Landesparteitags

In politischen Parteien findet die Willensbildung maßgeblich im Wege der Einbringung von Anträgen statt, über die insbesondere im Rahmen von Parteitagen abgestimmt wird. Je nach den parteiintern getroffenen Regelungen kann es zulässig sein, Namen und Kontaktdaten von Parteitagsdelegierten an bestimmte parteiinterne Akteure herauszugeben, um die Einbringung von Parteitagsanträgen und auf diese Weise die effektive Teilnahmemöglichkeit an der Mitwirkung an der politischen Willensbildung zu gewährleisten.

Ein Mitglied einer Partei fragte uns, ob es datenschutzrechtlich zulässig sei, wenn der Landesverband der Partei ihm – einem einzelnen Mitglied – und/oder der örtlichen Gliederungseinheit der Partei die Namen und Kontaktdaten der Delegierten zu einem Landesparteitag mitteilt. „Eigentlich" wollte das Mitglied wissen, ob ihm selbst oder zumindest „seiner" Ortsgliederung ein Anspruch auf Herausgabe der Namen und Kontaktdaten gegen den Landesverband zusteht.

Wir haben dem Mitglied vorab mitgeteilt, dass wir als Datenschutzaufsichtsbehörde nur die Frage beantworten können, ob eine Herausgabe (durch den Landesverband) datenschutzrechtlich zulässig wäre. Die Frage, ob er einen Herausgabeanspruch habe, sei nach den Regeln des Zivilrechts zu entscheiden und könne daher nicht Gegenstand einer datenschutzrechtlichen Prüfung sein.

Das anfragende Mitglied wollte mit dem Herausgabeverlangen erreichen, im Vorfeld des Parteitags Kontakt zu Delegierten aufnehmen zu können, um bei ihnen um Unterstützung für einen bestimmten Antrag zum Landesparteitag zu werben.

Die meisten politischen Parteien sind, so auch im vorliegenden Fall, als Vereine organisiert. Daher war aus unserer Sicht die einschlägige zivilgerichtliche Rechtsprechung zur Frage der Herausgabe von Mitgliederdaten durch Vereine an einzelne Vereinsmitglieder zu berücksichtigen. Maßgeblich sind insoweit vor allem die Grundsatzentscheidungen des Bundesgerichtshofs (BGH) vom 21. Juni 2010 und vom 25. Oktober 2010 (Az. jeweils II ZR 219/09), in denen der BGH ausführt, dass dem Mitglied eines Vereins ein Anspruch auf Offenbarung der Namen und Anschriften der Vereinsmitglieder dann zustehe, wenn das Mitglied ein berechtigtes Interesse an der Herausgabe habe, und der Herausgabe kein überwiegendes Interesse des Vereins oder der betroffenen Vereinsmitglieder entgegenstehe. Ein berechtigtes Herausgabeinteresse des Mitglieds kann laut BGH zum einen dann bestehen, wenn das Mitglied eine Mitgliederversammlung einberufen möchte, und der entsprechende Antrag nach den Festlegungen in der Vereinssatzung von einem bestimmten Quorum an Mitgliedern getragen werden muss. In diesem Fall habe das Mitglied ein berechtigtes Interesse an der Herausgabe der Namen und Adressen, um auf diesem Wege Kontakt zu anderen Mitgliedern aufnehmen zu können und so zu versuchen, das Quorum zu erfüllen. Neben dieser Fallgruppe erkennt der BGH einen Anspruch auf Herausgabe auch dann an, wenn das Vereinsmitglied aufgrund der konkreten Gegebenheiten auf die Kenntnis der Daten angewiesen ist, um das sich aus der Mitgliedschaft ergebende Recht auf Mitwirkung an der vereinsrechtlichen Willensbildung wirkungsvoll ausüben zu können.

Für den von uns geprüften Fall war vor diesem Hintergrund maßgeblich, ob ein einzelnes Parteimitglied und/oder die Ortsgliederung der Partei auf die Kenntnis von Namen und Anschriften der Delegierten zum Landesparteitag angewiesen ist, wenn das Mitglied bzw. die Ortsgliederung an der Willensbildung in der Partei mitwirken will und dazu ohne diese Kenntnis nicht hinreichend in der Lage wäre.

Daher galt es, die in der Satzung des Landesverbands und weiteren parteiinternen Regelwerken niedergelegten Regeln über die Mitwirkung der Mitglieder an der (politischen) Willensbildung im Landesverband der Partei zu betrachten. Diesen Regelungen war zu entnehmen, dass die Willensbildung auf Ebene des Landesverbandes maßgeblich durch Einbringung von Anträgen und Beschlussfassung über diese Anträge stattfindet. Als weitere Mittel zur Willensbildung in Parteien ist die Aufstellung von Kandidaten für politische Wahlen (z. B. Bundestags-, Landtagswahlen etc.) zu nennen; daneben sind auch weitere Instrumente zur Willensbildung (z. B. Mitgliederentscheide) denkbar. Es kam somit auf die Frage an, ob ein einzelnes Parteimitglied bzw. die Ortsgliederung der Partei ohne die Kenntnis von Namen und Anschriften der Delegierten zu einem Landesparteitag nicht in der Lage wäre, effektiv an der Willensbildung innerhalb der Partei mitwirken zu können. Da die Willensbildung auf Ebene des Landesverbands der betreffenden Partei jedenfalls maßgeblich durch Einbringung von Anträgen und die Beschlussfassung über die eingebrachten Anträge stattfindet, kam es somit darauf an, welchen Akteuren ein Antragsrecht für den Landesparteitag zusteht, sowie darauf, welche Stellen zur Beschlussfassung über eingebrachte Anträge zuständig sind.

Die Zuständigkeit zur Entscheidung über Anträge lag satzungsgemäß beim Landesparteitag. Ebenfalls satzungsgemäß kann nicht das einzelne Parteimitglied, sondern nur eine einzelne Ortsgliederung Anträge zum Landesparteitag einbringen.

Die Einbringung eines Antrags durch eine Ortsgliederung (sog. Initiativantrag) setzte allerdings nach der Satzung weiter voraus, dass der Antrag von einer bestimmten Anzahl an Delegierten des Landesparteitags – d. h. einem Quorum – unterstützt wird. Somit war festzuhalten, dass vorliegend eine Ortsgliederung antragsberechtigt zum Landesparteitag war, ein einzelnes Mitglied hingegen nicht – auch nicht etwa gemeinsam mit anderen beliebigen Mitgliedern oder Delegierten. Durch das Antragsrecht der Ortsgliederung zum Landesparteitag kann jedoch letztlich das einzelne Mitglied mittelbar an der parteiinternen Willensbildung mitwirken. Da die Ortsgliederung, um Anträge zum Landesparteitag stellen zu können, ein bestimmtes Quorum an Delegierten als Unterstützer gewinnen muss, besaß die Ortsgliederung nach unserer Auffassung ein berechtigtes Interesse, die Namen und Kontaktdaten der Delegierten zu erfahren, um durch Kontaktaufnahme mit diesen zu versuchen, das notwendige Quorum an Delegierten als Unterstützer zur Einbringung des Antrags zu erfüllen. Eine Herausgabe der Kontaktdaten der Delegierten an die Ortsgliederung wäre daher nach hiesiger Bewertung datenschutzrechtlich zulässig, wobei für eine Kontaktaufnahme die Herausgabe der Namen und postalischen Adressen der Delegierten ausreichend ist.

Einem einzelnen Parteimitglied steht hingegen – mangels eines eigenen Antragsrechts zum Landesparteitag – kein Herausgabeanspruch zu. Eine Herausgabe der Namen und Kontaktadressen an die Ortsgliederung wäre somit im vorliegenden Fall zulässig gewesen, eine Herausgabe an ein einzelnes Mitglied hingegen nicht.

17.2 Umgang mit Daten von Parteimitgliedern in den Parteiuntergliederungen

Nicht jeder Verstoß gegen parteiinterne Regularien zum Umgang mit Kontaktdaten von Mitgliedern stellt gleichzeitig einen datenschutzrechtlichen Verstoß dar.

Die Vorsitzende des Kreisverbands einer Partei beschwerte sich bei uns über den Umgang mit Mitgliederlisten des entsprechenden Kreisverbands durch den Bezirksverband, d. h. die dem Kreisverband örtlich übergeordnete Parteigliederung. Konkret ging es um die Zuleitung der aktualisierten Mitgliederliste sowie neuer Mitgliedsanträge durch den Bezirksverband an den Kreisverband. Nach Angaben der Kreisvorsitzenden hatte der Bezirksvorsitzende, dem diese Listen seitens der Landesmitgliederverwaltung zur Verfügung gestellt werden, die Listen in mindestens einem Fall nicht an sie, die Kreisvorsitzende, sondern an ein anderes, „einfaches" Mitglied des Kreisvorstands zugeleitet. Der Vorstand des Kreisverbandes hatte schon vorher einen Beschluss gefasst, wonach die vom Bezirksverband an den Kreisverband zuzuleitenden Mitgliederlisten allein an den/die Vorsitzende des Kreisverbands zuzuleiten seien, nicht jedoch an andere Personen. Über diesen Beschluss hatte der Kreisvorstand den Bezirksvorsitzenden informiert.

Wir haben in diesem Vorgang keinen Verstoß gegen gesetzliche Datenschutzregeln festzustellen vermocht. Festzuhalten war zunächst, dass die Frage, ob der Bezirksvorsitzende gegen parteiinterne Regelungen verstoßen hat, nicht durch uns als Datenschutzaufsichtsbehörde beurteilt werden kann, sondern allein durch die für die Durchsetzung parteiinterner Regelungen zuständigen Parteigremien. Diese Frage ist für die datenschutzrechtliche Bewertung des Vorgangs jedoch auch nicht maßgeblich; die datenschutzrechtliche Bewertung richtet sich vielmehr allein nach den gesetzlichen Vorschriften. Der Umstand, dass gemäß den parteiinternen Regelungen die Listen ausschließlich an den/die Kreisvorsitzenden hätten zugeleitet werden dürfen, bedeutet jedenfalls nicht zwingend auch eine unzulässige Übermittlung personenbezogener Daten oder einen sonstigen Verstoß gegen gesetzliche Datenschutzvorschriften.

Zunächst einmal kann schon in Frage gestellt werden, ob in der Zuleitung der Mitgliederlisten vom Bezirksverband an den Kreisverband eine „Übermittlung" personenbezogener Daten im Sinne von § 3 Abs. 4 S. 2 Nr. 3 BDSG liegt; dies wäre nur dann der Fall, wenn der Kreisverband gegenüber dem Bezirksverband als Dritter im Sinne des BDSG angesehen werden müsste, d. h. als eine vom Bezirksverband zu unterscheidende, eigenständige verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG. Selbst jedoch wenn man diese Frage bejaht, lag im vorliegenden Fall nach unserer Bewertung keine im Sinne von § 4 Abs. 1 BDSG „unzulässige" Übermittlung vor. Denn für die Frage, ob die Übermittlung zulässig oder unzulässig im Sinne von § 4 Abs. 1 BDSG ist, ist allein darauf abzustellen, ob die empfangende verantwortliche Stelle (nicht also die konkret datenempfangende Person) berechtigt ist, die Daten zu erhalten. Vorliegend wurden die Mitgliederlisten vom Bezirksverband an ein Mitglied des Kreisvorstands zugeleitet. Betrachtet man den Kreisverband als „verantwortliche Stelle" im Sinne von § 3 Abs. 7 BDSG, so liegt in der Zuleitung der Listen an das Mitglied des Kreisvorstands keine im Sinne von § 4 Abs. 1 BDSG unzulässige Übermittlung. Dies gilt jedenfalls, soweit die Listen dem Kreisvorstandsmitglied nicht für Zwecke zugeleitet wurden, die außerhalb seiner Funktion als Mitglied des Kreisvorstands liegen. Denn die Liste der Mitglieder des Kreisverbands durfte jedenfalls an den Kreisverband als „verantwortliche Stelle" und spezifisch an den Kreisvorstand als das für den Kreisverband handelnde Organ zugeleitet werden.

Die Frage, an welches Mitglied des Kreisvorstands genau die Daten gemäß parteiinternen Regelungen zuzuleiten sind, ist hingegen für die Bewertung der Übermittlung als „zulässig" oder „unzulässig" im Sinne von § 4 Abs. 1 BDSG nicht entscheidend, da die einzelnen Mitglieder des Kreisvorstandes ein und derselben „verantwortlichen Stelle" im Sinne von § 3 Abs. 7 BDSG (nämlich dem Kreisverband) angehören.

17.3 Veröffentlichung von Geburtstagen in bundesweiter Vereinszeitschrift

Vereine dürfen Geburtstage von Vereinsmitgliedern in Vereinszeitschriften oder ähnlichen Medien nur veröffentlichen, wenn sie die Betroffenen auf die Veröffentlichung hingewiesen und ihnen ein Widerspruchsrecht eingeräumt haben.

Ein bundesweit aktiver Verein landsmannschaftlicher Ausrichtung veröffentlichte in seiner Vereinszeitschrift routinemäßig Geburtstagsglückwünsche zu „runden" Geburtstagen von Vereinsmitgliedern; dabei wurden jeweils der Geburtstag und der aktuelle Wohnort des Mitglieds angegeben. Eine Frau, die Mitglied in dem Verein war, beschwerte sich bei uns über diese Praxis, da sie über die Veröffentlichung ihres Geburtstags nicht vorab informiert worden war und sie hierzu erst recht keine Einwilligung erteilt hatte.

Die Veröffentlichung von Geburtstagen von Vereinsmitgliedern in Vereinspublikationen ist in vielen Fällen üblich und nicht schlechterdings unzulässig. Nach unserer Auffassung gilt dies grundsätzlich auch bei einem bundesweit tätigen Verein wie im vorliegenden Fall. Der Umstand, dass sich vor der Eingabeführerin wohl noch nie ein Mitglied des Vereins über die – offensichtlich schon seit Jahren etablierte – Veröffentlichung in der Vereinszeitschrift beschwert hatte, mag für den konkret in Rede stehenden Verein als Beleg dienen, dass die Mitglieder hier zumindest typischerweise keine Einwände gegen diese Praxis haben und diese als üblich ansehen. Allerdings darf eben nicht pauschal bzw. für jeden Einzelfall davon ausgegangen werden, dass das betroffene Mitglied keine Einwände gegen eine Veröffentlichung hat. Daher sollte der Verein die Vereinsmitglieder – idealerweise bereits bei Eintritt in den Verein – ausdrücklich darauf hinweisen, dass eine solche Veröffentlichung üblicherweise stattfindet, sofern das Mitglied dem nicht widerspricht. Bei Mitgliedern, die trotz ausdrücklicher Information keinen Widerspruch einlegen, kann davon ausgegangen werden, dass sie keine überwiegenden schutzwürdigen Interessen im Sinne von § 28 Abs. 1 S. 1 Nr. 2 BDSG am Unterbleiben der Veröffentlichung haben, so dass die Veröffentlichung in diesen Fällen zulässig ist.

In dem von uns bearbeiteten Fall hatte der Verein seine Mitglieder nicht auf die geplante Veröffentlichung hingewiesen und sie – insoweit konsequent – auch nicht darauf hingewiesen, dass sie der Veröffentlichung widersprechen können. Nach unserer Intervention stellte der Verein seine Praxis jedoch um und bat neu eintretende Mitglieder im Formular fortan ausdrücklich um Erteilung einer Einwilligung in die Veröffentlichung. Was Bestandsmitglieder betrifft, erschien eine gesonderte umfassende Information des gesamten Bestands nach plausibler Darstellung des Vereins nicht realisierbar; wir teilten dem Verein mit, dass wir es hinsichtlich der Bestandsmitglieder als vertretbar ansehen, wenn die Betroffenen bei gegebener Gelegenheit (etwa im Zuge der Versendung von Informationsmaterial oder regulärer Korrespondenz) über die Widerspruchsmöglichkeit informiert werden.

18

Wohnungswirtschaft und Mieterdatenschutz

18 Wohnungswirtschaft und Mieterdatenschutz

18.1 Umfang an auszutauschenden Kontaktdaten in der Wohnungseigentümergemeinschaft

Die Wohnungseigentümergemeinschaft ist keine anonyme Gemeinschaft – die einzelnen Eigentümer haben einen Anspruch auf Kenntnis der Identität der anderen mit ihnen in der Eigentümergemeinschaft verbundenen Eigentümer. Die Bekanntgabe der E-Mail-Adresse oder Telefonnummer an die anderen Eigentümer ist indessen nicht zwingend und kann auch nicht per Beschluss der Eigentümergemeinschaft „angeordnet" werden.

Ein Wohnungseigentümer beschwerte sich bei uns darüber, dass der Verwalter einer Wohnungseigentümergemeinschaft es sich zur Gewohnheit gemacht hatte, mit den Eigentümern per E-Mail zu kommunizieren. Dabei verschickte er bisweilen E-Mails an alle Eigentümer und setzte dabei alle Empfängeradressen in das „CC-Feld" der E-Mail, so dass jedem Eigentümer die E-Mail-Adressen der übrigen Eigentümer zur Kenntnis gebracht wurden. Einer der Wohnungseigentümer war mit dieser Praxis nicht einverstanden.

Daraufhin erläuterten wir dem Verwalter, dass ein einzelner Eigentümer es nicht hinnehmen muss, dass seine E-Mail-Adresse (oder auch seine Telefonnummer) allen anderen Eigentümern bekannt gemacht wird. Zwar betont die Rechtsprechung, dass die Eigentümergemeinschaft keine anonyme Gemeinschaft ist und der einzelne Eigentümer das Recht hat, die Identität der anderen Eigentümer – etwa zum Zwecke einer Kontaktaufnahme – zu kennen. Hierfür genügt nach unserer Auffassung jedoch die Kenntnis der Namen und postalischen Adressen. Die Kenntnis der Telefonnummer oder E-Mail-Adresse ist für eine Kontaktaufnahme nicht erforderlich. Wir teilten dem Verwalter daher mit, dass er, wenn einzelne Eigentümer mit einer solchen Kommunikation per „offenem E-Mail-Verteiler" nicht einverstanden sind, er dies in dem betreffenden Einzelfall respektieren müsse.

Kurze Zeit später teilte uns der Wohnungseigentümer mit, dass die Eigentümergemeinschaft nun einen Beschluss gefasst habe, wonach die Kommunikation zwischen dem Verwalter und den Eigentümern „mit offenem E-Mail-Verteiler" stattzufinden habe, so dass allen Eigentümern die E-Mail-Adressen aller anderen Eigentümer bekannt gegeben werden. Der Verwalter habe daher nunmehr auf dieser Basis seine Praxis fortgesetzt.

Wir nahmen daraufhin erneut Kontakt zum Verwalter auf und teilten ihm mit, dass ein Beschluss der Eigentümergemeinschaft sich nicht über das Recht des einzelnen Eigentümers auf informationelle Selbstbestimmung hinwegsetzen könne. Der einzelne Eigentümer hat trotz eines solchen Beschlusses weiterhin das Recht, vom Verwalter zu verlangen, seine E-Mail-Adresse nicht mehr in das CC-Feld zu setzen und sie damit nicht mehr an die anderen Eigentümern zu übermitteln. Dem Eingabeführer teilten wir jedoch auch mit, dass unsere Behörde nicht über die Wirksamkeit des Beschlusses der Eigentümergemeinschaft in zivilrechtlicher Hinsicht entscheiden könne; letzteres obliegt allein der ordentlichen Gerichtsbarkeit.

18.2 Bekanntgabe von Hausgeld-Zahlungsrückständen in der Wohnungseigentümergemeinschaft

Der Verwalter der Wohnungseigentümergemeinschaft darf die Wohnungseigentümer im Vorfeld der Eigentümerversammlung darüber informieren, inwieweit die einzelnen Eigentümer ihre Hausgeldzahlungen erfüllt haben.

In unserem 5. Tätigkeitsbericht für 2011/2012 haben wir uns unter Nr. 16.3 zu der Frage geäußert, ob der Verwalter einer Wohnungseigentümergemeinschaft im Vorfeld der Eigentümerversammlung den Eigentümern eine „Saldenliste" zuschicken darf, die den Stand der Hausgeldzahlungen der einzelnen Eigentümer und somit auch etwaige Rückstände dieser bei den Hausgeldzahlungen aufführt. Wir haben an o.g. Stelle die Auffassung geäußert, dass eine „proaktive" Zusendung einer solchen Übersicht durch den Verwalter – ohne ein entsprechendes Verlangen des einzelnen Eigentümers – nicht erforderlich und daher im Ergebnis als unzulässig zu bewerten sei, jedenfalls sofern nicht im Hausverwaltervertrag eine explizite Verpflichtung des Verwalters zur Zusendung der Saldenliste geregelt ist.

Nach weiteren zwischenzeitlich von uns bearbeiteten Eingaben und nochmaliger Überprüfung halten wir an dieser Auffassung nicht weiter fest. Vielmehr sprechen bei nochmaliger Betrachtung die besseren Argumente dafür, die Zusendung im Ergebnis als zulässig anzusehen. Maßgeblich hierfür ist letztlich, dass die Eigentümer gemäß § 28 Abs. 5 Wohnungseigentumsgesetz (WEG) über die „Abrechnung" zu beschließen haben, die der Verwalter gemäß § 28 Abs. 3 WEG nach Ablauf jedes Kalenderjahres aufstellen muss. Die Beschlussfassung findet gemäß § 23 Abs. 1 WEG grundsätzlich im Rahmen der Eigentümerversammlung statt. Gegenstand der Beschlussfassung ist, wie bereits erwähnt, die Abrechnung. Diese muss gemäß Rechtsprechung eine sog. Einzelabrechnung für den jeweiligen Eigentümer sowie die sog. Gesamtabrechnung beinhalten. Zur Gesamtabrechnung gehören nach der Rechtsprechung (BGH, Urt. vom 04.12.2010 – V ZR 44/09; BGH, Urt. v. 11.10.2013 – V ZR 271/12) alle vom Verwalter tatsächlich empfangenen Einnahmen und von ihm tatsächlich getätigten Ausgaben. Das bedeutet: Die Eigentümer beschließen in der Eigentümerversammlung unter anderem eben auch über den in der Abrechnung darzustellenden Stand der Erfüllung der Hausgeldzahlungspflichten aller einzelnen Eigentümer. Daher muss der Verwalter in der von ihm den Eigentümern zur Beschlussfassung vorzulegenden Jahresabrechnung den Stand der Hausgeldzahlungen der einzelnen Eigentümer ausweisen, da diese eben Gegenstand der Beschlussfassung sind; die reine Angabe einer „Gesamtsumme" der Hausgeldabrechnungen in der Jahresabrechnung würde gemäß der o.g. Rechtsprechung keine ordnungsgemäße Jahresabrechnung darstellen.

Streiten könnte man nun noch über den Zeitpunkt, in dem die Mitteilung des Standes der Hausgeldzahlungen durch den Verwalter an die Eigentümer zulässig ist, namentlich ob diese schon vor der Eigentümerversammlung oder aber erst in der Versammlung selbst erfolgen darf. Insoweit könnte man auf den ersten Blick die Meinung vertreten, dass es ausreicht, wenn der Verwalter die Jahresabrechnung und damit (u. a. auch) den in der Abrechnung darzustellenden Stand der Hausgeldzahlungen der einzelnen Eigentümer erst in der Eigentümerversammlung selbst vorlegt. Dies würde jedoch bedeuten, dass die Eigentümer letztlich ohne Vorbereitung, quasi aufgrund einer reinen „Tischvorlage" über diese Abrechnung entscheiden müssten. Die besseren Argumente sprechen bei dieser Sachlage dafür, den Eigentümern zur Vorbereitung der Beschlussfassung eine gewisse Zeit einzuräumen. Wenn es, wie oben dargestellt, notwendig –

und damit datenschutzrechtlich zulässig – ist, den Eigentümern zur Beschlussfassung in der Eigentümerversammlung den Stand der Hausgeldzahlungen der einzelnen Eigentümer in der Jahresabrechnung darzustellen, dann muss es auch zulässig sein, die Jahresabrechnung mit der entsprechenden Darstellung nicht erst in der Versammlung selbst vorzulegen, sondern bereits in einem zeitlich angemessen bemessenen Vorfeld der Versammlung durch Zusendung der Jahresabrechnung (etwa im Rahmen der Zusendung der Sitzungsunterlagen). Zumindest kann eine solche Zusendung nicht als datenschutzrechtlich unzulässig gewertet werden.

18.3 Mitteilung der Heizkosten in der Wohnungseigentümergemeinschaft

Der Verwalter einer Wohnungseigentumsgemeinschaft sollte davon absehen, von sich aus („proaktiv") eine Liste mit den Heizkosten der einzelnen Wohnungseigentümer an die Eigentümer zu übersenden.

Ein Wohnungseigentümer beschwerte sich bei uns darüber, dass der Verwalter der Eigentümergemeinschaft tabellarisch in Papierform die für das Jahr 2015 anfallenden Heizkosten aller einzelnen Wohnungseigentümer an alle Eigentümer zur Kenntnis zugesandt hatte. Der Beschwerdeführer war damit nicht einverstanden, da er nicht wollte, dass alle anderen Eigentümer davon Kenntnis erhalten, welchen Betrag an Heizkosten er zu bezahlen hatte.

Der von uns zur Stellungnahme aufgeforderte Verwalter war sich keines datenschutzrechtlichen Verstoßes bewusst. Er argumentierte – insoweit zutreffend – dass in der Rechtsprechung ein umfassendes Einsichtsrecht jedes Wohnungseigentümers in die Verwaltungsunterlagen der Eigentümergemeinschaft anerkannt sei, und dass dieses Einsichtsrecht explizit auch das Recht zur Einsicht in die Einzelabrechnungen der übrigen Wohnungseigentümer umfasse (LG Frankfurt/Main, Beschl. v. 20.06.2016 – 2-13 S 13/14; OLG München, Beschl. v. 09.03.2007 – 32 Wx 177/06). Die Rechtsprechung hat insoweit betont, dass das Datenschutzrecht einer Einsichtnahme nicht entgegensteht, da die Wohnungseigentümergemeinschaft eben keine anonyme Gemeinschaft sei.

Auch unter Berücksichtigung dieser Rechtsprechung sind wir jedoch der Auffassung, dass eine proaktive, routinemäßige Zusendung einer Liste mit den Heizkosten aller einzelnen Eigentümer durch den Verwalter an die Wohnungseigentümer – wie geschehen – datenschutzrechtlich zumindest fraglich erscheint. Denn nach der Rechtsprechung ist das dem einzelnen Eigentümer zustehende Einsichtsrecht grundsätzlich in den Geschäftsräumen des Verwalters auszuüben (OLG München – 32 Wx 177/07); ein Anspruch des einzelnen Wohnungseigentümers auf Zusendung von Kopien besteht nicht. Es ist somit auch nicht sicher, ob alle einzelnen Eigentümer ihr Einsichtsrecht überhaupt ausüben möchten. Es ist vor diesem Hintergrund aber zumindest zu empfehlen, von einer proaktiven Zusendung beliebiger Einzelbelege – etwa zu Heizkosten – durch den Verwalter an die Eigentümer abzusehen, auch wenn einzuräumen ist, dass es vor dem Hintergrund des von der Rechtsprechung anerkannten umfassenden Akteneinsichtsrechts schwierig erscheint, ein solches Vorgehen als „Datenschutzverstoß" zu bewerten. Eine solche Praxis erscheint allerdings jedenfalls dann gut vertretbar, wenn ein entsprechender Beschluss der Eigentümergemeinschaft dies vorsieht.

Darüber hinaus halten wir es für zulässig, wenn der Verwalter den Eigentümern im Vorfeld der Eigentümerversammlung mit der Jahresabrechnung den Stand der Hausgeldzahlungen der einzelnen Eigentümer darstellt; denn der Stand der Erfüllung der Hausgeldzahlungen

durch die einzelnen Eigentümer ist Gegenstand der Beschlussfassung der Eigentümerversammlung, so dass es zulässig sein muss, den Eigentümern zur Vorbereitung der Beschlussfassung jedenfalls die Übersicht über den Stand der Hausgeldzahlungen aller einzelnen Eigentümer zu übersenden (dazu vgl. Kapitel 18.2).

18.4 Weitergabe der Telefonnummer des Mieters durch Vermieter an Wohnungsinteressenten

Der Vermieter darf die Telefonnummer des Mieters an Wohnungsinteressenten – etwa zum Zwecke der Vereinbarung eines Besichtigungstermins – nur mit Einwilligung des Mieters weitergeben.

Mehrfach beschwerten sich im Berichtszeitraum Mieter, die ihren Wohnraummietvertrag gekündigt hatten, darüber, dass der Vermieter und/oder eine Hausverwaltung ihre Telefonnummer zur möglichen Vereinbarung eines Besichtigungstermins an Wohnungsinteressenten weitergegeben hatten, ohne dass die Mieter hiervon wussten.

Eine solche Weitergabe stellt eine Übermittlung personenbezogener Daten dar und ist nur mit Einwilligung des Mieters zulässig. Hierauf haben wir die Vermieter bzw. die Hausverwaltungen in den von uns geprüften Fällen hingewiesen. Diese waren sich in den geprüften Fällen offenbar dessen nicht immer bewusst.

19

Videoüberwachung

19 Videoüberwachung

19.1 Pkw-Überwachung in Tiefgarage

Die Videoüberwachung eines Pkw-Aufzugs in einer Tiefgarage ist in begründeten Fällen vertretbar.

Hinsichtlich der Überwachung eines Pkw-Aufzugs in einer Tiefgarage hatten wir eine Anfrage erhalten. Die Tiefgarage des betroffenen Mehrfamilienhauses erstreckt sich über mehrere Stockwerke, wobei die Besitzer von Stellplätzen in den oberen Etagen mit einem Pkw-Aufzug dorthin gelangen. Mehrfach stießen Fahrzeuge schon von innen und von außen an die Aufzugstüren und beschädigten diese, wobei die Reparaturkosten jeweils beträchtlich waren. Die Verursacher konnten in keinem der Fälle ermittelt werden. Die beiden Eigentümer beabsichtigten deshalb, eine Videoüberwachung des Pkw-Aufzugs durchzuführen und fragten bei uns nach, ob dies datenschutzrechtlich zulässig sei.

Da es sich um eine nicht-öffentlich zugängliche Tiefgarage handelte, richtet sich die Zulässigkeit der Überwachung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Danach ist diese zulässig, wenn sie zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Verarbeitung oder Nutzung überwiegt. Aufgrund der in der Vergangenheit entstandenen Schäden und der Tatsache, dass die Verursacher nicht festgestellt werden konnten, ist ein berechtigtes Interesse an einer Videoüberwachung zu bejahen. Zu berücksichtigen ist, dass die Fahrzeuge nur während der kurzen Zeit der Nutzung des Aufzuges überwacht werden, so dass der Eingriff in das Persönlichkeitsrecht der Fahrer – vergleichsweise – nicht so bedeutend ist, wenn eine Auswertung auch nur bei Vorfällen erfolgt (was durch eine Protokollierung der Zugriffe nachvollziehbar gemacht werden könnte), der Kreis der Zugriffsberechtigten klein gehalten wird und die Nutzer des Aufzugs in geeigneter Weise auf die Videoüberwachung hingewiesen werden. Werden diese Voraussetzungen erfüllt, halten wir die Videoüberwachung für den genannten Zweck für vertretbar.

19.2 Verdeckte Videoüberwachung wegen Betrugsverdacht

Die verdeckte Videoüberwachung eines Mitarbeiters in einem Getränkemarkt kann bei Vorliegen eines Betrugsverdachts zulässig sein.

Eine Beschwerde im Berichtszeitraum bezog sich auf eine verdeckte Videoüberwachung in einem Getränkemarkt. Dort fielen der Revision hohe Auszahlungsbeträge aufgrund manuell ausgestellter Leergut-Bons auf. Die Geschäftsleitung wies darauf hin, dass ein manuelles Ausstellen nur bei einem Defekt des Leergutautomaten üblich sei. Eine genauere Überprüfung habe aber ergeben, dass der Leergutautomat stets funktionsfähig gewesen sei. Aufgrund eines Abgleichs der Vorfälle mit den Personaleinsatzplänen sowie den Boni-Daten habe sich der konkrete und begründete Verdacht ergeben, dass der Marktleiter Leergut-Bons ohne Berechtigung ausgestellt und diese dann eingelöst und somit eine Straftat begangen habe.

Man sei im Betrieb zu dem Ergebnis gekommen, dass eine Aufklärung der Straftat nur im Rahmen einer verdeckten Videoüberwachung möglich sei. Eine personengestützte Überwachung des Getränkemarkts als milderes Mittel sei ausgeschieden, weil eine gleichzeitige Kontrolle aller Bereiche des Getränkemarktes kaum möglich sei. Aus diesem Grund seien sechs

versteckte Videokameras installiert worden, um über eine Woche den Kassenbereich, die Leergutautomaten und den Tresor zu überwachen und damit zur Aufdeckung der Straftat beizutragen.

Da die Videokameras wegen einer vermuteten Straftat im Rahmen eines Beschäftigungsverhältnisses versteckt eingesetzt wurden, war die Datenerhebung und -verarbeitung nach § 32 Abs. 1 Satz 2 BDSG zu beurteilen. Danach dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn vorab zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Aufgrund der Vorkommnisse musste davon ausgegangen werden, dass weiterhin Straftaten zu Lasten des Unternehmens erfolgen. Es gab einen konkreten, begründeten Verdacht gegen den Leiter des Getränkemarkts. Ein milderes Mittel zur Aufklärung der Angelegenheit war dabei nicht erkennbar.

Da die Videoüberwachung von vornherein auf eine Woche beschränkt war und darüber hinaus die Kameras ausschließlich auf die zur Aufklärung der Straftat relevanten Bereiche ausgerichtet waren, sehen wir auch das schutzwürdige Interesse der anderen Mitarbeiter nicht beeinträchtigt. In Art und Umfang war die durchgeführte Videoüberwachungsmaßnahme im Hinblick auf deren Anlass nicht unverhältnismäßig. Insgesamt gesehen hielten wir die verdeckte Videoüberwachung daher für vertretbar.

19.3 Videoüberwachung zum Schutz vor Müllablagerungen

Wegen gravierender und wiederholter wilder Müllablagerung kann eine Videoüberwachung zulässig sein.

Wir erhielten eine Anfrage einer Hausverwaltung einer Eigentumswohnanlage. Es sei des Öfteren zu wilden Müllablagerungen im Müllraum gekommen. Durch das Entsorgen dieser wüsten Müllablagerungen drohen der Wohnungseigentümergemeinschaft Kosten, die nicht auf den Verursacher abgewälzt werden können, da dieser unbekannt sei. Um die Verursacher ausfindig machen zu können, erwog man das Installieren einer Videokamera.

Als Rechtsgrundlage kommt § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Betracht. Danach ist das Erheben, Verarbeiten und Nutzen personenbezogener Daten für die Erfüllung eigener Geschäftszwecke zulässig, wenn es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegen. Ein berechtigtes Interesse bejahten wir bei der geschilderten Situation. Wir hielten den Eingriff in das Persönlichkeitsrecht für vertretbar, wenn folgende Maßgaben erfüllt werden:

- Die Videoüberwachung muss auf den Müllraum begrenzt werden.
- Am Zugang zum Müllraum ist auf die Videoüberwachung hinzuweisen (in der Regel durch ein Schild).
- Die Daten sind, wenn es keine Vorfälle gab, binnen zwei Arbeitstagen zu löschen (unzulässige Müllablagerungen sind in dieser Zeit festzustellen).
- Eine Auswertung der Aufnahmen darf nur zum Zwecke der Aufklärung von Müllablagerungen erfolgen, wobei sich

dafür eine Auswertung im Vier-Augen-Prinzip durch zwei Personen empfiehlt.

Weiter empfahlen wir die Erstellung eines Konzepts, in dem der Zweck der Videoüberwachung, die Zugriffsregelung und die Speicherdauer schriftlich niedergelegt werden sollten, damit Betroffene die Möglichkeit haben, sich über den Umfang der Datenverarbeitung zu informieren. Außerdem forderten wir die Hausverwaltung auf, nach einem gewissen Zeitablauf bzw. dann, wenn ein Verursacher ermittelt wurde, zu überprüfen, ob die Videoüberwachung weiterhin erforderlich ist.

19.4 Weitergabe von Videoaufnahmen zur Geltendmachung zivilrechtlicher Ansprüche

Die Weitergabe von Videoaufnahmen durch den Kamerabetreiber an einen Dritten, damit dieser zivilrechtliche Ansprüche geltend machen kann, ist unzulässig.

Der Fahrer eines Mietwagens verursachte beim Befahren einer öffentlich zugänglichen Tiefgarage eines Hotels einen Schaden sowohl an der Tiefgarage als auch am Mietwagen. Das Hotel machte daraufhin seinen Anspruch auf Ersatz des ihm entstandenen Schadens gegenüber der Mietwagenfirma geltend. Diese möchte nun ihrerseits ihren zivilrechtlichen Anspruch aus dem mit dem Fahrer bestehenden Vertrag gegen diesen als Verursacher geltend machen.

Die Firma fragte dazu bei uns nach, ob es möglich ist, dass das Hotel ihr die Aufnahmen einer in der Tiefgarage befindlichen Videokamera, auf der die Verursachung des Unfalls zu sehen ist, als Beweismittel zur Verfügung stellt. Die Herausgabe der Aufzeichnungen ist nicht zulässig. Nach § 6b Abs. 3 Satz 2 BDSG ist eine Übermittlung für einen anderen Zweck nur zulässig, wenn dies zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung oder zur Verfolgung von Straftaten erforderlich ist. Eine Weitergabe der Aufnahmen zur Verfolgung von zivilrechtlichen Ansprüchen kommt deshalb nicht in Betracht.

19.5 Videoüberwachung in Schwimmbädern

Der Einsatz von Videoüberwachungsmaßnahmen in Schwimmbädern muss genau geprüft werden, wie im Zusatz zur Orientierungshilfe „Videoüberwachung in Schwimmbädern“ dargestellt wird.

Immer wieder erreichen uns Anfragen und Beschwerden zu Videokameras in Schwimmbädern. Gerade in den großen Erlebnisbädern und Thermen werden meist Videokameras eingesetzt, um die Zugänge zu den Umkleidebereichen sowie dortige Spinde zu überwachen, Drehkreuze zu weiteren, kostenpflichtigen Bereichen gegen unerlaubten Zugang zu schützen oder aber auch Beckenbereiche, die nicht direkt durch den zentralen Bademeisteraufsichtsposten einsehbar sind, über Monitore überwachen und aufzeichnen zu können.

Begründet wird diese umfassende Videoüberwachung in der Regel damit, dass bei Unfällen Aufzeichnungen benötigt würden, die bei der Klärung des Hergangs und damit bei der Frage der Haftung helfen sollen, sowie um Diebstahl, Belästigungen oder Übergriffe durch Besucher aufklären zu können bzw. die Sicherheit und den Schutz der Besucher zu gewährleisten.

Auch wenn eine Videoüberwachung zur Wahrung des Hausrechts oder zur Wahrnehmung eines berechtigten Interesses erforderlich ist, darf sie nur in Betrieb genommen werden, wenn schutzwürdige Interessen der Betroffenen nicht überwiegen. Grundsätzlich unzulässig sind Beobachtungen, die die Intimsphäre der Menschen verletzen, etwa die Überwachung

von Toiletten, Saunas, Duschen oder Umkleidekabinen. Die schutzwürdigen Interessen überwiegen außerdem häufig dann, wenn die Entfaltung der Persönlichkeit im Vordergrund steht. Dies ist beispielsweise in Restaurants, Erlebnis- und Erholungsparks oder Erlebnisschwimmbädern der Fall, d. h. an Orten an denen Leute gerne kommunizieren, essen, trinken oder sich erholen.

Da die Videoüberwachung in Schwimmbädern bundesweit stark zunimmt, hat der Düsseldorfer Kreis bereits im August 2015 einen Zusatz zur Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen" betreffend die „Videoüberwachung in Schwimmbädern" verabschiedet. Darin wird auf die speziellen Fragen zur Überwachung in Schwimmbädern eingegangen. Es wird Folgendes ausgeführt:

> *„Zur Abwehr von dem mit dem Baden verbundenen Gefahren ist eine Videoaufzeichnung nicht erforderlich. Im Ausnahmefall kann eine reine Beobachtung („verlängertes Auge") zulässig sein, wenn sie der Unterstützung der Badeaufsicht an besonders gefährlichen oder unübersichtlichen Orten dient. Die Gefährlichkeit dieser Stellen muss sich aufgrund objektiver Anhaltspunkte ergeben, beispielsweise, weil es bereits konkrete Vorfälle gegeben hat oder Erfahrungswerte für eine erhöhte Gefährlichkeit (wie z. B. bei Sprungtürmen, Rutschen, Kinderbecken) sprechen. Nicht ausreichend ist die allgemein erhöhte Unfallgefahr wegen des Aufenthalts im Wasser. Der Einsatz von Videoüberwachungstechnik kann kein Ersatz für Aufsicht durch Personal sein!"*

Eine Videoaufzeichnung nur oder hauptsächlich zum Ausschluss eines etwaigen Haftungsrisikos ist somit grundsätzlich nicht zulässig; für die Wahrnehmung der Verkehrssicherungspflicht ist kein Nachweis durch Videoaufzeichnungen erforderlich – zudem ist grundsätzlich der Geschädigte in der Beweispflicht. Sofern bereits Spindaufbrüche nachgewiesener Weise vorkamen, kann eine Überwachung der Spinde zulässig sein, sofern nicht gleichzeitig Bänke, Ablageflächen oder Umkleidebereiche mit erfasst werden.

Weitere Ausführungen, inwieweit Videobeobachtung und -überwachung zulässig ist, sind in der Orientierungshilfe „Videoüberwachung in Schwimmbädern" zu finden

Links:
www.lda.bayern.de/media/oh_video_schwimmbad.pdf

19.6 Verfolgung unzulässiger Dashcam-Nutzung durch Aufsichtsbehörde

Die Verfolgung einer unzulässigen Dashcam-Nutzung ist nur angezeigt, wenn ausreichende Beweismittel zum Nachweis der unzulässigen Nutzung vorliegen.

Die Nutzung von Dashcams begegnet nach wie vor einer großen Rechtsunsicherheit. Die Frage, ob und wenn ja, unter welchen Voraussetzungen sie genutzt und für welche Zwecke die Aufnahmen verwendet werden dürfen, ist mittlerweile Gegenstand zahlreicher Verfahren bei Datenschutzaufsichtsbehörden und auch bei Gerichten.

Datenschutzrechtlich ist die Nutzung von Dashcams als Erhebung und Verarbeitung personenbezogener Daten zu bewerten, soweit die Aufnahmen im öffentlichen Straßenverkehr erfolgen. Zulässig sind die Aufnahmen dann, wenn entweder eine Einwilligung der von der Aufnahme betroffenen Personen vorliegt, was in der Praxis ausgeschlossen ist, oder es eine Rechtsgrundlage gibt, die dies erlaubt. Infrage kommt insoweit § 6b BDSG, wonach eine Videobeobachtung in öffentlich zugänglichen Bereichen insbesondere nur zulässig ist, soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist

und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. In aller Regel geben Personen, die bei Polizeikontrollen auf den Zweck der Nutzung ihrer Dashcams angesprochen werden, an, dass sie diese Aufnahmen im Falle eines Unfalls verwenden wollen, um den Hergang dieses Unfalls zu dokumentieren (jedenfalls solange sie der Auffassung sind, dass sie diesen nicht selbst verschuldet haben).

Wir, insoweit bestätigt durch ein Urteil des Verwaltungsgerichts Ansbach vom 12. August 2014, Az. 4 K 13.01634, sind der Auffassung, dass die Interessen aller anderen Verkehrsteilnehmer, nicht aufgenommen zu werden, gegenüber dem Interesse des Dashcam-Betreibers eindeutig überwiegen.

Wir haben im Rahmen von Vorträgen oder Besprechungen Polizeidienststellen in Bayern über diese Rechtslage informiert. Insbesondere die Polizeidienststellen in Mittelfranken haben in den Jahren 2015 und 2016 immer wieder bei Fahrzeugkontrollen Ereignismeldungen oder Ordnungswidrigkeitenanzeigen aufgenommen, wenn ihnen Dashcams aufgefallen sind, und diese an uns weitergeleitet. Soweit die Verfahren als Ordnungswidrigkeitenverfahren eingegangen sind (13), waren diese auch als Ordnungswidrigkeitenverfahren weiterzuführen. Soweit lediglich Ereignismeldungen eingegangen sind (35), hätten wir die Möglichkeit gehabt, diese Verfahren im sog. aufsichtlichen Verfahren fortzuführen. Dabei hätte die Aufsichtsbehörde den Sachverhalt gegebenenfalls noch weiter aufklären und dann entscheiden müssen, ob ein Datenschutzverstoß gegeben ist oder nicht. Für den Fall, dass ein Datenschutzverstoß vorliegt, hätte die Behörde eine Anordnung (Verwaltungsakt) mit dem Ziel erlassen können, die Kamera in dem für rechtswidrig erkannten Umfang nicht mehr zu nutzen und vorhandene Aufnahmen zu löschen. Nachdem sich dieser Appell schon häufig aus den Unterlagen ergeben hat, die von der Polizei vorgelegt wurden, haben wir derartige Verfahren nicht mehr als aufsichtliche Verfahren fortgeführt.

Für den Fall der Verfahrensbeendigung musste dann, wenn kein förmliches Ordnungswidrigkeitsverfahren eröffnet war, keine weitere Information an den Dashcam-Nutzer ergehen. Sofern Ordnungswidrigkeitenverfahren eingestellt wurden, mussten und wurden die Beteiligten darüber informiert.

Statistisch lässt sich der Ablauf und Ausgang der Verfahren wie in der unten angefügten Tabelle darstellen. Bei den Zahlen fällt auf, dass im Jahr 2015 knapp die Hälfte aller Verfahren und im Jahr 2016 bis auf einen Fall alle Verfahren durch die Datenschutzaufsichtsbehörde eingestellt wurden. Der Grund dafür lag darin, dass die Gerichte, die über die Einsprüche gegen die Bußgeldbescheide entschieden haben, in den mündlichen Verhandlungen zum Ausdruck brachten, dass von der Aufsichtsbehörde nachgewiesen werden müsse, dass die Kamera tatsächlich benutzt wurde, sowie dass (auf sichergestellten Aufnahmen) nachweisbar ist, dass personenbezogene Daten (Menschen oder Fahrzeugkennzeichen) in einer Art und Weise enthalten sind, dass sie auch tatsächlich identifiziert werden können. Da nur in den

	Summe Dashcam-Verfahren bei BayLDA	davon von Polizei / Staatsanwaltschaft abgegeben	Einstellung durch BayLDA	Bußgeldbescheid BayLDA	ohne Rechtsmittel unanfechtbar geworden	Einspruch eingelegt	von Gericht gehalten	von Gericht eingestellt	Verfahren läuft noch
2015	34	31	18	16	11	5	1	3	1
2016	18	17	17	1	-	1	-	-	1

allerwenigsten Fällen im Rahmen der polizeilichen Ermittlungen der Sachverhalt so dokumentiert und mit Beweismitteln versehen an uns abgegeben wurde, wurden die Verfahren eingestellt.

Für unsere Tätigkeit nicht motivierend waren Gerichtsentscheidungen, in denen zwar festgestellt wurde, dass ein datenschutzrechtlicher Verstoß vorliegt, dieser aber vom Gericht ohne nähere Begründung als „nicht als ahndungswürdig" angesehen und das Verfahren daher eingestellt wurde.

Wir haben die Polizeidienststellen deshalb darauf hingewiesen, dass aus verfahrensökonomischen Gründen nur noch dann Verfahren wegen der Nutzung von Dashcams an die Datenschutzaufsichtsbehörde weitergeleitet werden sollten, wenn durch die Polizeibediensteten vor Ort die unzulässige Nutzung dokumentiert und die entsprechenden Beweismittel – d. h. Speicherkarten mit Aufnahmen auf denen identifizierbare Personen und/oder Kfz-Kennzeichen erkennbar sind – sichergestellt oder von den Fahrzeugführern freiwillig der Polizei übergeben wurden.

20

Fahrzeugdaten

20 Fahrzeugdaten

20.1 Gemeinsame Erklärung mit dem Verband der Automobilindustrie

Als Grundlage für die Behandlung datenschutzrechtlicher Fragestellungen bei vernetzten und nicht vernetzten Kraftfahrzeugen wurde zusammen mit dem Verband der Automobilindustrie (VDA) ein Papier erarbeitet, das als „Gemeinsame Erklärung" im Januar 2016 veröffentlicht worden ist.

Im Hinblick auf die fortschreitende informationstechnische Ausstattung der Kraftfahrzeuge und deren Anbindung an das Internet sowie der absehbaren Vernetzung der Verkehrsteilnehmer untereinander und mit der Verkehrsinfrastruktur hatten wir im Jahre 2014 eine Wiederaufnahme von Gesprächen mit dem VDA angestoßen, um gemeinsame Positionen in Datenschutzfragen zu erreichen (siehe dazu Nr. 20.2 unseres 6. Tätigkeitsberichts).

Links:
www.lda.bayern.de/media/baylda_report_06.pdf

Im Laufe des Jahres 2015 konnte zwischen den Datenschutzaufsichtsbehörden und dem VDA in mehreren Gesprächsrunden Einigkeit zu einer Reihe von Datenschutzfragen erreicht werden, was dann in eine am 26. Januar 2016 veröffentlichte „Gemeinsame Erklärung" mündete.

Links:
www.lda.bayern.de/media/dsk_gemeinsame_erklaerung_vda.pdf

Bedeutsam dabei ist vor allem das gemeinsame Verständnis, wann die bei der Kfz-Nutzung anfallenden Daten als personenbezogen im Sinne des Datenschutzrechts anzusehen sind und dass die Information der Kfz-Halter und Fahrer über die bei der Kfz-Nutzung anfallenden Daten verbessert werden muss.

Für Anfang 2017 ist angestrebt, einen neuen Muster-Informationstext der Autohersteller für die Kfz-Halter und Fahrer endgültig abzustimmen.

Wichtig ist uns zu der umfangreichen Datenverarbeitung bei der Nutzung von Kraftfahrzeugen auch, dass die Fahrzeugnutzer möglichst durch verschiedene Optionen über die Verarbeitung und Nutzung personenbezogener Daten selbst bestimmen können. Die Automobilhersteller streben nach ihren Aussagen z. B. an, durch standardisierte Symbole im Cockpit den aktuellen Vernetzungsstatus des Fahrzeugs erkennbar anzuzeigen und Möglichkeiten der jederzeitigen Aktivierung und Deaktivierung dieses Status vorzusehen. Vom Nutzer eingegebene Informationen (z. B. Komfortdaten wie Sitzeinstellung, bevorzugte Radiosender, Navigationsdaten, Kontaktdaten etc.) muss der Nutzer jederzeit selbst ändern oder zurückstellen können. Einschränkungen der Löschbarkeit bestehen bei rechtlichen Verpflichtungen oder dann, wenn entsprechende Daten im Zusammenhang mit Garantie- sowie Gewährleistungen oder der Produkthaftung von Bedeutung sind oder deren Verfügbarkeit für den sicheren Fahrzeugbetrieb erforderlich ist.

20.2 Datenerhebung nach tödlichem Verkehrsunfall mit Car-Sharing-Fahrzeug

In Strafprozessen können Fahrzeugdaten den Fahrer belasten.

Presseorgane berichteten über einen Strafprozess mit Schlagzeilen, dass ein Kfz-Hersteller zu einem Verkehrsunfall ein Fahrzeugbewegungs-

profil an das Gericht weitergegeben hätte. Bei dem Unfall hatte ein Fahrer mit einem gemieteten sog. Car-Sharing-Fahrzeug infolge weit überhöhter Geschwindigkeit innerorts einen Radfahrer tödlich verletzt.

Unsere Ermittlungen bei den beiden beteiligten bayerischen Unternehmen ergaben, dass das Gericht für die Aufklärung des schwerwiegenden Unfalls mit den dann gesetzlich gegebenen Mitteln des Strafprozessrechts beim Kfz-Hersteller und bei dem Car-Sharing-Unternehmen die dort vorliegenden Daten zu dem Fahrzeug und der konkreten Fahrt herausverlangt hatte. In Kombination dieser Daten und mit den Feststellungen am Unfallort konnte dem Fahrer nachgewiesen werden, dass er innerhalb der Stadt viel zu schnell gefahren ist und er deshalb den tödlichen Unfall schuldhaft verursacht hat.

Bei den beteiligten Unternehmen hat sich für uns folgendes ergeben: Das Car-Sharing-Unternehmen speichert für die Vertragsabwicklung die Personalien sowie die Fahrzeugbuchungs- und Zahlungsdaten des Automieters. Zusätzlich werden rechtlich und technisch getrennt davon beim Kfz-Hersteller im Rahmen des mit den Fahrzeugmietern vertraglich vereinbarten Geschäftsmodells auch Bewegungsdaten des Fahrzeugs (GPS-Positionen, Uhrzeiten, Geschwindigkeiten) für einige Tage gespeichert. Im Hinblick auf die gegebenen vertraglichen Vereinbarungen des Fahrzeugmieters mit dem Car-Sharing-Unternehmen und dem Kfz-Hersteller war dagegen von unserer Seite nichts Grundsätzliches einzuwenden. Die Informationen der Fahrzeugmieter zur Erhebung und Verwendung der Fahrtendaten für einen Mietzeitraum in den Vertragsbedingungen waren nach unserer Auffassung allerdings zu verdeutlichen, was inzwischen erfolgt ist.

20.3 Auskünfte nach § 34 BDSG von Kfz-Herstellern bei Motor-Tuning

Ein Auskunftsanspruch nach § 34 BDSG gegenüber dem Kfz-Hersteller zu legalem Motor-Tuning besteht, wenn dadurch Gewährleistungsansprüche vereitelt werden.

Von Kfz-Haltern werden bei Kfz-Herstellern immer wieder durch Auskunftsanträge nach § 34 BDSG eventuell vorliegende Informationen verlangt, um ein vermutetes Tuning durch den vorherigen Halter aufzuklären. Daten über Veränderungen an einem Fahrzeug im Zeitraum eines früheren Halters sind zunächst auf diesen früheren Halter personenbeziehbar im Sinne des BDSG. Dadurch, dass das Eigentum (bzw. der Besitz) an einem Fahrzeug wechselt, gehen nicht eventuell auf vorherige Halter personenbeziehbare Daten automatisch (auch) in die Personenbeziehbarkeit zu dem aktuellen Halter über, sondern nur dann, wenn diese Daten aufgrund eines bestimmten Ereignisses, z. B. Bearbeitung oder Ablehnung eines Gewährleistungsantrags, beim Hersteller (auch) zu dem aktuellen Halter hinzu gespeichert bzw. genutzt wurden.

In einem uns vorgetragenen Fall konnte der aktuelle Halter hierzu auch einen Auskunftsanspruch nach § 34 BDSG gegenüber dem Hersteller geltend machen, weil die dort gespeicherten Informationen (private Tuning-Maßnahmen durch den Vorbesitzer, deshalb Ablehnung eines Gewährleistungsanspruchs) auch den aktuellen Halter betrafen und sich auf ihn bezogen. Da mit einem zulässigen Tuning eine rechtmäßige Veränderung der Fahrzeugsubstanz durch den Eigentümer (den vorherigen Halter) vorliegt, besteht insoweit jedoch kein genereller Auskunftsanspruch nach § 34 BDSG gegenüber dem Hersteller. Es verbleibt dann bei einem eventuellen zivilrechtli-

chen Auskunftsverlangen direkt gegenüber dem Vorbesitzer.

Ausblick zur DS-GVO:
Wir gehen davon aus, dass bei solchen Sachverhaltenen unter Geltung der DS-GVO die dann nach Art. 6 Abs. 1 f) zu erfolgende Interessenabwägung im Hinblick auf die DS-GVO-Regelungen zur Zweckbindung (Art. 6 Abs. 4) und zu einer fairen Verfahrensweise nach den Grundsätzen von Treu und Glauben (Art. 5 Abs. 1 a) in vergleichbarer Weise ausfällt.

20.4 Nachweis des Halterzeitraums und der Berechtigung für Auskünfte nach § 34 BDSG

Ein Kfz-Halter muss bei Auskunftswünschen nach § 34 BDSG zu Fahrzeugdaten seine Berechtigung belegen.

Wenn Kfz-Halter bei Kfz-Werkstätten oder Kfz-Herstellern Auskunftsanträge nach § 34 BDSG zu dort anlässlich von Reparatur-, Wartungs- und Garantiesachverhalten oder sog. Connect-Diensten gespeicherten Fahrzeugdaten verlangen, ist zunächst zu klären, welche Daten zu dem aktuellen Halterzeitraum gehören und welche Daten die Daten von Vorbesitzern sind. Mit der Zulassungsbescheinigung kann z. B. von einem anfragenden Fahrzeughalter der Zeitraum seiner Haltereigenschaft dargelegt werden, soweit es um nur auf den Halter beziehbare Daten geht (z. B. bei der Werkstatt gespeicherte Wahrnehmung von Serviceterminen, Reparaturen, Tuning-Maßnahmen). Sind dabei Daten betroffen, die sich (auch) auf Fahrer eines Kfz beziehen können (wie evtl. bei der Werkstatt oder beim Hersteller gespeicherten Bremswerte, Motordrehzahlen oder Fahrtstreckendaten), muss der Halter entweder versichern, dass er der einzige Fahrer mit diesem Auto ist oder andernfalls die Einwilligung der übrigen Fahrer beibringen.

20.5 Gefälschte Kilometerstände

Bei Gebrauchtfahrzeugen sind gefälschte Kilometerstände laut Untersuchungen des ADAC eine Massenerscheinung, um für die Fahrzeuge einen höheren Erlös zu erzielen. Der Datenschutz steht in begründeten Verdachtsfällen den Aufklärungsmaßnahmen der betrogenen Fahrzeugkäufer nicht entgegen.

In einigen Fällen wandten sich Kfz-Halter, Kfz-Werkstätten oder Kfz-Hersteller an uns mit Fragen zu Auskünften bei mutmaßlich gefälschten Kilometerständen eines Gebrauchtfahrzeugs. Hat ein Kraftfahrzeughalter nachvollziehbare schlüssige Anhaltspunkte dafür, dass der Kilometerstand des gekauften Gebrauchtfahrzeugs in unzulässiger Weise auf einen niedrigeren Stand zurückgesetzt worden ist, möchte er für sein weiteres zivil- und strafrechtliches Vorgehen möglichst viele Informationen zu eventuellen Tätern und zum wahren Kilometerstand erlangen.

Dabei versuchen Kraftfahrzeughalter auch über Auskunftsersuchen zu den eigenen Daten nach § 34 BDSG oder Anfragen zu einer Übermittlung von Daten zu Vorbesitzern nach § 28 Abs. 2 BDSG bei Kfz-Werkstätten und beim betreffenden Kfz-Hersteller Licht ins Dunkel zu bringen. Kfz-Werkstätten oder Hersteller müssen einerseits berechtigten Auskunftsansprüchen nach § 34 BDSG nachkommen. Andererseits wollen Werkstätten und Hersteller bei darüber hinausgehenden Auskunftswünschen ihrer Kunden gemäß § 28 Abs. 2 BDSG im Hinblick auf die Kunden-Zufriedenheit eine sachgerechte, aber wenn möglich auch kundenfreundliche Entscheidung treffen.

§ 34 BDSG gewährt nur einen Anspruch auf Auskunft über bei einer Werkstatt oder dem Kfz-Hersteller zur Person des Betroffenen gespeicherten Daten. In Sachverhalten von gefälschten Kilometerständen beziehen sich die

fraglichen Daten zum einen auf den aktuellen Halter des Fahrzeugs, zum anderen aber auch auf Vorbesitzer und eventuell sonst in Betracht kommende Täter (sog. Daten mit Doppel-/Mehrfach-Bezug). Zu einem geltend gemachten Auskunftsanspruch nach § 34 BDSG müssen angefragte Werkstätten und Hersteller die möglicherweise entgegenstehenden überwiegenden rechtlichen Interessen eines Dritten gemäß § 34 Abs. 7 i.V.m. § 33 Abs. 2 Nr. 3 BDSG prüfen, um eventuell unbeteiligte Dritte nicht in einen Betrugsverdacht zu bringen. Während Auskünfte über bei einer Kfz-Werkstatt oder beim Kfz-Hersteller gespeicherten anderen Kilometerständen zu einem bestimmten Fahrzeug danach regelmäßig möglich sein werden, trifft das auf Namen möglicher Täter nicht zu. Denn Daten über Werkstatt- oder Servicearbeiten, Kulanzregelungen etc., welche z. B. ein früherer Halter eines PKW bei einer Werkstatt oder einem Hersteller hinterlassen hat, sind auf diesen Halter personenbeziehbar im Sinne des BDSG. Dadurch, dass das Eigentum (bzw. der Besitz) an einem Fahrzeug wechselt, gehen nicht eventuell auf vorherige Halter personenbeziehbare Daten über Werkstatt- oder Servicearbeiten automatisch (auch) in die Personenbeziehbarkeit zu dem aktuellen Halter über, sondern z. B. nur dann, wenn diese Daten aufgrund eines bestimmten Ereignisses, z. B. Bearbeitung eines Garantie-/Gewährleistungsantrags, (auch) zu dem aktuellen Halter hinzu gespeichert wurden.

Ein sonstiger Auskunftsantrag eines Halters beim Hersteller zu diesen Daten ist datenschutzrechtlich nach § 4 Abs. 1 und § 28 Abs. 2 Nr. 2a BDSG zu beurteilen. Es ist dabei Sache des anfragenden Halters, ein überwiegendes berechtigtes Interesse nach § 28 Abs. 2 Nr. 2a BDSG schlüssig darzulegen und soweit erforderlich zu begründen. Nur wenn Werkstatt oder Hersteller eine Datenübermittlung aufgrund der Interessenabwägungsvorschrift in § 28 Abs. 2 Nr. 2a BDSG in Erwägung ziehen, muss die nach dem BDSG verantwortliche Stelle die neben den Interessen des anfragenden Halters bestehenden anderen Interessenlagen prüfen, um nicht eventuell unbeteiligte Dritte unberechtigt in einen Betrugsverdacht zu bringen. Dabei kann sich bei Sachverhalten einer nach allen Umständen mit großer Wahrscheinlichkeit durch den vorherigen Halter durchgeführten Tachomanipulation ergeben, dass dieser Person keine überwiegenden Interessen nach § 28 Abs. 2 Nr. 2a BDSG zukommen, die eine Übermittlung seiner Kontaktdaten durch Werkstatt oder Hersteller an den nachfolgenden (betrogenen) Halter ausschließen. In Zweifelsfällen oder bei unklaren Sachverhaltssituationen kann eine Datenübermittlung auch von der Einwilligung des früheren Halters abhängig gemacht werden, der sich dadurch von einem Verdacht entlasten kann. Weitergehende Nachforschungen in strafrechtsrelevanten Fällen sind dann Sache der staatlichen Ermittlungsbehörden.

Ausblick zur DS-GVO:

Wir nehmen an, dass künftig die nach Art. 6 Abs. 1 f) zu erfolgende Interessenabwägung in vergleichbarer Weise ausfällt.

21

Datenpannen

21 Datenpannen

Bereits im Kapitel 2.1.5 haben wir dargestellt, wie stark die Zahl der bei uns eingegangenen Meldungen zu § 42a BDSG-Vorkommnissen in den letzten Monaten angestiegen ist. Jedoch möchten wir dabei betonen, dass uns tatsächlich wohl nach wie vor nur ein Bruchteil der vorgefallenen Datenpannen gemeldet wird. Dies erkennen wir zum Beispiel darin, dass uns im Bankenumfeld, in dem § 42a BDSG-relevante Daten verarbeitet werden, nur bestimmte Banken Meldungen machen. Wir schließen daraus aber nicht, dass gerade dies die Banken sind, die nicht sorgsam mit Kundendaten umgehen und regelmäßig Datenschutzverstöße begehen. Im Gegenteil: Wir erkennen, dass es sich hierbei um Geldinstitute handelt, die eigene Fehler rasch erkennen, pflichtbewusst handeln und zur Aufarbeitung beitragen wollen – auch im Sinne der eigenen Compliance.

Leider müssen wir feststellen, dass nicht jede verantwortliche Stelle diesen Weg einschlagen möchte und Geschehenes daher lieber unter den Teppich gekehrt wird in der Hoffnung, dass ein Vorfall nicht an das Tageslicht gelangt. Eine solche Entscheidung kann unter Umständen verhängnisvoll werden – das zeigen uns die Fälle, in denen wir aus der Presse von Datenpannen nachträglich erfahren haben. Hier stellten wir den verantwortlichen Stellen natürlich die Frage, warum nicht die erforderliche Meldung bei uns als zuständige Aufsichtsbehörde gemacht wurde. Die Begründungen waren zuletzt teils abenteuerlich. Die meisten teilten aber – wohl ehrlich – mit, nicht gewusst zu haben, dass eine solche Meldung bei uns erforderlich gewesen wäre. Aus diesem Grund möchten wir in diesem Kapitel noch einmal die Gelegenheit nutzen, grundlegende Arten von meldepflichtigen Vorfällen der Jahre 2015 und 2016 beispielhaft darzustellen, in der Hoffnung, dass Unternehmen ähnliche Fehler vermeiden oder wenn doch etwas passiert, ihrer gesetzlichen Verpflichtung nachkommen und uns informieren.

Ausblick zur DS-GVO:
Im Kapitel 2.1.5 haben wir in einem kurzen Ausblick auf die neuen Artikel 33 und 34 DS-GVO zum künftigen Umgang mit solchen Datenpannen hingewiesen. An dieser Stelle möchten wir ergänzend hinzufügen, dass die zuständigen Aufsichtsbehörden bei Verantwortlichen, die Datenpannen bewusst verschweigen oder nicht fristgerecht melden, nach jetzigem Kenntnisstand über einen deutlich größeren Bußgeldrahmen verfügen.

21.1 Hacking-Angriffe: Jagd nach digitalen Identitäten

Kundendaten von Webseiten sind oft (viel zu) leichte Beute für Internetverbrecher – Millionen Nutzer werden so unfreiwillig zu Opfern.

Ein deutliches Wachstum im Bereich der gemeldeten Datenpannen haben wir gerade im kriminellen Hacking-Umfeld vernommen. Der Begriff „Cybercrime" ist schon länger in aller Munde. Durch die – leider erfolgreichen – Attacken der jüngsten Vergangenheit auf führende internationale IT-Konzerne wie Yahoo, Ebay, LinkedIn oder Sony sind auch eine Vielzahl von Privatpersonen nun schon einmal selbst Betroffene von Hacking-Attacken geworden. Aber auch kleinere Unternehmen in unserer Zuständigkeit geraten vermehrt in den Fokus der sog. Black Hats, wie destruktive Hacker genannt werden. Im „besten" Fall informiert die verantwortliche Stelle ihre Kunden zeitnah über den Angriff und dessen Ausmaß, nennt konkrete Maßnahmen zur Schadensminimierung und unterstützt die Kunden im Umgang mit dem Datenverlust. Oft geschieht es aber, dass die verantwortliche Stelle die Kunden gar nicht informiert, oder wie im Fall von Yahoo, erst Jahre später.

Dass für betroffene Nutzer jedoch eine reale (Folge-)Bedrohung nach solchen Angriffen besteht und man als Betroffener tatsächlich zeitnah selbst reagieren muss, zeigen die Beobachtungen im Darknet: Dort werden die gestohlenen Nutzerdaten zum Spottpreis angeboten, ohne dass die betroffenen Personen wissen, dass ihre Daten gerade versteigert werden. Klassischerweise befinden sich in einem solchen Datensatz Name, E-Mail-Adresse, Passwort, Telefonnummer, Informationen zu Geburtstagen sowie Sicherheitsfragen zur Feststellung der Identität der Nutzer. Auch wenn keine Bank- oder Kreditkartendaten abhandengekommen sind, sind dennoch die Voraussetzungen für die Meldung einer Datenpanne erfüllt. Nach § 15a TMG hat ein Diensteanbieter die Vorschriften aus § 42a BDSG zu berücksichtigen, wenn er feststellt, dass bei ihm gespeicherte Bestands- oder Nutzungsdaten unrechtmäßig übermittelt worden sind, oder wie im Fall eines solchen Hacking-Angriffs, auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind. Gleichzeitig müssen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der betroffenen Nutzer drohen. Dies betrachten wir bspw. dann als eingetreten, wenn Daten wie E-Mail-Adresse mit Passwort abhandenkommen. Durch die unrechtmäßige Kenntniserlangung der E-Mail-Adresse in Kombination mit einem Passwort durch Dritte besteht eine reale Bedrohung für die schutzwürdigen Interessen des Nutzers. Es handelt sich hierbei schließlich um eine Art digitale Identität, die es zu schützen gilt. Sollte ein Nutzer das gleiche Passwort bei mehreren Diensten nutzen, besteht ein weiteres, hohes Missbrauchsrisiko durch den Angreifer. Aber selbst wenn der Nutzer das entwendete Passwort ausschließlich für die gehackte Webseite verwendet hat, kann ein Angreifer in manchen Fällen durch die Art und die Struktur des Passworts ein Schema der Zusammensetzung erkennen und andere Passwörter des Nutzers "erraten" (z. B. musterMAX17). Aus diesem Grund haben wir in solchen Fällen darauf hingewirkt, dass die verantwortliche Stelle in ihrem verpflichtenden Informationsschreiben an die Betroffenen auch auf die Bedrohungslage für andere Dienste, die der Nutzer mit der E-Mail-Adresse (und ggf. dem Passwort) nutzt, eingehen, und den Betroffenen empfehlen, umgehend neue, sichere Passwörter zu setzen. Zudem mussten wir – zum Glück nur wenigen – verantwortlichen Stellen verdeutlichen, dass sie dafür Sorge tragen müssen, dass ein Login mit den gestohlenen Daten unterbunden wird. Die Identitätsfeststellung des „echten" Nutzers kann hierbei für Unternehmen dann zum Problem werden, wenn die Angreifer rasch reagieren und versuchen die Konten zu übernehmen. Hier helfen leider auch keine Sicherheitsabfragen mehr, wenn die zugehörigen Antworten ebenso gestohlen wurden. Lediglich eine Authentifizierung mit einem weiteren Faktor, wie z. B. einer SMS an eine hinterlegte Mobilfunknummer, kann hier vorbeugend wirken und im Schadensfall unterstützen.

Wir müssen somit festhalten, dass Login-Verfahren, die nur aus E-Mail-Adresse und Passwort bestehen, eher als kritisch zu bezeichnen sind – so komfortabel sie für den Nutzer auch erscheinen. Für Webanwendungen mit hohem Schutzbedarf (z. B. im medizinischen Umfeld oder Online-Banking) sind diese Login-Verfahren daher nicht geeignet. Etwas entschärfen lassen sich solche Vorfälle nur, wenn das Verfahren zur Speicherung der Passwörter dem Stand der Technik entspricht und die verantwortliche Stelle von Kunden sichere, d. h. lange und komplexe, Passwörter gefordert hat – in diesen Fällen ist dann für Angreifer eine Berechnung nicht mehr lohnenswert bzw. zum Teil überhaupt nicht in einem verhältnismäßigen Zeitraum durchzuführen.

Abschließend möchten wir noch ergänzen, dass wir in wenigen Fällen durch ähnlich lautende Datenschutzbeschwerden auf bis dato unbekannte Hacking-Vorfälle aufmerksam gemacht wurden. Versierte Nutzer hatten jeweils für bestimmte Webshops eine spezielle E-Mail-

Adresse eingerichtet, z. B. shop-a@xyz.de, und diese Adresse dann lediglich bei der verantwortlichen Stelle hinterlegt. Nun hatten sich mehrere Betroffene bei uns beschwert, dass sie über eine solche von ihnen eingerichtete E-Mail-Adresse mit Phishing-Angriffen konfrontiert oder durch Spam belästigt werden. Da auf Grund des Vorgehens der Betroffenen ausgeschlossen werden konnte, dass die E-Mail-Adresse durch den Nutzer selbst in irgendeiner Weise anderweitig veröffentlicht oder übermittelt wurde, lag die Vermutung nahe, dass die verantwortliche Stelle entweder die Daten bewusst weitergegeben hat oder gehackt wurde. Da wir bei einer bestimmten verantwortlichen Stelle im Berichtszeitraum mehrere solcher Beschwerden von unterschiedlichen Betroffenen erhalten haben, die verantwortliche Stelle jedoch gegenüber den Betroffenen einen Hacking-Angriff abstritt, haben wir uns schließlich selbst durch eine Vor-Ort-Kontrolle davon überzeugt, wie es zu der „Datenweitergabe" kam. Die Vermutung des Hacking-Angriffs hat sich dann im Rahmen der Datenschutzprüfung erhärtet.

21.2 Sicherheitslücken bei Web-Shops

Content Management Systeme (CMS) werden nicht immer aktuell gehalten, wodurch Angreifern das Ausnutzen von Sicherheitslücken erleichtert wird.

Es kommt leider immer noch dazu, dass gerade kleinere Unternehmen CMS unbedarft nutzen und diese nach Inbetriebnahme nicht weiter aktuell halten. Meist gehen die Betreiber wohl davon aus, dass die Systeme dauerhaft ausreichend sicher seien, oder es sollen die laufenden Betriebskosten der Webseite gering gehalten werden. Da aber gerade die weit verbreiteten CMS attraktive Angriffsziele für Datendiebe sind, werden immer wieder neue Schwachstellen gefunden und kommuniziert. Folglich muss man als verantwortliche Stelle besondere Obacht geben und auf entsprechende Sicherheitshinweise des jeweiligen CMS-Herstellers zeitnah reagieren – oder einen fachkundigen IT-Dienstleister damit beauftragen. Wir empfinden es zumindest als blauäugig, ein solches System einmal einzurichten und ungepatcht über Jahre online anzubieten.

Im Berichtszeitraum wurden in unserer Zuständigkeit bspw. gravierende Lücken in Magento-Shop-Systemen und MongoDB-Datenbanken bekannt. Obwohl sowohl die betroffenen Software-Anbieter als auch namhafte IT-Zeitungen darüber berichteten und den Handlungsbedarf kommunizierten, fanden wir mehrere bayerische verantwortliche Stellen, die entsprechende Sicherheitslücken trotz deutlich verstrichener Zeit nicht geschlossen hatten. Grundsätzlich löst eine solche Schwachstelle noch keine Verpflichtung zu einer Meldung nach § 15a TMG aus. Jedoch konnten wir in manchen Fällen feststellen, dass die vorhandene Sicherheitslücke nachweislich von Angreifern auf der jeweiligen Webseite ausgenutzt worden ist und dadurch gezielt Schadcode zum Abfangen von Bankdaten der Nutzer platziert wurde. Somit waren die Voraussetzungen für § 15a TMG erfüllt.

21.3 Verschlüsselungstrojaner und Malware

Erpressungsversuche durch verschlüsselte oder geklaute Kundendaten haben explosionsartig zugenommen – viele Verantwortliche zahlen und schweigen.

In den Medien wurde in den vergangenen Jahren über die Verbreitung von Verschlüsselungstrojanern und anderer Erpressungs-Malware berichtet. So hatte bspw. heise security im Sommer 2016 über eine große Infektionswelle durch die Ransomware „Locky" informiert. Vor allem durch gefälschte Bewerbungs-

und Rechnung-E-Mails wurde der Schadcode, der sich meist in einer JavaScript-Datei im Dateianhang befand, übermittelt. Mit eingetretener Infektion, d. h. nachdem ein Mitarbeiter die Datei ausführte, wurden im betroffenen Unternehmen ganze Datenträger so verschlüsselt, dass ein Arbeiten mit den Daten nicht mehr möglich war. Die Täter forderten via Bildschirmmeldung Lösegeldzahlungen per Bitcoin. Da es sich hierbei um gravierende kriminelle Machenschaften handelt, waren wir als Datenschutzaufsichtsbehörde richtigerweise nicht (erste) Anlaufstelle, sondern entweder die Polizei zum Zweck der Strafanzeige oder gleich das Bayerische Landeskriminalamt und das Bayerische Landesamt für Verfassungsschutz, die beide im Bereich des Cybercrime als Spezialisten regelmäßig mit Fällen dieser Art umgehen.

Nichtsdestoweniger wurden auch wir mit solchen Erpressungen konfrontiert. Das lag daran, dass zum Teil nicht klar war, ob es lediglich zu einer Verschlüsselung von Daten gekommen ist (wodurch zumindest Verfügbarkeit, Integrität und Vertraulichkeit der Daten gefährdet war), oder ob es auch zu Datenabflüssen zu den unbekannten Angreifern kam. Tatsächlich konnten wir in wenigen Fällen feststellen, dass durchaus weiterer Schadcode neben den Verschlüsselungstrojaner aktiv war, der für Datenübermittlungen aus dem jeweiligen Unternehmensnetzwerk nach außen sorgte. Bei einem Unternehmen musste daher bspw. die unbefugte Kenntnisnahme von Kontodaten der Kunden angenommen werden, woraus eine Einstufung als Datenpanne nach § 42a BDSG erfolgte.

21.4 Skimming

Skimming ist nach wie vor verbreitet, um illegal Daten von Bankkunden an Geldautomaten auszulesen und anschließend missbräuchlich zu verwenden. Trotz neuer Schutztechniken gelingt es Skimmern immer wieder an Bankdaten heranzukommen.

Berichte über – zum Teil äußerst raffinierte – Manipulationen an Geldautomaten nehmen leider nicht ab. So haben auch wir im Berichtszeitraum wieder direkt von Fällen erfahren, bei denen es Tätern durch die gezielte Anbringung von zusätzlicher Technik (z. B. spezielle Tastatur, anderes Lese-Gerät oder Mini-Kamera) gelungen ist, Kartendaten und PIN von Kunden heimlich mitzulesen. Mit den „gewonnenen" Daten können Täter allgemein meist Kartendoubletten erstellen und Geld von den betroffenen Bankkundenkonten abheben. Diese Transaktionen finden in der Regel außerhalb von Deutschland statt, so dass sich die Täter nach Abhebung des Geldes mit dem Betrag „aus dem Staub" machen können.

Wir halten an unserer Einschätzung fest und bewerten Skimming-Vorfälle nach wie vor als meldepflichtige § 42a BDSG-Vorfälle. Die finanziellen Schäden für die Betroffenen sind teilweise nicht unerheblich, so dass – zumindest kurzfristig – durchaus schwerwiegende Beeinträchtigungen drohen können. Allerdings muss positiv festgehalten werden, dass die Banken in der Regel den Schaden ersetzen. Es bleibt aber auch künftig ein Wettlauf mit der Zeit zwischen Banken und Skimmern, da beide Seiten ständig die eingesetzte Technik für ihre Zwecke optimieren.

Am Rande erwähnen möchten wir dabei, dass uns auch von gesprengten Geldautomaten berichtet wird. Hierbei wird meist das gesamte Gehäuse des Automaten vollständig zerstört. In einem uns gemeldeten Fall wurde sogar ein

Teil des Bankgebäudes durch die Detonation in Mitleidenschaft genommen. Es handelt sich dabei aber um keine § 42a Vorfälle, da die Täter bei einer solchen Sprengung lediglich das Geld im Automaten als Ziel erkennen und im Regelfall keine Möglichkeit (und auch kein Interesse daran) haben, auf Daten von Kunden zuzugreifen.

21.5 Fehlversendung von Unterlagen oder Datenträgern

Bei einer Fehlversendung von sensiblen Daten können zumindest gezielte Versuche zur Schadensminimierung unternommen werden, wenn die Gegenseite bekannt ist – ansonsten bleibt oft Unklarheit, welches Schadensausmaß für die Betroffenen wirklich droht.

Der wachsende Arbeitsdruck führt dazu, dass Mitarbeiter zum Teil auch kritische Arbeiten schnell und routinemäßig abhandeln müssen – einfach weil ihnen keine zusätzliche Zeit hierfür gewährt wird. Gerade im Umgang mit sensiblen Daten sollte jedoch eine größere Sorgfalt geboten sein, da hier schließlich der mögliche Schaden um ein Vielfaches höher ausfallen kann – egal ob ein finanzieller Verlust, ein Image-Schaden oder die Offenbarung von Geheimnissen droht. Uns wurden im vergangenen Berichtszeitraum mehrere Fehlversendungen von sensiblen Unterlagen mitgeteilt, bei denen die Unachtsamkeit des versendeten Mitarbeiters wohl die ausschlaggebende Ursache für die Datenpanne war.

Wir hatten einige Fälle von fehlerhaft versendeten Papierunterlagen, z. B. mit detaillierten Daten zu aufgenommenen Krediten und Kontenübersichten oder aber auch ganze Arztbriefe mit Diagnosedaten, die an die falschen Patienten geschickt wurden. Auch wurde uns ein Fall gemeldet, bei dem eine unverschlüsselte USB-Festplatte fehlgesendet wurde. Dies geschieht jedoch viel seltener als die Fehlleitung eines Faxes oder einer E-Mail. Vor allem bei E-Mails ist es oft nur die Auswahl eines falschen Kontakts aus dem Adressbuch, und schon besteht die Gefahr einer Datenpanne. So wurden uns einige solcher Fälle gemeldet, bei denen durch die Fehlversendung von E-Mails mit Anhängen, aber auch durch Faxe, sensible personenbezogene Daten, zum Teil auch über Berufsgeheimnisträger, in nicht unerheblichen Umfang fehlgesendet wurden. In einem Fall war dies für den Versender „doppelt bitter", da die fehlgesendeten vertraulichen Informationen auch noch an die Konkurrenz gesendet wurden.

Wie im letzten Tätigkeitsbericht unter Kapitel 21.2 aufgeführt, bleiben wir bei unserer Auffassung, dass Fehlversendungen an sich nur durch eine sorgfältige Arbeitsweise verhindert werden können, im Alltag aber wohl nie gänzlich auszuschließen sind. Entsprechend sind organisatorische Maßnahmen zu treffen, die die Mitarbeiter bei der Ausführung ihrer Arbeiten, gerade im Umgang mit der Versendung sensibler Daten, bestmöglich unterstützen.

21.6 Einbruch und Entwendung von Datenträgern

Durch Verschlüsselung von Datenträgern nach dem Stand der Technik kann vermieden werden, dass Unbefugte trotz physikalischen Besitzes eines gestohlenen Datenträgers auch an die geschützten Daten gelangen.

Wie im vorangegangenen Berichtszeitraum kam es erneut zu gezielten Entwendungen von IT-Geräten sowie zu Einbrüchen, bei denen Datenträger mehr oder weniger bewusst entwendet wurden. Als Datenpanne ist ein solcher Vorfall dann zu melden, wenn zum einen die Datenträger personenbezogene Daten enthalten, die auf Grund ihrer Datenart als „sensibel"

einzustufen sind und zum anderen auch schwerwiegende Beeinträchtigungen der Betroffenen drohen können. Beim Diebstahl von mobilen Datenträgern ist daher oft die entscheidende Datenschutzfrage, ob und wenn ja, nach welchem Verfahren die Daten verschlüsselt wurden. Handelt es sich um ein Verschlüsselungsverfahren, das als ausreichend sicher im konkreten Anwendungsszenario einzustufen ist, so ist davon auszugehen, dass der Unbefugte mit verhältnismäßigen Mitteln nicht an die gespeicherten Daten gelangen kann. Im Alltag stellen wir jedoch fest, dass gerade Backup-Medien, die für Angreifer einen umfassenden Datens(ch)atz darstellen, oft noch unverschlüsselt oder ungeschützt abgelegt werden. So findet man bspw. Sicherungs-DVDs in einem gesonderten Schrank in der Hoffnung, dies wäre eine ausreichende Schutzmaßnahme gegen Einbrecher – was offensichtlich nicht der Fall ist. Aus diesem Grund betonen wir, dass grundsätzlich eine Meldung nach § 42a BDSG erforderlich ist, wenn auf einem entwendeten Datenträger keine ausreichenden kryptographischen Verfahren zum Schutz der Daten vor unbefugten Zugriff zur Anwendung kamen (und gleichzeitig die Voraussetzungen für die § 42a BDSG-Meldung ansonsten erfüllt sind). Relevant ist daher insbesondere für die zahlreichen Berufsgeheimnisträger wie Ärzte und Steuerberater, aber auch für das Bankenwesen, dass nicht nur im Umgang mit mobilen Datenträgern Verschlüsselungsverfahren eingesetzt werden, sondern auch bei der Datenspeicherung auf Tablets, Notebooks und klassischen stationären PCs.

Eine im Berichtszeitraum erneut aufgetretene Betrugsmasche, die ebenso unter die Kategorie „Entwendung von Datenträgern" fällt, war das Herausfischen von bereits ausgefüllten Papier-Überweisungsträgern aus den hierfür speziell vorgesehenen Bankbriefkästen. Den Tätern war es jeweils gelungen, zahlreiche Überweisungen herauszuziehen. Mit den darauf befindlichen Daten wurden dann betrügerische Überweisungen zum Schaden der betroffenen Bankkunden getätigt. Somit waren in diesen Fällen die Voraussetzungen für eine Meldung nach § 42a BDSG erfüllt. Die Banken haben daher nicht nur uns, sondern selbstverständlich auch ihre Kunden informieren müssen. Nach unserem Kenntnisstand wurde in allen Fällen den betroffenen Bankkunden der entstandene Schaden erstattet. Vermieden hätte dies werden können, wenn die betroffenen Banken moderne Sicherheitsbriefkästen für Überweisungen eingesetzt hätten, die ein solches Herausfischen nahezu unmöglich machen. Im Rahmen der Aufarbeitung des Vorfalls haben wir dies mit den Verantwortlichen besprochen, die uns gegenüber angaben, dass entsprechende bauliche Änderungen vorgenommen werden.

22

Technischer Datenschutz und Informationssicherheit

22 Technischer Datenschutz und Informationssicherheit

22.1 (Un)sicherheit digitaler Kommunikation

Eine datenschutzrechtliche Bewertung von Messenger-Diensten wie WhatsApp ist für uns beim Einsatz in bayerischen Unternehmen kaum zu leisten.

WhatsApp bezeichnet sich gemäß den eigenen Nutzungsbedingungen selbst als sog. Messenger-Dienst. Dies bedeutet, dass der Dienst insbesondere die Erbringung einer Kommunikationsleistung beinhaltet, wie z. B. den Versand von Text-, Bild-, Ton- und Videonachrichten. Aus datenschutzrechtlicher Sichtweise liegt WhatsApp daher wie andere Messenger-Dienste in der Zuständigkeit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Grundlage hierfür ist das Telekommunikationsgesetz.

Nichtsdestotrotz erhalten auch wir immer wieder Anfragen zum Einsatz von WhatsApp. Konkret geht es meist darum, unter welchen Rahmenbedingungen WhatsApp in bayerischen Unternehmen eingesetzt werden darf. Dabei kommt es zu unterschiedlichen Fragen wie die des Beschäftigtendatenschutzes, des Umgangs mit Berufsgeheimnissen und der IT-Sicherheit. Ein einfacher Verweis von uns auf die Zuständigkeit der BfDI für WhatsApp als Telekommunikationsdienst (TK-Dienst) hat sich bislang nicht angeboten, da es um die datenschutzrechtliche Bewertung von Geschäftsprozessen in bayerischen Unternehmen geht, wodurch ein Beratungsauftrag für uns durchaus gegeben war. So hatten wir Fälle, bei denen Arztpraxen und Apotheken WhatsApp als alternative Kontaktmöglichkeit (z. B. zur Terminvereinbarung oder Rezeptbestellung) einsetzen wollten. Ebenso hatten wir Anfragen, bei denen Banken oder andere Unternehmen innerhalb der eigenen Organisation WhatsApp als Kommunikationsmittel für die Beschäftigten nutzen wollten.

Bei Anfragen dieser Art konnten wir bisher lediglich eine vorbehaltliche Bewertung vornehmen. Das liegt daran, dass uns nach wie vor kein offizielles Datenschutzprüfergebnis des TK-Dienstes WhatsApp seitens einer Aufsichtsbehörde bzw. der BfDI vorliegt. Wir sind daher von den über den Dienst veröffentlichten Informationen abhängig. WhatsApp hat nach eigenen Angaben inzwischen eine Ende-zu-Ende-Verschlüsselung für die Kommunikationsinhalte eingeführt. Inwieweit diese tatsächlich den Sicherheitsanforderungen entspricht, entzieht sich unserer Kenntnis. Datenschutzrechtlich problematisch bleibt darüber hinaus weiterhin die Verarbeitung von Metadaten zu den Nachrichten in den USA sowie die Erhebung der Kontaktdaten aus dem Adressbuch der Nutzer. Ebenso bleibt letztendlich kritisch, wie das „Zusammenwirken" von WhatsApp und Facebook tatsächlich abläuft bzw. ablaufen wird.

Wir beurteilen daher für den Augenblick, dass das Angebot zur WhatsApp-Kommunikation durch ein Unternehmen an Kunden grundsätzlich dann nicht weiter von uns bemängelt wird, wenn vom Unternehmen auf die Datenschutzbedenken ausdrücklich hingewiesen und den Kunden gleichzeitig parallel ein anderer, von uns als sicher eingestufter Kommunikationsweg angeboten wird (z. B. verschlüsselter E-Mail-Versand per PGP); der Kunde kann sich in einem solchen Fall frei für oder gegen eine WhatsApp-Kommunikation entscheiden.

Eine WhatsApp-Kommunikation innerhalb eines Unternehmens unter den Beschäftigten bewerten wir allerdings als kritisch und schwer durchführbar. Es bestehen viele grundsätzliche Datenschutzbedenken. Gerade da im innerbetrieblichen Umfeld andere, sichere elektronische Kommunikationswege eingerichtet, genutzt und überprüft werden können, sollte auf diese zurückgegriffen werden.

22.2 Sichere Gestaltung von Passwort-Verfahren bei Webseiten

Der sorglose Umgang mit Passwörtern auf Webseiten stellt nicht nur für die Nutzer, sondern auch für die Betreiber ein datenschutzrechtliches Problem dar.

Bereits in den beiden vergangenen Tätigkeitsberichten hatten wir ausführlich über die Gefahren von Authentisierungsverfahren bei Webseiten über Nutzername und Passwort berichtet (Kapitel 19.2 im 5. Bericht, Kapitel 22.7 im 6. Bericht). Da sich in diesem Berichtszeitraum nicht nur Anfragen, sondern auch Beschwerden von Betroffenen hierzu häuften und wir in Prüfungen zudem feststellen mussten, dass grundlegende Anforderungen an einen sicheren Umgang mit Passwörtern durch Webseitenbetreiber zum Teil ignoriert werden, haben wir uns entschlossen, nachfolgend noch einmal wesentliche Aspekte hierzu festzuhalten.

Eine sichere Gestaltung von Passwort-Verfahren bei Webseiten zeichnet sich durch mehre Komponenten aus:

- Mindestanforderung an Länge und Komplexität des Passworts als Vorgabe durch den Webseitenbetreiber
- Hinweis auf die Passwortstärke für den Nutzer bei der Auswahl des Passworts
- Geeignetes Verfahren zur Speicherung der Passwörter beim Webseitenbetreiber
- Geeignetes Verfahren zum Zurücksetzen eines Passworts („Passwort-Vergessen"-Funktion)

Die Mindestanforderung an Länge und Komplexität des Passworts ist abhängig vom Einsatzzweck (Welche Daten sollen dadurch geschützt werden?) sowie vom dazugehörigen Passwortspeicherverfahren (Wie lange dauert es, ein Passwort unter einem bestimmten Hashverfahren zu berechnen?). Die Anforderung an die Passwortkomplexität geht somit von der Annahme aus, dass ein Angreifer einen gewissen Aufwand betreibt, um Passwörter entweder am Zielsystem selbst automatisiert auszuprobieren (wenn keine Sperrung trotz zahlreicher Versuche erfolgt) oder ein Unbefugter nach einem Passwort-Diebstahl versucht, dieses selbst zu berechnen und somit das ursprüngliche Passwort zu „knacken". Somit besteht im Datenschutz die gängige Empfehlung an ein sicheres Passwort, mindestens 10 – besser 12 – Zeichen zu verwenden, bestehend aus einer Kombination von Buchstaben (Groß- und Kleinschreibung), Ziffern und Sonderzeichen.

Sollte ein Nutzer sich jedoch kein sehr langes und komplexes Passwort merken wollen, so kann alternativ ein weniger sicheres Passwort gewählt werden, wenn der Nutzer im Rahmen der Passwortvergabe auf die Stärke bzw. Schwäche des Passworts ausreichend hingewiesen wird. Ein Unterschreiten der je nach Einsatzzweck definierten Mindestlänge und Mindestkomplexität darf jedoch nicht erfolgen (z. B. Passwort „123" oder „abc"). Bei der Darstellung der Passwortstärke haben sich in der Praxis sogenannte Passwortbalken etabliert, die den Nutzer auch über eine farbliche Änderung unmittelbar die Stärke des Passworts signalisieren.

Eine weitere entscheidende Komponente zur sicheren Gestaltung von Passwort-Verfahren sind die dazugehörigen Verfahren zur Speicherung der Passwörter. Diese sind von den Webseitenbetreibern nicht im Klartext, sondern durch geeignete kryptographische Verfahren verschlüsselt zu speichern. Hierbei ist darauf zu achten, dass ein Verfahren nach dem Stand der Technik verwendet wird. So sind bspw. MD5 und SHA1 nicht geeignet, da die Rekonstruktion eines Passworts auf Grund der effizienten Berechnung dieser Verfahren ohne großen Aufwand möglich ist. Auch existieren bereits

verschiedene vorberechnete Tabellen, sog. Rainbow-Tables, in denen Passwörter verschiedenster Komplexität und die dazugehörigen Hashwerte aus gängigen Hashverfahren enthalten sind. Bessere Verfahren wären bspw. SHA-3 oder auch RIPEMD320. Darüber hinaus existieren auch Verfahren wie bcrypt oder PBKDF2, die ineffizient zu berechnen sind und in manchen Fällen eine praktikable Lösung darstellen.

Ebenso ist für ein sicheres Passwortverfahren mitentscheidend, wie der Nutzer über sein Passwort informiert wird, z. B. im Rahmen eines Zurücksetzens. Wichtig ist hierbei, dass ein Passwort nicht im Klartext per E-Mail übermittelt wird. Stattdessen bieten sich Links mit zeitlich begrenzter Gültigkeit an, die dem Nutzer per E-Mail angeboten werden.

22.3 Verschlüsselung bei Mailservern (STARTTLS)

Mailserver sind so zu konfigurieren, dass eine ausreichende Transportverschlüsselung bei der Übermittlung von E-Mails ermöglicht wird.

Wie bereits in unserem letzten Tätigkeitsbericht beschrieben, haben wir im September 2014 eine Großprüfung zum Thema STARTTLS und Perfect Forward Secrecy in Bayern durchgeführt. Hierzu hatten wir im Rahmen einer automatisierten Onlineprüfung insgesamt 2236 Mailserver bayerischer verantwortlicher Stellen (nach § 3 Abs. 7 BDSG) daraufhin überprüft, ob sie den gesetzlichen Anforderungen zur IT-Sicherheit nach § 9 BDSG und der Anlage zu § 9 BDSG entsprechen. Geprüft wurde dabei insbesondere, ob die Mailserver über die Möglichkeit verfügen, verschlüsselt zu kommunizieren (Transportverschlüsselung) und dabei die Technik Perfect Forward Secrecy vorrangig unterstützen.

Wir haben uns entschieden, an dieser Stelle erneut darüber zu berichten, da wir auch im vergangenen Berichtszeitraum intensiv mit der Thematik beschäftigt waren. Während die meisten kontrollierten Unternehmen keine Schwierigkeiten hatten, die geforderten Maßnahmen umzusetzen, gab es einzelne Vorgänge, die sich zum Teil bis Herbst 2016 hingezogen haben. Das lag daran, dass wir zunächst die Unternehmen umfassend beraten haben und die benötige Zeit zur Umsetzung eingeräumt hatten – nach spätestens einem Jahr haben wir uns dann aber bei den noch offenen Fällen zur Einleitung von Anordnungen entschieden.

Konkret haben wir hierbei angeordnet, dass die E-Mail-Server so umzustellen sind, dass diese eine Transportverschlüsselung nach dem Stand der Technik unterstützen, so dass bei Verwendung von STARTTLS (opportunistisch) auch die Verschlüsselungstechnik Perfect Forward Secrecy wirksam zur Anwendung kommt. Die sowohl technisch als auch rechtlich ausführlich begründeten Anordnungen umfassten bis zu zehn Seiten. Wir haben für den Fall, dass eine verantwortliche Stelle der Anordnung nicht nachkommen möchte, ein Zwangsgeld in Höhe von 8.000 Euro angedroht. Alle verantwortlichen Stellen sind aber unserer Aufforderung unmittelbar nach Erhalt der Anordnung nachgekommen, so dass in keinem dieser Fälle das Zwangsgeld, sondern lediglich die Verwaltungsgebühr in geringer dreistelliger Höhe zu bezahlen war.

Somit möchten wir festhalten, dass die Anforderung von STARTTLS mit Perfect Forward Secrecy auch mittels Anordnungen von uns durchgesetzt wird.

22.4 Verschlüsselung bei Webseiten (HTTPS)

Eine erforderliche Maßnahme zum Schutz personenbezogener Daten bei Webseiten und anderen Diensten, die das HTTP-Protokoll nutzen, ist ein gut konfiguriertes HTTPS.

Werden personenbezogene Daten über das Internet versendet, so ist eine wirksame Verschlüsselung mit einem kryptographischen Verfahren nach dem Stand der Technik zwingend erforderlich. Wird das HTTP-Protokoll zur Übertragung genutzt, so ist entsprechend eine HTTPS-Verschlüsselung zu verwenden. Diese (Mindest-)Anforderung besteht für Webseitenbetreiber schon lange und wurde auch von uns im vergangenen Tätigkeitsbericht u. a. im Kapitel 22.4 aufgenommen.

Während wir bei Prüfungen im Online-Banking-Segment ebenso wie bei Webshops dies als üblich und meist gut umgesetzt erkennen, müssen wir feststellen, dass bei vielen „gewöhnlichen" Webseiten keine HTTPS-Verschlüsselung zum Einsatz kommt, obwohl die Seiten personenbezogene Daten übertragen. Eine solche Übertragung kann sich bspw. dann ergeben, wenn auf einer Webseite ein Kontaktformular vorhanden ist, ein Login für Nutzer angeboten wird oder auch eine persönliche Beitragskommentierung möglich ist. In diesen Fällen betrachten wir eine HTTPS-Verschlüsselung unabhängig vom Schutzbedarf als erforderlich. Bei einem normalen Schutzbedarf, also keine Übertragung von besonderen personenbezogenen Daten nach § 3 Abs. 9 BDSG, sondern bspw. lediglich Name, Anschrift, Telefonnummer und E-Mail-Adresse, sehen wir eine Transportverschlüsselung mit HTTPS als notwendig, aber auch ausreichend an. Dagegen bei einem hohen Schutzbedarf, wie bspw. Angaben über Gesundheit, Sexualleben, politische Meinungen oder religiöse Überzeugungen, gelten strengere Vorschriften. Hier ist zusätzlich zu HTTPS auch eine Ende-zu-Ende-Verschlüsselung, d. h. eine Inhaltsverschlüsselung, erforderlich. Diese Anforderung haben wir zuletzt gerade im Bereich von Ärzten und Apotheken vermehrt kommunizieren müssen und in einem separaten Kapitel in diesem Bericht behandelt (Kapitel 16.4).

Die Erforderlichkeit von HTTPS begründet sich u. a. aus der Weitergabekontrolle in der Anlage zu § 9 BDSG, die festlegt „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". Damit die Verschlüsselung ausreichend wirksam ist, muss nach unserer Einschätzung der Webserver so konfiguriert sein, dass primär kryptographische Verfahren zum Schlüsseltausch verwendet werden, die in die Klasse „Perfect Forward Secrecy" fallen. Diese Forderung leitet sich ebenfalls aus der Anlage zu § 9 BDSG ab, die u. a. bei der Weitergabekontrolle Verschlüsselungsverfahren nach dem Stand der Technik fordert. Wir verweisen hierbei auch auf die veröffentlichte Entschließung „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation" der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. März 2014.

Damit eine HTTPS-Verschlüsselung dem Stand der Technik entspricht, muss auf u. a. folgende Punkte geachtet werden:

- Es dürfen keine veralteten Protokollversionen unterstützt werden (SSL2, SSL3).
- Es sollte TLS 1.2 als Standardprotokollversion verwendet werden.
- Es muss die Verschlüsselungstechnik Perfect Forward Secrecy (PFS) eingesetzt werden.
- Die Schlüssellänge des SSL-Zertifikats sollte mindestens 2048-Bit betragen.

- Die Verfahren SHA-1 und RC4 sollten nicht (mehr) verwendet werden.
- Die Heartbleed-Lücke darf nicht vorhanden sein.
- Die Verwendung von HTTP Strict Transport Security (HSTS) ist zu prüfen.
- Es dürfen keine selbstsignierte Zertifikate genutzt werden, sondern welche einer als vertrauenswürdigen eingestuften offiziellen Zertifizierungsstelle.

22.5 Die Kehrseite der Verschlüsselung

Beim Einsatz verschlüsselter Kommunikation darf nicht vergessen werden, dass Schadcode unter Umständen unerkannt bis zum Endgerät des Nutzers gelangen kann. Verfahren, um verschlüsselte Angriffe zu erkennen (wie z. B. SSL Inspection), können ein erhebliches Sicherheitsrisiko darstellen und zudem datenschutzrechtlich unzulässig sein.

Während wir Verschlüsselungsverfahren stets als geeignete technische Maßnahme zum Schutz personenbezogener Daten kommunizieren und diese auch im Rahmen unserer Prüfungen fordern (HTTPS, STARTTLS, PGP, etc.), haben wir erkannt, dass manche verantwortliche Stellen dadurch irrtümlich ihre eigenen Prozesse als „absolut sicher" betrachten. Diesen Trugschluss möchten wir hier begegnen und vor möglichen Risiken warnen.

Bedrohungen zu erkennen ist bspw. eine der Aufgaben von Firewalls. Jedoch haben viele auf dem Markt verfügbare Produkte das Problem, dass bei verschlüsselter Kommunikation eine solche Bedrohung unter normalen Umständen nicht erkannt werden kann – Malware und andere Angriffstechniken können über den verschlüsselten Kanal „mitschwimmen". In diesen Fällen muss ein Unternehmen die Entscheidung treffen, ob die verschlüsselte Kommunikation mit diesen Nebenwirkungen akzeptiert wird oder ob man versucht, die verschlüsselten Verbindungen aufzubrechen, um so Schadcode zu erkennen. Das letztgenannte Vorgehen wird insbesondere beim Knacken von https-Verbindungen (mit SSL-Zertifikaten) „SSL Inspection" genannt und funktioniert ähnlich wie Man-in-the-Middle-Verfahren. Dies bedeutet gleichzeitig einen fragwürdigen Eingriff in die vertrauliche Kommunikation der Mitarbeiter. Kritisch zu hinterfragen ist hierbei vorallem, welche Regelungen im Betrieb zum Umgang mit E-Mail- und Internetnutzung getroffen wurden. Ist die private Nutzung zulässig, so ist ein Aufbrechen dieser verschlüsselten privaten Kommunikation ohne Einwilligung nicht zu rechtfertigen. Aber auch in anderen Fällen dürfte sich die Rechtfertigung des Einsatzes von SSL Inspection datenschutzrechtlich als Herausforderung darstellen.

Nichtsdestoweniger sind Verfahren wie SSL Inspection in der Praxis durchaus verbreitet, auch wenn über deren Einsatz meist geschwiegen wird. SSL Inspection wird oft als Heilsbringer bezeichnet, birgt jedoch selbst eigene Risiken: Einerseits, weil die Umsetzung durch die Hersteller der Softwareprodukte zum Teil durchaus fehlerhaft gestaltet werden und dem Nutzer dadurch größere Sicherheitsrisiken entstehen können, andererseits aber auch, weil dennoch nicht jeder Schadcode und Angriff erkannt wird, der Nutzer sich aber womöglich in trügerischer Sicherheit wähnt. Das größte Problem jedoch ist, dass ein Client im Unternehmen im Endeffekt nur noch eine vertrauenswürdige Kommunikation mit der eigenen SSL Inspection Software des Unternehmens aufbauen kann. Man kann sich dadurch nicht sicher sein, ob sich auch ein (weiterer) Angreifer zwischen dem eigentlichen Zielsystem und der Unternehmen-SSL-Inspection-Anwendung eingeklinkt hat. Durch den Einsatz von SSL Inspection können somit (ungewollt) gerade die Sicherheitsmaßnahmen ausgehebelt wer-

den, die SSL-Verschlüsselung den Anwendern bietet.

Eine der wichtigsten Komponenten zum Schutz vor verschlüsseltem Schadcode ist es daher, die Mitarbeiter entsprechend zu sensibilisieren und darauf vorzubereiten, dass Schadcode womöglich bis zu ihrem PC gelangen kann und dort erkannt – und nicht ausgeführt – werden muss. Dies ist bspw. auch bei PGP relevant, damit keine verschlüsselten E-Mails heimlich Schadcode bis zum Endnutzer transportieren und dann ohne nähere Prüfung nach der Entschlüsselung ausgeführt werden (z. B. bei gefälschten Bewerbungen und Rechnungen).

22.6 Phishing, Spam und sonstige unerwünschte E-Mails

Durch Phishing versuchen Angreifer nicht nur von Privatpersonen sensible Daten zu erschleichen, sondern auch von Unternehmen.

Wir beschäftigen uns seit vielen Jahren mit den verschiedenen Formen unerwünschter elektronischer Post. Bei echten Werbe-E-Mails, die von verantwortlichen Stellen bewusst an die Empfänger mit gezielter Werbeabsicht versendet worden sind, jedoch vom Betroffenen als lästig, unzulässig oder in einer anderen Weise als störend empfunden werden, können wir den datenschutzrechtlichen Rahmen entsprechend ausschöpfen und durch unser Fachreferat den Beschwerdefall effektiv überprüfen. In diese Kategorie fällt z. B. der klassische Werbe-Newsletter, bei dem durch die Möglichkeit eines eigenen Opt-Outs für Nutzer auch eine einfache Lösung gegen den weiteren Erhalt der Nachrichten besteht. Bei Spam stehen wir dagegen vor der meist unlösbaren Herausforderung, den tatsächlichen Versender ausfindig zu machen oder weiterführende Aufklärungsarbeit zu leisten.

Im Alltag fällt es vielen Privatpersonen sehr schwer zu unterscheiden, ob es sich um eine echte Nachricht handelt oder um Spam-Mails mit gefälschter Absender-Adresse. Spam wird meist als Sammelbegriff für alle unerwünschten elektronischen Nachrichten verwendet. Wir haben im Berichtszeitraum zahlreiche solcher Spam-Nachrichten zugeleitet bekommen mit der Bitte, gegen den Absender vorzugehen. In der Regel verschleiert der Absender seine wahre Identität, so dass auch wir mit verhältnismäßigem Aufwand keine Identitätsfeststellung durchführen können. Meldet uns also ein Betroffener, dass in seinem E-Mail-Postfach eine Spam-Nachricht gelandet ist, jedoch kein Schaden auf Grund nicht erfolgter Interaktion entstanden ist, so können wir ihm nur Tipps im Umgang mit Spam mit auf den Weg geben und ein Löschen der Nachricht empfehlen. Da die Beeinträchtigung im Persönlichkeitsrecht des Einzelnen durch den Erhalt von Spam insgesamt überschaubar ist und es sich gleichzeitig um ein Massenphänomen im Internet handelt, bitten wir Bürgern uns grundsätzlich keine Beschwerden wegen Spam-Nachrichten zukommen zu lassen, da diese in der Regel nicht weiter verfolgt werden können.

Link:
www.bsi-fuer-buerger.de

Handelt es sich dagegen um Phishing-Nachrichten, wird versucht, vom Empfänger ein Passwort oder andere sensible Daten abzufischen. Klassische Angriffe erfolgen hier durch gefälschte Online-Banking-Seiten, Online-Bezahlverfahren und Webshops. So wurden uns bspw. täuschend echte Nachrichten sowie die dazugehörigen nachgebauten Seiten von Amazon, PayPal, eBay und Payback von Beschwerdeführern zugeleitet. Die Namen der echten hinter dem Dienst stehenden Firmen werden dabei gezielt missbräuchlich verwendet, weshalb diese Unternehmen oft im eigenen Interesse Warnungen zu diesem Thema veröffentlichen, damit Nutzer prüfen können, ob es sich jeweils um eine echte oder gefälschte Nachricht handelt. Opfern solcher Betrugs-

versuche raten wir dringend, sich an die örtliche Polizeidienststelle zu wenden und Strafanzeige zu erstatten.

Link:
www.polizei-praevention.de/themen-und-tipps/phishing.html

Im Berichtzeitraum haben wir festgestellt, dass nun auch Unternehmen verstärkt in den Fokus solcher Angriffe geraten. Durch sog. Spear-Phishing-Attacken werden Mitarbeiter einer Organisation gezielt persönlich angegriffen und zunächst versucht, Vertrauen zum potentiellen Opfer aufzubauen, indem vertrauenswürdige Identitäten vorgetäuscht werden (z. B. E-Mail vom Vorgesetzten, Sicherheitsabfrage vom IT-Administrator). Erst nachdem das Opfer sich auf das Täuschungsmanöver eingelassen hat, wird in weiteren Schritten versucht, vertrauliche Daten möglichst unauffällig zu erschleichen. Im Herbst 2016 wurde ein mittelfränkisches Unternehmen Opfer eines solchen Betrugs und verlor nach eigenen Angaben 40 Millionen Euro. In diesem Fall wurde durch gefälschte Dokumente und Identitäten über elektronische Kommunikationswege Geld auf Auslandskonten transferiert. In den Medien wurde ausführlich über den Angriff berichtet und dieser als größter Betrugsvorfall dieser Art – zumindest in der jüngsten Vergangenheit in Deutschland – eingestuft (uns liegen selbst keine Kenntnisse über Vorfälle in vergleichbarer Größenordnung vor).

Wir halten es folglich für sehr wichtig, die Mitarbeiter im Umgang mit elektronischer Kommunikation zu schulen und über aktuelle Betrugsmaschen zu informieren. Social Engineering findet immer größere Verbreitung und ist als Gefahr ähnlich kritisch einzustufen wie Ransomware in gefälschten E-Mails.

22.7 iCloud und Apple Care: Fremde Kontaktdaten auf iPhones

Arbeiten von Apple-Servicemitarbeitern können dazu führen, dass Nutzer plötzlich fremde Kontaktdaten bei eigenen Apple-Geräten vorfinden.

Wir hatten zunächst eine Beschwerde eines einzelnen iPhone-Nutzers erhalten, der uns gegenüber angab, fremde Kontakteinträge unbekannten Ursprungs auf seinem Apple-Gerät vorzufinden. Heikel an der Angelegenheit war, dass es sich zum Teil um vertrauliche Nummern von hochrangigen Politikern handelte. Im Rahmen der Beschwerdebehandlung konnte der Eingabeführer nachweisen, dass mehrere hundert unbekannte Einträge in seinem iPhone vorgehalten wurden.

Wir haben uns der Sache angenommen und nicht nur umfangreichen Rechercheaufwand betrieben, sondern auch versucht, an eigenen Labor-Geräten den Sachverhalt zu rekonstruieren. Ein Fehlverhalten des Nutzers konnte genauso rasch ausgeschlossen werden wie ein Hacking-Vorfall. Während unsere iPhone-Untersuchungen selbst ergebnislos blieben, konnten wir im Internet durch glaubhafte Schilderungen weiterer Nutzer von vergleichbaren Fällen bei iPhones erfahren, so dass wir ein grundsätzliches Problem der Apple iCloud vermuteten. Da wir in der Vergangenheit zum Teil durchaus konstruktive Antworten seitens Apple Deutschland erhalten hatten, haben wir in Rücksprache mit dem Eingabeführer Kontakt zu Apple herstellen wollen, um den konkreten Fall aufzuarbeiten. Weil wir aber nach einem knappen Verweis auf die nicht vorhandene Zuständigkeit keine weiterführende Antwort von Apple erhielten, haben wir den Vorgang schließlich an die irische Datenschutzaufsichtsbehörde weitergegeben, die laut eigener Bewertung für Apple zuständig ist. Die Behörde hat kurze Zeit später im Rahmen ihrer Öffent-

lichkeitsarbeit umfassend über das zugrundliegende Datenschutzproblem (ohne Nennung des Falles) berichtet und bekanntgegeben, Untersuchungen bei Apple diesbezüglich anzustreben. Über den weiteren Verlauf und das Ergebnis einer solchen Untersuchung sind wir leider nicht informiert worden.

Auf Grund dessen, dass sich auch Medien den Vorfällen annahmen, konnte zumindest ausfindig gemacht werden, dass die konkrete Ursache beim Dienst „Apple Care" zu vermuten war. Durch die damit verbundenen Servicearbeiten hatten wohl Apple-Mitarbeiter in der Vergangenheit bereits mehrmals im Rahmen von Support-Bearbeitungen Fehler gemacht und Daten nicht korrekt synchronisiert. Wie wir erfahren haben, können scheinbar bei einer solchen Untersuchung durch Apple-Servicemitarbeiter persönliche Daten aus der iCloud eines Nutzers auf Apple-Testgeräte übertragen und nach der Reparatur wieder auf das Nutzergerät zurückgespielt werden. Durch falsch zurückgespielte iCloud-Daten bei Arbeiten an mehreren iPhones scheint es dann zu einer Vermischung von Kontaktdaten gekommen zu sein.

Der Beschwerdefall zeigt, dass sich bei Datensynchronisierungen von Cloud-Daten nicht nur durch die automatisierte Verarbeitung Fehler ereignen können, sondern auch durch Supportarbeiten einzelner Mitarbeiter. Wenn über ähnlich gelagerte Fälle von Nutzern gehäuft berichtet wird, kann es sich sogar um strukturelle Mängel der Organisation im Umgang mit den personenbezogenen Daten des Nutzers handeln. Die Vertraulichkeit und Integrität der Daten war zumindest im geschilderten Fall nicht mehr gewährleistet.

22.8 Installer-Software mit Tracking-Add-On

Kostenfreie Download-Hilfen haben zum Teil Tracking-Features oder Werbung im Gepäck, um sich durch die Daten der Nutzer zu finanzieren.

Gegenstand einer Datenschutzbeschwerde des vergangenen Berichtszeitraums war die von einem Unternehmen angebotene Installer-Software. Mit dieser App konnten Nutzer auf der viel frequentierten Webseite des Unternehmens zahlreiche kostenfreie Softwareprodukte (Freeware) herunterladen und auf dem eigenen Gerät installieren. Der Beschwerdeführer hat dabei vorgetragen, dass bei Installation und Verwendung des Installers versteckt Webseitenaufrufe im Hintergrund erfolgen würden, bei denen eindeutig personenbezogene Daten des Nutzers übertragen werden. Diese Aufrufe würden nach Einschätzung des Beschwerdeführers offensichtlich für Trackingzwecke genutzt. Da keine Informationen zu dieser Verarbeitung, insbesondere zum Tracking, vorhanden seien, könne sich ein Nutzer weder ausreichend über das Diensteangebot informieren noch widersprechen. Auch sei es einem Nutzer unklar, an wen Daten übertragen werden, da in den Nutzungshinweisen bzw. Datenschutzbestimmungen des Installers lediglich von Drittanbietern gesprochen werden würde. Der Beschwerdeführer hat uns ergänzend einen Link genannt, unter dem eine strukturierte Aufarbeitung des fragwürdigen Verhaltens des Installers zu finden war.

Wir haben uns dem Sachverhalt angenommen und versucht, die Datenübertragungen zunächst selbst nachzuvollziehen. Da auch wir die beschriebene Problematik im Umgang mit den Installer zumindest bei alten Versionen der Software erkannten, haben wir die verantwortliche Stelle kontaktiert. Das Unternehmen gab uns gegenüber zuerst an, dass die Vorwürfe des Beschwerdeführers sich auf alte, nicht mehr

angebotene Produktversionen beziehen und in der aktuellen Version des Installers keine versteckten Aufrufe mehr stattfinden. Das Unternehmen hat darauf hingewiesen, dass es sich bei dem angebotenen Installer-Produkt um eine freiwillige, kostenfreie Download-Hilfe handelt, welche dem Nutzer das Herunterladen, Entpacken und Installieren von Drittsoftware erleichtern soll, aber nicht zwangsläufig genutzt werden muss. Im Rahmen des Ausführungsprozesses würde der Nutzer sowohl über die Allgemeinen Geschäftsbedingungen als auch über die Datenschutzerklärung informiert. Das Unternehmen gab explizit an, dass keine personenbezogenen Daten des Nutzers über die genannten Zwecke hinaus verarbeitet oder an Dritte weitergegeben würden.

Der Installer ist aus unserer Sicht in der Tat als Download-Hilfe anzusehen, die den Nutzer bei dem Herunterladen und der Installation von Drittanbietersoftware zwar unterstützt, jedoch nicht verpflichtend genutzt werden muss. Ein Nutzer kann, wenn er ein Softwareprodukt bei der verantwortlichen Stelle herunterladen möchte, auch den Weg einer manuellen Installation wählen, so dass der Installer nicht zwangsläufig in Anspruch genommen werden muss. Der Installer wird unserer Kenntnis nach zudem nur bei vergleichsweise wenigen ausgewählten Download-Angeboten zur Verfügung gestellt, bei denen dann aber die genannte Wahlmöglichkeit geboten ist. Auch ist darauf hinzuweisen, dass es jedem Nutzer freigestellt ist, ob er von der Webseite des Unternehmens Softwareprodukte (kostenlos) herunterlädt oder nicht. Nichtsdestoweniger muss für einen Nutzer transparent sein und bleiben, welche Datenverarbeitungsvorgänge hinsichtlich seiner personenbezogenen Daten bei Nutzung des Installers stattfinden. Ob und in welcher Form in der Vergangenheit hierzu ein datenschutzrechtliches Defizit bestand, lässt sich nachträglich kaum oder nur mit einem nicht gerechtfertigten Aufwand feststellen. Zum Zeitpunkt der Beschwerdeuntersuchung konnten wir feststellen, dass eine eigene FAQ-Seite zum Installer vom Unternehmen eingerichtet wurde, die viele der aufgeworfenen Fragestellungen beantwortet und dadurch die Nutzer unserem Empfinden nach umfangreich über die Rahmenbedingungen der Nutzung des Installers informiert.

Die vorgetragene Beschwerde hat gezeigt, dass gerade kostenfreie Installer-Apps eine gewisse Datenschutzbrisanz auslösen können. Selbstverständlich können diese Dienste wie üblich zu ihrer eigenen Finanzierung Daten der Nutzer erheben, wenn sich dies im zulässigen Rahmen abspielt. Findet jedoch im Hintergrund eine Datenverarbeitung statt, von der der Nutzer letztendlich nichts weiß, so ist die Verarbeitung als unzulässig einzustufen. Derzeit haben wir keine Hinweise, dass durch die Verwendung der aktuellen Installer-Version aus dem Beschwerdefall personenbezogene Daten der Nutzer unrechtmäßig zu Tracking- oder Werbezwecken verarbeitet werden. Bei solchen Einschätzungen im technischen Umfeld handelt es sich jedoch immer nur um Momentaufnahmen, da die Releasezyklen im App-Umfeld sehr kurz sind und die Releases sich in ihrem Datenverarbeitungsverhalten wesentlich voneinander unterscheiden können.

Ausblick zur DS-GVO:

Die DS-GVO legt großen Wert darauf, dass auch im Internet Nutzer transparent und verständlich über Datenverarbeitungen unterrichtet werden. Somit werden wir weiterhin im Rahmen unserer personellen Möglichkeiten die Transparenz solcher angebotenen Dienste untersuchen und uns davon überzeugen, dass die Datenverarbeitungsvorgänge entsprechend den gesetzlichen Vorgaben erfolgen.

22.9 RFID-Einsatz in Textilreinigungen

Textilreinigungen können sog. RFID-Etiketten in Kleidungsstücken einsetzen, wenn die Etiketten nur im Nahfeldbereich auslesbar sind, das Angebot freiwillig gestaltet wird und die Kunden ausreichend über die Verwendung informiert werden.

Der vergangene Berichtzeitraum hat uns gezeigt, dass die Verwendung der RFID-Technik durchaus vielseitige Einsatzszenarien hervorbringt. Während wir bereits bei Verfahren der Zutrittskontrolle (z. B. Zimmerkarte in Hotels) und des bargeldlosen Zahlens (u. a. Geldkarten, Smartphones) damit konfrontiert wurden, haben wir im Berichtszeitraum zum ersten Mal eine Beschwerde zur Anwendung von RFID in Reinigungen erhalten. Konkret wurde uns vorgetragen, dass in einer Textilreinigung die Verpflichtung bestehe, RFID-Knöpfe in die eigenen Hemden einnähen lassen zu müssen. Zudem würden bei der Reinigung am Terminal zahlreiche personenbezogene Daten der Kunden abgefragt, ansonsten hätte man einen höheren Preis zu bezahlen.

Da wir bislang keinerlei datenschutzrechtliche Erfahrung zum Ablauf einer solchen Datenverarbeitung in Reinigungen hatten, haben wir der verantwortlichen Stelle eine Vielzahl an Fragen gestellt, damit uns eine Einschätzung des Sachverhalts ermöglicht wurde. So fragten wir einerseits, welche persönlichen Daten der Kunden abgefragt und elektronisch erfasst werden, zu welchem Zweck diese Daten der Kunden erhoben werden, inwieweit die Kunden darüber informiert werden, dass es sich um einen freiwilligen Vorgang handelt und ob man auch auf die Preisgabe der eigenen persönlichen Daten verzichten kann. Anderseits wollten wir auch mehr über die eingesetzten RFID-Etiketten (RFID Laundry Tags) erfahren, so dass wir uns erkundigten, welche RFID-Etiketten in Kleidungsstücke eingenäht werden. Erläutern musste uns die verantwortliche Stelle hierbei sowohl den Ablauf des Einnähens als auch die technischen Hintergründe sowie Details darüber, welche Daten auf einem solchen Etikett gespeichert werden. Ebenso von Interesse waren für uns die Punkte, inwieweit eine Verknüpfung mit dem bereits gespeicherten Profil eines Kunden erfolgt und ob die Kunden einerseits gefragt werden, ob sie mit dem Einnähen des Knopfes einverstanden sind - und diesen andererseits ggf. auch wieder entfernen lassen können.

Uns wurde vom Unternehmen mitgeteilt, dass tatsächlich RFID-Knöpfe in Hemden eingenäht werden, um eine Identifikation der Textilien und somit eine Zuordnung zum Besitzer innerhalb der Reinigung zu ermöglichen. Dies sei auf Grund der Vielzahl an Kundenaufträgen für eine effiziente Auftragssteuerung erforderlich. Es wurde uns signalisiert, dass die Eingabe personenbezogener Daten am Kundenterminal (PC) auf rein freiwilliger Basis stattfinden würde und eine alternative anonyme Nutzung der Reinigung nach wie vor möglich sei. Des Weiteren wurde uns geschildert, dass lediglich RFID-Chips verwendet werden, die nur in unmittelbarer Nähe ein Auslesen der Trägerinformation (ID) ermöglichen würde. Hierzu haben wir das technische Beiblatt der RFID-Chips erhalten, aus dem hervorgeht, dass der Lesebereich auf maximal 3 cm beschränkt ist. Zudem wurde angegeben, dass Kunden transparent und verständlich über den Einsatz der RFID-Knöpfe informiert werden und ein Annähen grundsätzlich nur mit der Zustimmung der Kunden stattfindet, wodurch eine Freiwilligkeit gegeben sei. Da uns glaubhaft versichert wurde, die elektronischen Etiketten ausschließlich für den angegebenen Zweck einzusetzen und keine Bewegungsprofile der Kunden zur Nachverfolgung angestrebt werden, sahen wir in dem praktizierten Verfahren keinen datenschutzrechtlichen Verstoß und somit keine Notwendigkeit, dass die Textilreinigung das bislang praktizierte Verfahren ändern müsste.

22.10 Offline-Tracking

Unternehmen setzen verstärkt auf Offline-Tracking-Techniken, um das Lauf- und Kaufverhalten von Kunden anhand deren Smartphones gezielt zu überwachen und auf Grund kommerzieller Interessen systematisch auszuwerten.

Im vergangenen Tätigkeitsbericht haben wir im Kapitel 22.10 darüber berichtet, dass Besucherstrommessungen mittlerweile über die eigenen Smartphones der Kunden erfolgen. Dieser Trend hat in den letzten zwei Jahren weiter zugenommen. Uns haben nicht nur Unternehmen, die entweder Produkte für solche Trackingzwecke einsetzen wollten oder damit beworben wurden, um Rat gebeten, sondern auch Hersteller von Hard- und Software, die künftig einen großen Markt vor sich sehen, um Einschätzung bzw. Genehmigung gebeten.

Da sich das Thema Offline-Tracking nicht regional auf Bayern beschränkt, haben wir angeregt, eine Arbeitsgruppe hierfür zu gründen und mit den anderen Aufsichtsbehörden zu einheitlichen Bewertungen und schließlich einem daraus resultierenden einheitlichen Vollzug zukommen. Als Unterarbeitsgruppe (UAG) des Arbeitskreises Medien hat sich die UAG Offline Tracking zweimal im Berichtszeitraum getroffen, um die bislang bekannten Einsatzszenarien zu diskutieren. Im Ergebnis kann hierbei festgehalten werden, dass die unterschiedlichsten Techniken und Anwendungsmöglichkeiten existieren, wodurch eine pauschale Aussage zur datenschutzrechtlichen Zulässigkeit von Offline-Tracking unmöglich wird. Die einzelnen Ergebnisse der UAG sollen auf unserer Webseite veröffentlicht werden.

Wir haben bislang Verfahren kennengelernt, die neben dem WLAN-Signal der Smartphones auch auf Bluetooth und das Mobilfunksignal zurückgreifen. Gemeinsames Ziel ist dabei, den Standort des Smartphones (und damit des Nutzers) möglichst exakt in geringen Zeitintervallen zu erkennen, um so schließlich ein Bewegungs- und Aktivitätsprofil jedes Nutzers zu erstellen. Auch eine Ortung über sog. Sound Beacons wurde uns bekannt, bei dem auf das Mikrofon der Mobilgeräte zurückgegriffen wird. Eine datenschutzrechtliche Bewertung dieser Verfahren ist sehr schwierig, da eine Vielzahl an Faktoren zu berücksichtigen ist. Es stellen sich verschiedene Fragen, wie z. B. wer konkret überwacht wird und darüber informiert wurde (u. a. ist zu unterscheiden zwischen Kunden, Passanten, Betriebsrat, Beschäftigte), wie lange eine Speicherung der erhobenen Daten stattfindet, ob die erhobenen Daten direkt verarbeitet und evtl. anonymisiert werden, ob ein filialübergreifendes Tracking praktiziert wird (Re-Identifizierung von Nutzern), ob der Nutzer hierbei aktiv einwilligt (z. B. mittels App) oder heimlich ohne dessen Wissen überwacht wird.

Wie im Kapitel 3.10 dargelegt, wollten wir prüfen, welche Unternehmen in Bayern solche Verfahren einsetzen, um dann deren Zulässigkeit im Konkreten zu prüfen. Leider haben in der Prüfung alle angeschriebenen verantwortlichen Stellen den Einsatz verneint. Allerdings wurden wir bspw. im Rahmen einer Beschwerde darüber informiert, dass eine Einzelhandelsfiliale im Eingangsbereich ein Hinweisschild über Smartphone-Tracking angebracht hat. Wir haben in einer am Tag darauf stattfindenden spontanen Vor-Ort-Kontrolle geprüft, welches Verfahren dort praktiziert wird und konnten in der Tat den Einsatz eines Offline-Tracking-Verfahrens mittels WiFi feststellen. Es handelte sich allerdings um einen eingeschränkten Testbetrieb einer einzelnen Filiale einer großen Modehauskette, die zunächst prüfen wollte, wie wirtschaftlich der Betrieb und wie gut die daraus gewonnenen Erkenntnisse seien. Nachdem wir das Gespräch mit den Verantwortlichen gesucht hatten, wurde der Betrieb seitens des Unternehmens eingestellt – eine weitergehende technische und rechtliche Aufarbeitung war dann für uns nicht mehr möglich.

22.11 Windows 10

Der Einsatz von Windows 10 verursacht gravierende datenschutzrechtliche Probleme in Unternehmen, die bislang nicht gelöst werden konnten. Der größte Kritikpunkt besteht in der automatisierten Übermittlung von Nutzerdaten ohne ausreichende Transparenz und Deaktivierungsmöglichkeit.

Seit dem Erscheinen von Windows 10 als neues Microsoft-Betriebssystem haben wir zahlreiche Anfragen zu dessen Zulässigkeit in bayerischen Unternehmen erhalten. Es ist unstrittig, dass es sich bei der datenschutzrechtlichen Bewertung eines Betriebssystems um eine komplexe und aufwendige Angelegenheit handelt, schon alleine weil unterschiedliche Versionen und Einsatzszenarien existieren. Aus diesem Grund haben wir versucht, in Abstimmung mit weiteren Aufsichtsbehörden (auch anderer EU-Länder) Windows 10 näher zu begutachten. Der Prozess dieser Untersuchung wurde bereits 2015 gestartet und war zum Zeitpunkt des Redaktionsschlusses dieses Berichts zwar nicht abgeschlossen, aber weit fortgeschritten.

Im Rahmen von Beschwerden gaben uns gegenüber viele Nutzer bereits wenige Tage nach der Einführung von Windows 10 an, sich über die datenschutzunfreundlichen Voreinstellungen (vorallem im Rahmen der Express-Installation) des Betriebssystem zu ärgern. Das System sei so eingestellt, dass möglichst viele Daten vom Nutzer an Microsoft übertragen werden. Des Weiteren wurde kritisiert, dass ein Abschalten der Übertragung von Diagnose- und Nutzungsdaten zumindest in der Home- und Pro-Version nicht möglich ist. Und ebenso „untragbar" fanden es einige Nutzer, dass Updates nicht deaktiviert, sondern nur noch herausgezögert werden konnten. So kam es in uns bekannten Fällen während des normalen Arbeitens urplötzlich zu mehrstündigen Updates.

Verschiedene IT-Fachzeitschriften und Sicherheitsexperten hatten frühzeitig ihre eigenen Ergebnisse bei der Untersuchung der Datenströme beim Einsatz von Windows 10 veröffentlicht und uns dadurch indirekt die Möglichkeit gegeben, die datenschutzrechtlichen Problemfälle zu sammeln und zu kategorisieren. So steht bislang im Raum, dass durch den Einsatz von Windows 10 regelmäßig Telemetrie-Daten, Cortana-Abfragen und aufgerufene URLs in die dazugehörige Microsoft-Cloud übertragen werden. Darunter befinden sich eine Vielzahl personenbezogener Daten, so dass eine Reihe an kritischen Datenschutzfragen entsteht. Setzt ein Unternehmen Windows 10 ein, müsste bspw. geprüft werden, ob die Datenübermittlung in das entsprechende Land, z. B. die USA, rechtlich zulässig ist, ob hierbei durch Microsoft womöglich die Voraussetzung einer Auftrags(daten)verarbeitung vorliegt, inwieweit der Beschäftigtendatenschutz tangiert wird, ob Betriebsgeheimnisse ausreichend geschützt sind und ob neben dem Datenschutz allgemein auch die IT-Sicherheit im Unternehmen gewährleistet werden kann.

Wir sind mittlerweile bei unserer Untersuchung dank hilfreicher Ergänzungen aus anderen EU-Ländern weiter vorangekommen. Ziel ist es nun zeitnah die neu gewonnenen Erkenntnisse Microsoft vorzulegen und um Stellungnahme zu bitten. Microsoft war bislang bemüht, die eigenen Verarbeitungsprozesse gegenüber den Aufsichtsbehörden transparent offen zu legen. Nun haben bereits mehrere Aufsichtsbehörden umfassende Nachfragen gestellt, die Microsoft als nächsten Schritt behandeln und beantworten muss. Danach wird sich zeigen, inwieweit eine Anpassung hinsichtlich der festgestellten Mängel erfolgt. Wir hoffen zeitnah über den Ausgang dieser Prüfung öffentlich Aussagen tätigen zu können, damit für verantwortliche Stellen klar wird, unter welchen Rahmenbedingungen Windows 10 aus datenschutzrechtlichen Gesichtspunkten eingesetzt werden darf.

23

Bußgeldverfahren

23 Bußgeldverfahren

Bußgeldverfahren bleiben nach wie vor ein Schwerpunkt unserer Tätigkeit. Gegenüber dem vorherigen Berichtszeitraum ist die Zahl der von uns bearbeiteten Bußgeldvorgänge noch einmal deutlich von 117 auf 173, d. h. fast 50%, angestiegen.

Wir haben im Berichtszeitraum 2015/2016 insgesamt 173 Bußgeldvorgänge bearbeitet. Dabei haben wir entweder einen Bußgeldbescheid erlassen, eine Verwarnung ausgesprochen oder das Verfahren eingestellt.

In 52 Fällen wurden von uns Geldbußen festgesetzt, von denen 37 im Berichtszeitraum ohne Einspruch rechtskräftig wurden. Bei den übrigen Fällen wurde Einspruch gegen den Bußgeldbescheid eingelegt. In vielen dieser Verfahren kam es jedoch nicht zu einer Einstellung, sondern zu einer Reduzierung der Bußgeldhöhe. In einem anderen Fall haben wir eine Verwarnung mit Verwarnungsgeld ausgesprochen. Bei den übrigen Vorgängen, bei denen ein Bußgeld im Raum stand, haben wir entweder kein förmliches Bußgeldverfahren eingeleitet oder das Verfahren nach Einleitung eingestellt.

Von den festgesetzten 52 Geldbußen waren 34 im dreistelligen Bereich, d. h. bis maximal 999 Euro. Im vierstelligen Bereich haben wir in den letzten zwei Jahren 13 Bußgelder festgelegt, im fünfstelligen Bereich insgesamt 5.

Wie schon in den vorangegangenen Berichtszeiträumen finden sich unter den Geldbußen sowohl solche, die gegen die „verantwortliche Stellen" im datenschutzrechtlichen Sinne (§ 3 Abs. 7 BDSG), etwa gegen Unternehmen, festgesetzt wurden, als auch solche gegen Mitarbeiter von verantwortlichen Stellen. Unter den Geldbußen gegen verantwortliche Stellen sind jedoch auch solche dabei, bei denen die verantwortliche Stelle eine natürliche Person ist, etwa ein Einzelunternehmer.

Weitere Fälle von Geldbußen gegen natürliche Personen betrafen etwa Geldbußen gegen Fahrzeughalter, die unter Einsatz so genannter Dashcams (Dashboard Cameras), die sie in ihren Fahrzeugen angebracht haben, anlasslos den Straßenverkehr filmten und dabei unbefugt personenbezogene Daten erhoben und verarbeiteten. In diesem Fall ist der Fahrzeughalter, der die Kamera zum Einsatz bringt, „verantwortliche Stelle" im datenschutzrechtlichen Sinne (siehe auch 19.6).

Gegen verantwortliche Stellen, die juristische Personen oder Personenvereinigungen sind (etwa GmbH, OHG, e.V.), ist die Festsetzung von Geldbußen gesetzlich gemäß § 30 OWiG nur möglich, wenn der Verstoß durch ein vertretungsberechtigtes Organ oder ein Mitglied eines solchen Organs oder durch eine andere Person begangen wurde, die eine Leitungsfunktion innerhalb der betreffenden juristischen Person bzw. Personenvereinigung wahrnimmt. Hingegen ist aus Anlass datenschutzrechtlicher Verstöße durch Mitarbeiter, die keine Leitungsfunktion innehaben, eine Ahndung des hinter dem Mitarbeiter stehenden Unternehmens mit Geldbuße nur möglich, wenn einer Person mit Leitungsfunktion zumindest ein Verstoß gegen die in § 130 Abs. 1 OWiG geregelte betriebliche Aufsichtspflicht zur Last zu legen ist. Voraussetzung für die Festsetzung einer Geldbuße gegen die Leitungsperson und/oder das Unternehmen selbst ist somit in diesen Fällen der Nachweis eines Verstoßes gegen die betriebliche Aufsichtspflicht durch eine Leitungsperson des Unternehmens. Zur betrieblichen Aufsichtspflicht gehört u. a. auch die Ergreifung derjenigen organisatorischen Maßnahmen im Unternehmen, die erforderlich sind, um im Rahmen der Tätigkeit des Unternehmens Verstöße gegen datenschutzrechtliche Vorschriften zu vermei-

den. Soweit wir im Rahmen unserer Ermittlungen Anhaltspunkte für derartige organisatorische Mängel innerhalb eines Unternehmens gewinnen, ist daher regelmäßig eine weitere Aufklärung erforderlich, um abschließend bewerten zu können, ob die unternehmerischen und betrieblichen Abläufe mangelhaft organisiert waren. Sofern ein organisatorischer Mangel bei der Tätigkeit des Unternehmens zu einem Verstoß – etwa seitens eines Mitarbeiters – gegen eine bußgeldbewehrte datenschutzrechtliche Vorschrift geführt hat, der verhindert oder zumindest wesentlich erschwert worden wäre, wenn die erforderlichen organisatorischen Vorkehrungen getroffen worden wären, ist nach § 130 Abs. 1 OWiG die Festsetzung einer Geldbuße wegen Aufsichtspflichtverstoßes möglich. Von dieser Möglichkeit haben wir in geeigneten Fällen Gebrauch gemacht.

Die im Berichtszeitraum verhängten Geldbußen betrafen Sachverhalte, die wie folgt skizziert werden können:

- anlassloses Filmen im Straßenverkehr mit Hilfe von Dashboard Cameras aus Fahrzeugen heraus (mehrere Fälle);
- unzulässige Übermittlung der IP-Adressen von Webseitennutzern durch den Einsatz von Tracking-Tools;
- Verwendung einer E-Mail-Adresse für werbliche Zwecke trotz Werbewiderspruchs (mehrfach);
- fehlender Hinweis auf das Werbewiderspruchsrecht;
- Versendung einer E-Mail mit offenem E-Mail-Verteiler (mehrfach);
- nicht rechtzeitige Auskunft nach § 34 BDSG an einen Betroffenen (mehrfach);
- unrichtige Auskunft nach § 38 Abs. 3 BDSG an die Datenschutzaufsichtsbehörde (mehrfach);
- unzulässige Beschaffung von Patientendaten für nichtdienstliche Zwecke durch Mitarbeiterin einer Arztpraxis bei einer anderen Arztpraxis;
- Aushang von Krankheitslisten von Mitarbeitern am „Schwarzen Brett";
- Einsatz von Auftragsdatenverarbeitungsverträgen, die nicht den Anforderungen gem. § 11 Abs. 2 Satz 2 BDSG entsprachen;
- wiederholte Faxversendung an unrichtigen Empfänger durch eine Arztpraxis;
- Verkauf/Ankauf (Übermittlung) von Kundendaten (auch Nicht-Listendaten) im Zuge eines Asset Deal ohne vorherige Einräumung einer Widerspruchsmöglichkeit für die Kunden;
- Zusendung eines Faxbriefs mit ärztlichem Befundbericht durch Klinik an eine zentrale Faxeinlaufstelle einer Behörde statt an die Beihilfestelle;
- Mitteilung des Kontostands durch Bankmitarbeiter an einen Unbefugten;
- zweckändernde Nutzung von Anleger-Adressdaten für anwaltliche Werbung;
- Zusendung eines anwaltlichen Schreibens mit personenbezogenen Daten an eine „vermutete" anwaltliche Vertreterin;
- unberechtigte Einholung einer Bonitätsauskunft für private Zwecke;
- Mitteilung offener Forderungen durch eine Kfz-Werkstatt an die Mutter der Lebensgefährtin des Kunden;
- Übermittlung einer ärztlichen Diagnose durch Arzt an die Mutter des Patienten ohne Einwilligung;
- Bestellung eines Datenschutzbeauftragten, der einer Interessenkollision unterliegt;
- Übermittlung von Bestands- und Nutzungsdaten von Nutzern eines Telemediendienstes an einen anderen Te-

lemediendienst ohne Einwilligung der Nutzer.

Aus dieser Übersicht wird deutlich, dass die Ahndungen mit Geldbuße eine breite Palette von Verstößen aus den unterschiedlichsten Lebenssachverhalten betrafen. Dennoch seien nachfolgend einige Fallgruppen hervorgehoben, die uns entweder in zahlenmäßiger Hinsicht in besonderer Weise beschäftigt haben oder aufgrund der Besonderheiten des Sachverhalts von Interesse sind.

Besonders erwähnt werden sollen zwei Bußgeldbescheide, die wir im Zusammenhang mit einer Übermittlung von Kundendaten im Zuge einer Geschäftsveräußerung in der Form eines sog. Asset Deal erlassen haben. Hier hatte der Betreiber eines Online-Shops seinen Shop an ein anderes Unternehmen derselben Branche veräußert und hierbei auch die Daten der Kunden übermittelt, darunter die E-Mail-Adressen und die Kaufhistorie. Die Kunden waren vorher über den geplanten Verkauf nicht informiert worden (Näheres vgl. unter Kapitel 13.1). Dieser Fall steht nach unserer Beobachtung recht exemplarisch für eine regelrechte Fallgruppe, die in der Praxis häufig anzutreffen ist. Wir vertreten nach wie vor die Auffassung, dass Kundendaten – jedenfalls soweit sie über die in § 28 Abs. 3 Satz 2 BDSG genannten sog. Listendaten hinausgehen – auch im Zuge einer Geschäftsveräußerung nicht an einen anderen Rechtsträger übergeben werden dürfen, ohne den Kunden vorher zumindest eine Widerspruchsmöglichkeit gegen die Übermittlung ihrer Daten einzuräumen. Inzwischen zeigt sich aber, dass unsere – auch über die Presse wiederholt kommunizierte – Rechtsauffassung in der Praxis bekannter geworden ist. Dafür spricht, dass wir im Berichtszeitraum zahlreiche Beratungsanfragen von Unternehmen und Insolvenzverwaltern erhalten haben, die eine Veräußerung von Kundendaten im Zuge von Asset Deals planten und denen unsere Presseinformationen zu diesem Thema zur Kenntnis gelangt waren. Wir werden unsere Bemühungen um Information zu dieser wichtigen Fallgruppe fortsetzen.

Des Weiteren verdient eine Geldbuße Erwähnung, die wir gegen ein Unternehmen festgesetzt haben, das mehrere Dienstleister als Auftragsdatenverarbeiter engagiert hatte, hierbei jedoch die im Gesetz geregelten inhaltlichen Anforderungen an einen schriftlichen Auftrag zur Auftragsdatenverarbeitung nicht erfüllt hat. Insbesondere fehlten den schriftlichen Aufträgen detaillierte, spezifische und auf den konkreten Auftragsdatenverarbeiter bezogene Festlegungen zu den technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten gemäß § 9 BDSG und der Anlage zu § 9 BDSG, obwohl solche Regelungen gemäß § 11 Abs. 2 Satz 2 Nr. 3 BDSG im schriftlichen Auftrag zwingend zu treffen sind. Die von dem Unternehmen abgeschlossenen schriftlichen Aufträge beschränkten sich jedoch bei der Beschreibung der technisch-organisatorischen Maßnahmen auf die formelhafte Wiederholung des Gesetzeswortlauts aus der Anlage zu § 9 BDSG, wonach der Auftragnehmer bspw. Maßnahmen treffen müsse, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren etc.. Derartige Wiederholungen des Gesetzeswortlauts ohne Darstellung der gerade beim jeweiligen Auftragnehmer getroffenen spezifischen Maßnahmen zur Erfüllung der einzelnen Anforderungen der Anlage zu § 9 BDSG sind unzureichend. Regelungen zur Auftragsdatenverarbeitung, die die Anforderungen des § 11 Abs. 2 Satz 2 BDSG nicht umfassend erfüllen, stellen eine Ordnungswidrigkeit nach § 43 Abs. 1 Nr. 2b BDSG dar. Weil wir in unserer Prüfungstätigkeit immer wieder feststellen, dass die Regelungen zu den beim Auftragnehmer zu treffenden technischen und organisatorischen Maßnahmen in den schriftlichen Aufträgen zur Auftragsdatenverarbeitung zum Teil zu wenig konkret bzw. zu unspezifisch sind, haben wir es für wichtig angesehen, in diesem – schon aufgrund der großen Anzahl der betroffenen Auftragsdatenverarbeitungsverhältnisse – beson-

ders exponierten Fall wegen dieses Missstands gegen den verantwortlichen Auftraggeber eine Geldbuße auszusprechen (siehe auch 5.5.).

Wie schon in den vorangegangenen Berichtszeiträumen erreichte uns eine große Anzahl von Bußgeldvorgängen im Wege von Abgaben durch die Staatsanwaltschaften gemäß § 43 OWiG an unser Haus als Bußgeldbehörde. Die Zahl derartiger Abgaben ist im Berichtszeitraum gegenüber den vorangegangenen Zeiträumen noch einmal deutlich angestiegen. Die Staatsanwaltschaften nehmen inzwischen augenscheinlich mehr und mehr datenschutzrechtliche Sachverhalte in den Blick und übergeben bei Anhaltspunkten auf einen datenschutzrechtlichen Verstoß die Vorgänge an die für die Ahndung datenschutzrechtlicher Ordnungswidrigkeiten zuständigen Bußgeldbehörden.

Von den 52 Bußgeldbescheiden haben wir zwei zurückgenommen, nachdem die Betroffenen im Rahmen eines Einspruchs neuen Sachvortrag vorgenommen haben. In fünf Fällen wurden Bußgeldbescheide durch die Amtsgerichte aufgehoben, wobei in drei dieser Fälle unsere Rechtsauffassung dem Grunde nach gerichtlich bestätigt wurde, die Gerichte jedoch die Ahndungswürdigkeit anders bewerteten als wir dies taten. Insgesamt haben wir die Beobachtung gemacht, dass Amtsgerichte datenschutzrechtliche Ordnungswidrigkeitenvorgänge bisweilen noch als recht „exotische" Sachverhalte betrachten und möglicherweise daher gelegentlich dazu tendierten, die Schwere von Verstößen niedriger einzuschätzen als wir es getan haben. In diesem Zusammenhang sehen wir es als geradezu eine Aufgabe der für die Verfolgung und Ahndung datenschutzrechtlicher Ordnungswidrigkeiten zuständigen Bußgeldbehörden an, datenschutzrechtliche Verstöße konsequent mit Geldbuße zu ahnden, um auf diese Weise auch die praktischen Erfahrungen der Amtsgerichte mit datenschutzrechtlichen Sachverhalten zu intensivieren und den Gerichten so mehr Erfahrungshintergrund zur Einordnung um zum Verständnis datenschutzrechtlicher Vorgänge und Verstöße zu verschaffen.

Stichwortverzeichnis

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27
91522 Ansbach

Telefon: 0981 53 1300
Telefax: 0981 53 98 1300
E-Mail: poststelle@lda.bayern.de
Web: www.lda.bayern.de