Berliner Beauftragte für
Datenschutz und Informationsfreiheit

Datenschutz und Informationsfreiheit

Bericht 2015

be Berlin

BERICHT

der Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2015

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat dem Abgeordnetenhaus und dem Senat jährlich einen Bericht über das Ergebnis ihrer Tätigkeit vorzulegen (§§ 29 Berliner Datenschutzgesetz, 18 Abs. 3 Berliner Informationsfreiheitsgesetz). Der vorliegende Bericht schließt an den am **25. März 2015** vorgelegten Jahresbericht 2014 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 2015 ab.

Wiederum werden die über Berlin hinaus bedeutsamen Dokumente in einem gesonderten Band („Dokumente 2015“) veröffentlicht.

Dieser Jahresbericht ist über das Internet (http://www.datenschutz-berlin.de/) abrufbar.

Impressum

Herausgeberin:	Berliner Beauftragte für Datenschutz und Informationsfreiheit Friedrichstr. 219, 10969 Berlin Telefon: (030) +138 89-0 Telefax: (030) 215 50 50 E-Mail: mailbox@datenschutz-berlin.de Internet: http://www.datenschutz-berlin.de/
Disclaimer:	Bei den im Text enthaltenen Verweisen auf Internet-Seiten (Links) handelt es sich stets um „lebende“ (dynamische) Verweisungen. Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat vor Drucklegung zwar den fremden Inhalt daraufhin überprüft, ob durch ihn eine mögliche zivilrechtliche oder strafrechtliche Verantwortlichkeit ausgelöst wird. Für spätere Veränderungen dieses fremden Inhalts ist er jedoch nicht verantwortlich.
Satz:	LayoutManufaktur.com
Druck:	Brandenburgische Universitäts- und Verlagsgesellschaft mbH

Inhalt

Einleitung

2015 war ein Jahr der extremen Gegensätze für den Datenschutz wie für die Informationsfreiheit. Nach den Terroranschlägen im Januar in Paris entbrannte auch in Deutschland eine Diskussion darüber, ob die bestehenden Gesetze zur Bekämpfung des Terrorismus ausreichen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sah sich genötigt, wie schon nach dem 11. September 2001 erneut darauf hinzuweisen, dass es in unserem Land „zu keiner Verschiebung zugunsten staatlicher Überwachung und zulasten freier und unbeobachteter Aktionen, Bewegung und Kommunikation der Bürgerinnen und Bürger kommen" darf.[1] Die Datenschutzbeauftragten haben unterstrichen, dass die Terroristen eines ihrer Ziele erreicht hätten, wenn jeder Eingriff in die informationelle Selbstbestimmung zugelassen würde.

Trotz des Hinweises der Datenschutzbeauftragten auf die Ungeeignetheit der Vorratsdatenspeicherung und ohne ausreichende Berücksichtigung der Feststellungen des Europäischen Gerichtshofs in seinem Urteil vom 8. April 2014 ist auf Bundesebene ein Gesetz zur Wiedereinführung der Vorratsdatenspeicherung verabschiedet worden. Ob dieses Gesetz, gegen das mehrere Verfassungsbeschwerden erhoben worden sind, vor dem Bundesverfassungsgericht und dem Europäischen Gerichtshof Bestand haben wird, ist mehr als fraglich. Nach den neuerlichen Terroranschlägen in Paris im November zeichnet sich ab, dass auch die pauschale Verarbeitung der Daten von Flugpassagieren, die in die Europäische Union kommen oder sie verlassen, Gesetz werden wird, obwohl auch die Geeignetheit und Verhältnismäßigkeit dieser Maßnahme nicht belegt sind.

Ein positiver Durchbruch ist demgegenüber bei der Schaffung eines neuen europäischen Rechtsrahmens für den Datenschutz gelungen.[2] Sowohl über die Datenschutz-Grundverordnung als auch über die Richtlinie zum Datenschutz in den Bereichen Justiz und Inneres wurde politisch eine Einigung erzielt, auch

1 Entschließung vom 18./19. März 2015: Datenschutz nach „Charlie Hebdo": Rechtsstaat und Grundrechte beweisen sich gerade in Zeiten terroristischer Bedrohung!, Dokumentenband 2015, S. 10

2 Siehe 2.1

wenn die formelle Annahme durch den europäischen Gesetzgeber bei Redaktionsschluss noch ausstand. Die künftige Verordnung kann als Grundgesetz für den Datenschutz in Europa angesehen werden, das sowohl für den privaten als auch für den öffentlichen Bereich gelten und in weiten Teilen an die Stelle des Datenschutzrechts in Deutschland treten wird. Volle Wirksamkeit wird die Grundverordnung erst Mitte 2018 entfalten. Bis dahin muss im Detail geprüft werden, welche Anpassungen im Bundesrecht und im Berliner Landesrecht erforderlich sind. Die Datenschutzaufsicht und die ihr zur Verfügung stehenden Durchsetzungsmittel werden durch die Datenschutz-Grundverordnung wesentlich gestärkt. Die gleichzeitig beschlossene Richtlinie zum Datenschutz in den Bereichen Justiz und Inneres lässt den Gesetzgebern in Deutschland mehr Gestaltungsspielraum, den sie allerdings nicht zu einer Absenkung des Datenschutzniveaus nutzen sollten. Ziel der 2012 eingeleiteten Europäischen Datenschutzreform war es stets, zu einer möglichst weitgehenden Harmonisierung der Datenschutzbestimmungen in Europa auf hohem Niveau zu kommen.

Auch der Europäische Gerichtshof hat im zurückliegenden Jahr in mehreren Urteilen bekräftigt, dass er sich als „Grundrechtsgericht" versteht und insbesondere dem Datenschutz einen hohen Stellenwert beimisst. Vor allem sein Urteil vom 6. Oktober zum sog. Safe Harbor-Abkommen[3] wird weitreichende Auswirkungen auf den Datenschutz beim Export von Daten europäischer Bürgerinnen und Bürger nicht nur in die USA, sondern in alle außereuropäischen Staaten haben. Der Gerichtshof hat den Grundsatz unterstrichen, dass wesentliche Elemente des europäischen Datenschutzes die Daten bei ihrer Weitergabe in Drittländer begleiten müssen. Zwar muss der Datenschutz im Zielland nicht identisch mit dem europäischen Recht sein, es muss dort aber ein im Wesentlichen gleichwertiges Datenschutzniveau herrschen. Wo dies nicht der Fall ist, können die Daten nur ausnahmsweise und unter eingeschränkten Voraussetzungen exportiert werden. Die deutschen und europäischen Datenschutzbehörden sind nun in der Pflicht, diese Grundsätze in die Praxis umzusetzen. Ob die gerade gefundene politische Verständigung zwischen der Europäischen Union und den Vereinigten Staaten von Amerika[4] über die Bedingungen für nicht nur ausnahmsweise zulässige Datentransfers diesen Anforderungen tatsächlich genügt, wird gegenwärtig geprüft.

3 Siehe 14.1
4 Sog. EU-US Privacy Shield

Das Urteil des Europäischen Gerichtshofs sollte von den Netzbetreibern und Diensteanbietern, aber auch von der Politik als Chance verstanden werden, verstärkt Technologien und Dienste anzubieten und zu fördern, bei denen die personenbezogenen Daten vorrangig in Deutschland oder Europa verarbeitet werden. Erste Angebote dieser Art zeichnen sich bereits ab. Auch wenn der Datenexport in außereuropäische Länder weiterhin notwendig sein wird, ist dieser wettbewerbspolitische Effekt des Safe Harbor-Urteils nicht zu unterschätzen. Auch mehrere Start Ups und Geschäftsideen, die in Berlin entwickelt werden, machen deutlich, dass Datenschutz ein Wettbewerbsvorteil sein kann („Datenschutz made in Berlin“).[5] Entgegen anderslautenden Behauptungen bremst der Datenschutz weder die Digitalisierung noch die Gründung neuer Unternehmen, sondern kann im Gegenteil zum Motor für Innovationen werden.

Es ist offenkundig, dass die große Zahl von Flüchtlingen in der Stadt zu erheblichen Problemen auch für den Datenschutz und die Privatsphäre geführt hat, selbst wenn der Bericht hierzu kein eigenes Kapitel enthält. Es war und ist offenbar nicht möglich, Flüchtlingen in Massen- und Notunterkünften einen angemessenen Schutz ihrer Privatsphäre zu ermöglichen. Datenschutz und der Schutz der Privatsphäre sind Menschenrechte, die auch Flüchtlingen unabhängig von ihrem Status zustehen. Auch deshalb müssen so schnell wie möglich Unterkünfte gefunden werden, die den Flüchtlingen Privatheit ermöglichen.

Sowohl auf Bundes- wie auf Landesebene werden gegenwärtig durch gesetzliche Maßnahmen Kompetenzen gebündelt und Aufgaben bei einzelnen Behörden konzentriert. Das ist im Grundsatz richtig. Gleichwohl muss daran erinnert werden, dass der Gesetzgeber auch bei der Verarbeitung von Daten der Flüchtlinge von den datenschutzrechtlichen Grundsätzen der Erforderlichkeit und Zweckbindung nicht abweichen darf. In den zukünftigen zentralen Datenbanken werden teilweise sensitive Daten (z. B. über den Gesundheitszustand oder – auf freiwilliger Basis – die Religionszugehörigkeit) gespeichert, auf die nicht alle beteiligten Behörden und Bediensteten innerhalb einer Behörde zugreifen dürfen. Flüchtlinge genießen keinen „Datenschutz 2. Klasse“.

5 Siehe 2.6

Weniger der Datenschutz als vielmehr die Informationsfreiheit spielte eine wichtige Rolle bei den Verhandlungen über ein Transatlantisches Freihandelsabkommen (TTIP).[6] Dieses Abkommen stößt auf beiden Seiten des Atlantiks aus verschiedenen Gründen auf Widerstand. Die Verhandlungen wurden und werden aber insbesondere durch einen erheblichen Mangel an Transparenz erschwert, der in der Öffentlichkeit und in den Parlamenten für zusätzliches Misstrauen sorgt. Die deutschen Informationsfreiheitsbeauftragten haben dies kritisiert.[7]

Anderseits ist es zu begrüßen, dass mit Rheinland-Pfalz ein weiteres Bundesland nach Hamburg sein Informationsfreiheitsgesetz durch ein Transparenzgesetz abgelöst hat.[8] Es ist zu hoffen, dass auch im Land Berlin die Zeichen der Zeit erkannt werden und die Verwaltung zur proaktiven Bereitstellung von Informationen – neben dem Informationszugang auf Antrag – verpflichtet wird.

Da der Berichtszeitraum (1. Januar bis 31. Dezember 2015) noch in die Amtszeit des bisherigen Berliner Beauftragten für Datenschutz und Informationsfreiheit, Dr. Alexander Dix, fällt, wird in dem Bericht an verschiedenen Stellen noch die männliche Form für den/die Beauftragte/n nach Art. 47 der Verfassung von Berlin verwendet.

6 Siehe 16.1.2

7 Entschließung vom 30. Juni 2015: Mehr Transparenz bei den Verhandlungen über das Transatlantische Freihandelsabkommen (TTIP), Dokumentenband 2015, S. 127

8 Siehe 16.1.3

1 Digitale Verwaltung

1.1 Anliegenmanagement – Ordnungsamt-Online

Im Rahmen des Modernisierungsprogramms ServiceStadtBerlin 2016 wurde das Projekt „Einführung eines Anliegenmanagementsystems (AMS) für die Berliner Ordnungsämter“ initiiert.[9] Mit diesem Verfahren sollen Bürgerinnen und Bürger die Möglichkeit erhalten, Meldungen zu Störungen im öffentlichen Raum über verschiedene Meldewege dem zuständigen Ordnungsamt zu übermitteln. Meldungen an die Ordnungsämter können dabei über Internet, E-Mail, Fax, Telefon (115) und per Handy-App erfolgen. Möchte man keine Rückantwort, sondern nur eine Störung melden, kann dies auch ohne Angabe von persönlichen Daten, also anonym erfolgen. Die Meldungen sollen unabhängig vom Meldeweg medienbruchfrei in das IT-Fachverfahren überführt und im Internet veröffentlicht werden, wobei den Bürgerinnen und Bürgern anhand eines Ampelsystems der jeweilige Bearbeitungsstand signalisiert werden soll. Eine Veröffentlichung von personenbezogenen oder personenbeziehbaren Daten wie z. B. Kfz-Kennzeichen darf dabei aber nicht erfolgen.

Das Fachverfahren soll in allen 12 bezirklichen Ordnungsämtern zum Einsatz kommen. Es wird zwar zentral vom Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) im IT-Dienstleistungszentrum (ITDZ) betrieben, die Datenhaltung erfolgt aber getrennt für jeden Bezirk, und die datenschutzrechtliche Verantwortung trägt jedes bezirkliche Ordnungsamt für seinen Bereich. Diese Konstellation muss durch vertragliche Regelungen zur Verarbeitung personenbezogener Daten im Auftrag nach § 3 Berliner Datenschutzgesetz (BlnDSG) schriftlich festgelegt werden. So entstand im Rahmen dieses Verfahrens ein für die bezirklichen Ordnungsämter und das LABO allgemeingültiges Regelwerk, bestehend aus einem Rahmen-Verfahrensauftrag mit den allgemeinen Rahmenbedingungen, allgemeinen Leistungen des LABO und der Bezirke, einer Ergänzung zum Rahmen-Verfahrensauftrag mit den Festlegungen zur Auftragsdatenverarbeitung und einem Einzelleistungsschein für das IT-Verfahren „AMS“. Solch eine Aufteilung ermöglicht eine zukünftige einheitliche und

9 Zum Vorläuferprojekt „Maerker“ siehe JB 2013, 1.6

transparente Grundlage für die Zusammenarbeit zwischen dem LABO und den Bezirksämtern und erfordert bei weiteren Verfahren jeweils nur noch die Erstellung eines Einzelleistungsscheins.

Mittlerweile ist das Verfahren in zwei Bezirken im Pilotbetrieb. Gleich zu Beginn mussten wir jedoch feststellen, dass bei mehreren Meldungen personenbezogene bzw. personenbeziehbare Daten im Portal Ordnungsamt-Online über das Internet abrufbar waren. So waren Kfz-Kennzeichen direkt im Meldungstext oder Fotos mit erkennbaren Kfz-Kennzeichen enthalten. Wir haben darauf hingewiesen, dass bei der Übernahme der Meldungen und Veröffentlichung im Internet durch Beschäftigte des jeweiligen Ordnungsamtes offenbar nicht die gebotene Sorgfalt beachtet wird. So sind Kfz-Kennzeichen zu schwärzen oder unlesbar zu machen. Das zuständige Ordnungsamt hat versichert, dass die Mitarbeiterinnen und Mitarbeiter im Ordnungsamt nochmals daraufhin sensibilisiert und belehrt werden.

Im Portal Ordnungsamt-Online dürfen keine personenbezogenen Daten von Bürgerinnen und Bürgern (z. B. Kfz-Kennzeichen) veröffentlicht werden.

1.2 Support-Ende von Windows XP – was nun?

Immer wieder wird in der Presse über Sicherheitslücken in Betriebssystemen von Microsoft berichtet. Über sie können Angreifer z. B. einen schädlichen Code auf den Rechnern einschleusen, Programme installieren, Nutzerkonten anlegen oder Daten ausspähen. Betroffen sind oftmals alle aktuellen Windows-Versionen. In diesen Fällen sollten Nutzer schnellstmöglich die Update-Funktion aktivieren. Sehr häufig ist auch Microsoft Windows XP betroffen, für das kein Sicherheitsupdate mehr verfügbar ist und die Sicherheitslücken somit nicht geschlossen werden können. Diese mit den Sicherheitsupdates für aktuelle Windows-Versionen veröffentlichten Lücken können dann gezielt von Angreifern auf Rechnern ausgenutzt werden, die noch mit dem veralteten Betriebssystem Windows XP ausgestattet sind.

In der Berliner Verwaltung kommt jedoch immer noch im deutlichen Ausmaß das im Jahr 2001 veröffentlichte Betriebssystem Windows XP zum Einsatz.

Am 8. April 2014 stellte die Firma Microsoft letztmalig Sicherheitsupdates für Windows XP zur Verfügung, danach endete der offizielle Support. Damit stieg das Risiko eines erfolgreichen Angriffs erheblich. Auch der vom ITDZ Berlin für die Berliner Verwaltung eingekaufte verlängerte Support, der gewährleistete, dass Sicherheitslücken weiterhin angemessen geschlossen wurden, lief im April 2015 aus.

Sicherheitslücken können insbesondere dadurch entstehen bzw. ausgenutzt werden, dass z. B. die Geräte mit Schadcode auf verschiedenen Wegen in Berührung kommen:

- durch Aufruf von mit Schadcode infizierten Webseiten, insbesondere durch die Nutzung eines veralteten Webbrowsers (z. B. Microsoft Internet Explorer 8),
- durch die Installation mit Schadcode versehener Anwendungen (Programmen), auch als Anhang einer E-Mail,
- durch Ansicht mit Schadcode versehener Dokumente, die per E-Mail, einem Datenspeicher im Netz (z. B. Dropbox) oder über Datenträger an einer lokalen Schnittstelle auf das Gerät übertragen wurden,
- über eine Netzwerkverbindung mit einem von Schadcode betroffenen Computer.

Das Betriebssystem Microsoft Windows XP sollte grundsätzlich nicht mehr eingesetzt werden und der Umstieg auf ein aktuelles Betriebssystem umgehend erfolgen. Ist dies jedoch derzeit nicht einsetzbar, können folgende Maßnahmen ergriffen werden, um das Risiko einer Manipulation bzw. Infektion zu verringern:

1. Maßnahmen, die direkt am Gerät vorgenommen werden:
   - Auswahl und regelmäßiger Wechsel eines sicheren Passwortes,
   - Installation des letzten Updates für Windows XP,
   - Installation eines aktuellen Virenscanners, der fortlaufend aktualisiert wird,
   - Installation eines alternativen „aktuellen“ Browsers (z. B. Firefox oder Chrome),

- Aktivierung der Betriebssystem-Firewall,
- Verhinderung des automatischen Abspeicherns von Inhalten durch Deaktivierung entsprechender Plug-Ins,
- Einschränkung der Rechte, damit z. B. eine unberechtigte Software-Installation oder Systemänderung verhindert wird,
- Installation der neuesten Programmversion des „Enhanced Mitigation Experience Toolkit", welches die Ausnutzung bekannter Sicherheitsschwachstellen verhindern soll.

2. Betrieb des Computers im sog. Windows XP Kiosk-Modus, der den PC nach jedem Neustart in einen zuvor definierten Zustand zurückversetzt und zwischenzeitliche Änderungen oder Manipulationen unwirksam macht.

3. Einsatz des Betriebssystems in einer virtuellen Umgebung, in der nur der Aufruf und Betrieb eines Fachverfahrens möglich ist und z. B. USB-Geräte nicht unterstützt werden sowie ein Datenaustausch über eine gemeinsame Zwischenablage verhindert wird.

4. Technische Unterbindung des Internetzugangs oder spezielle Abschottung an den Netzübergängen durch Sicherheitskomponenten, die Bedrohungen erkennen und bekannten Schadcode aus dem Datenstrom herausfiltern bzw. abweisen (z. B. gestaffelte Firewallsysteme, Web Application Firewall, Webgateway oder Virenscanner). Beschränkungen der aufrufbaren Webseiten (Whitelists).

5. Spezielle Systeme im Netzwerk oder auf den Computern, die entsprechendes Angriffsverhalten erkennen und abweisen. Damit soll z. B. verhindert werden, dass Daten unerlaubt aus dem System herausgeschmuggelt werden.

6. Beschränkung des Zugriffs auf externe Speichermedien bzw. Schnittstellen, damit ein Datenaustausch wirkungsvoll unterbunden werden kann.

7. Virtualisierung des Zugriffs auf E-Mails oder Beschränkung des E-Mail-Verkehrs auf Nachrichten mit Anhängen, die auf Schadcodes geprüft wurden.

8. Einsatz eines Terminalservers, der dem Arbeitsplatzcomputer in einem abgeschotteten Fenster den Zugriff auf das Internet ermöglicht. Ein Datenaustausch zwischen den beiden Arbeitswelten wird unterbunden.

9. Für das Surfen im Internet kann auch der Einsatz einer sog. „Sandbox“ genutzt werden. Hierbei kann z. B. der Internet-Browser in einem Bereich ausgeführt werden, der vom restlichen Betriebssystem isoliert ist. Schadsoftware soll durch diesen Schutz der Zugriff auf die Festplatte nicht möglich sein. Nach Beendigung des Programms werden evtl. vorgenommene Änderungen – vergleichbar mit dem Kiosk-Modus - gelöscht.

Für alle aufgeführten Maßnahmen, die meist aufeinander aufbauend zu verstehen sind, muss jedoch eine spezielle Sicherheitsbetrachtung für jeden Einzelfall durchgeführt werden, denn grundsätzlich ist jede Bedrohung aktueller und den Schutzmaßnahmen einen Schritt voraus.

Vom Einsatz eines vom Hersteller nicht mehr unterstützten Betriebssystems ist grundsätzlich abzuraten. Ansonsten muss ein hoher Aufwand an weiterführenden Maßnahmen zum Schutz der neu entstandenen Risiken durchgeführt werden.

1.3 Nochmals: E-Recruiting – das Jobportal der Berliner Verwaltung

Im letzten Jahresbericht berichteten wir über das neue Jobportal, das in vielen Berliner Einstellungsbehörden eingesetzt wird.[10] Seinerzeit konnte dank der guten Zusammenarbeit zwischen den Datenschutzbeauftragten und der Projektgruppe für das IT-Verfahren innerhalb kürzester Zeit ein relativ gutes Datenschutzniveau erreicht werden. Es blieben aber noch einige Punkte offen.

Zwischenzeitlich wurde das verfahrensspezifische Sicherheitskonzept überarbeitet, es ist bei Bedarf fortzuschreiben. Die Umsetzung der darin genannten Maßnahmen ist von elementarer Bedeutung und wird zu gegebener Zeit einer Kontrolle unterzogen.

Da sich diese Software auch an Wirtschaftsunternehmen richtet, sind Zugriffe aus dem Verfahren heraus auf soziale Netzwerke wie XING oder Facebook

10 JB 2014, 6.3

möglich. Wir haben auf die Unzulässigkeit solcher Zugriffe hingewiesen und mitgeteilt, dass die Daten ausschließlich bei den betroffenen Bewerberinnen und Bewerbern zu erheben sind.

Da im Rechte- und Rollenkonzept weitreichende Zugriffsberechtigungen definiert werden, kommen der Protokollierung und Auswertung von Zugriffen eine besondere Bedeutung zu. Es müssen Maßnahmen ergriffen werden, mit denen festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat. Der Zweck der Protokollierung besteht darin, ein Verfahren zur Verarbeitung personenbezogener Daten so transparent zu machen, dass die Ordnungsmäßigkeit bzw. Rechtswidrigkeit einer Verarbeitung nachweisbar ist. Protokolldaten müssen Auskunft über den Zeitpunkt und die Bezeichnung eines Ereignisses (oder Tätigkeit), die mit dem Ereignis (oder Tätigkeit) befasste Person und den Zweck der Tätigkeit geben.

Problematisch ist die Nutzung einer Export-Funktion. Jeder Datenexport mit personenbezogenen Daten ist zu unterbinden, da hier nicht mehr kontrolliert werden kann, was nach dem Export mit den gespeicherten Daten geschieht. Es greifen weder das Rechte- und Rollenkonzept noch die ansonsten eingerichteten Schutzvorkehrungen oder Löschfristen außerhalb des Verfahrens. Hier wird die Verantwortung an die einsetzenden Behörden übertragen, die einen entsprechenden Schutz einrichten müssen. Für die Fortentwicklung des Verfahrens sollte berücksichtigt werden, dass die benötigten Daten im Verfahren zur Verfügung gestellt werden und somit ein Datenexport ausgeschlossen wird.

Auch wenn bisher den meisten Empfehlungen gefolgt wurde, sind noch Nacharbeiten notwendig. Wir werden das Verfahren weiterhin aufmerksam begleiten.

1.4 EALS – Elektronisches Anmelde- und Leitsystem

Das webbasierte Elektronische Anmelde- und Leitsystem (EALS) unterstützt Schülerinnen und Schüler sowie die beteiligten Schulen bei dem Übergang von den weiterführenden Schulen zu den Lehrgängen und Bildungsgängen

der beruflichen Schulen. Hierbei muss sichergestellt sein, dass die Daten der Schülerinnen und Schüler nur von den notwendigen Stellen einsehbar sind und die freie Entscheidung der Betroffenen bzw. ihrer Erziehungsberechtigten gewahrt wird.

Neben den Stammdaten der Schülerinnen und Schüler sowie der Erziehungsberechtigten werden auch Daten zur bisherigen Schul- bzw. Berufsausbildung erhoben. Des Weiteren werden Berufswunsch bzw. Qualifikationsinteressen aufgenommen sowie die Angabe von Wunschschulen unterstützt.

Der Zweck der Verarbeitung ist es, den gesamten Prozess des Schulwechsels zu vereinfachen und vor allem der Senatsverwaltung für Bildung, Jugend und Wissenschaft eine Übersicht zu ermöglichen. So soll die gesetzliche Verpflichtung erfüllt werden, jedem Schulbesucher auf Wunsch eine Anschlussperspektive anzubieten. Mit dem System hofft man, z. B. frühzeitig etwaige Mängel an entsprechenden Angeboten (Bildungseinrichtungen, Fachrichtungen) zu erkennen, sodass ein rechtzeitiges Umsteuern möglich ist. Diesem Zweck dienen auch die vorgesehenen Datenweiterleitungen u.a. an die Berufsberatungsstellen der Bundesagentur für Arbeit und die bezirklichen Jugendberatungsstellen. Das EALS ist zugleich ein wichtiger Baustein für die Jugendberufsagenturen.[11]

Die Teilnahme an dem Verfahren beruht auf der Einwilligung der Betroffenen bzw. ihrer Erziehungsberechtigten. Die uns vorgelegte Einwilligungserklärung entsprach nicht den Erfordernissen, da nur eine pauschale Einwilligung in sämtliche Aspekte der Datenverarbeitung vorgesehen war, die zudem offenließ, in welchen Fällen Datenübermittlungen an welche Empfänger stattfinden. Dies entspricht nicht den Anforderungen an Transparenz und Freiwilligkeit. Wir haben eine Überarbeitung der Einwilligungserklärung nahegelegt, die die Freiheit lässt, die notwendigen Stammdaten und ggf. freiwillige Daten wie Telefonnummer und E-Mail-Adresse auch an die bezirklichen Jugendberatungsstellen bzw. an den Berufsberater weiterzuleiten, wenn keine Aufnahme in der Wunschschule möglich war.

Auch konnten wir einige technische Hinweise zu dem Verfahren geben. Die nunmehr differenzierten Einwilligungserklärungen, die zuerst auf dem

11 Siehe JB 2014, 4.3

papierenen Anmelde- und Leitbogen durch Ankreuzfelder kenntlich gemacht werden, müssen auch in der elektronischen Darstellung dieses Formulars umgesetzt werden, um im Bedarfsfall die Datenweitergabe an bzw. die Freigabe für die entsprechenden Stellen steuern zu können. Zudem müssen im System auch Statusinformationen darüber abgelegt werden, ob der betreffende Bogen bereits unterschrieben und von der bisherigen (abgebenden) Schule geprüft wurde. Die Statusinformationen sind notwendig, um eine Weiterleitung von Daten ohne vorliegende Einwilligung zu vermeiden.

Bezüglich der IT-Sicherheit haben wir den Einsatz einer Zwei-Faktor-Authentifizierung für die Benutzer nahegelegt, die auf mehr als einige wenige Datensätze zugreifen können. Neben dem Passwort könnte der zweite Sicherheitsfaktor die Beschränkung auf ein bestimmtes Endgerät, auf das Verwaltungsnetz einer bestimmten Schule oder auch der Besitz bzw. Zugang zu Gegenständen wie einer Chipkarte oder einem TAN-Generator sein.

Bei vielen Verfahren, die personenbezogene Daten mit Einwilligung der Betroffenen verarbeiten, wird nicht in ausreichendem Maße berücksichtigt, dass den Einwilligenden freigestellt sein muss, ob und in welchem Umfang bzw. zu welchen Zwecken sie einer Verarbeitung ihrer Daten zustimmen. Andernfalls wäre eine wichtige Voraussetzung für die Wirksamkeit der Einwilligung, die Freiwilligkeit, nicht gewährleistet. Alle wesentlichen Entscheidungsmöglichkeiten müssen auch in technischen Systemen umgesetzt werden.

1.5 eVAk – Begleitung des neuen Verfahrens

Die Verwaltungsakademie Berlin (VAk) testet derzeit ein webbasiertes Anmeldeverfahren (eVAk) für die angebotenen Fortbildungsveranstaltungen. Mit eingebunden in das Anmeldeverfahren sind die Fortbildungsbeauftragten ausgewählter Pilotbehörden. Auch unsere Dienststelle beteiligte sich an dem Pilotbetrieb.

Das Online-Portal soll die notwendigen Schritte von der Auswahl eines Fortbildungsangebotes über die Beantragung in der eigenen Behörde bis zur

Bestätigung der Teilnahme erleichtern. Auf dem Portal der VAk können die Beschäftigten aus dem Gesamtkatalog der angebotenen Veranstaltungen leicht die sie interessierenden Veranstaltungen finden. Bisher erfolgte der weitere Ablauf, der die Einbeziehung der Fortbildungsbeauftragten sowie die jeweilige Behördenleitung erfordert, ausschließlich auf Papier.

Ein Teil dieses aufwendigen Verfahrens wird demnächst durch ein Online-Verfahren vereinfacht. Bestandskunden der VAk können nunmehr selbstständig die ersten Schritte der Auswahl und Anmeldung zu einer Fortbildungsveranstaltung unternehmen. Die Fortbildungsbeauftragten können in ihren Accounts die Anmeldungen der ihnen zugeordneten Beschäftigten einsehen und die behördeninternen Schritte zur Genehmigung initiieren. Die VAk entscheidet dann je nach Verfügbarkeit, ob eine Teilnahme ermöglicht wird. Nach der Veranstaltung können sowohl die Fortbildungsbeauftragten als auch die Beschäftigten entsprechende Teilnahmebescheinigungen herunterladen.

Datenschutzrechtliche Fragen ergaben sich in Bezug auf die Historie der von den Beschäftigten besuchten Veranstaltungen sowie den Anmelde- bzw. Teilnahmestatus. Insbesondere bei einem Wechsel des Arbeitsplatzes stellte sich die Frage, ob Informationen über bisher besuchte Veranstaltungen automatisch für die neuen Fortbildungsbeauftragten zugänglich sein sollten. Nach Aussage der VAk sollen das die Beschäftigten beim Behördenwechsel selbst entscheiden können (Einwilligungslösung).

Um eine breite Nutzung des Online-Angebotes von Anfang an zu ermöglichen, erhalten sämtliche bisherige Kunden der VAk einen Account für das Online-Portal. Zuerst war hierfür eine Lösung vorgesehen, bei der die Logins mit generischen Passwörtern versehen waren. Diese Lösung entsprach jedoch in keiner Weise den Anforderungen: Für jeden Account waren allenfalls 600 Passwörter möglich, die sich innerhalb kurzer Zeit durchprobieren lassen. In enger Kooperation zwischen der VAk und uns konnte hierfür eine sichere Lösung gefunden werden, die dennoch den über 70.000 Kunden die einfache Nutzung des Online-Zuganges ermöglicht. Hierfür wird für die Erstaktivierung des Online-Accounts eine E-Mail an die dienstliche E-Mail-Adresse der Beschäftigten über das vergleichsweise geschützte Intranet der Berliner Verwaltung gesendet, die einen zeitlich befristeten Aktivierungslink enthält.

Die IT-Sicherheit kann leicht durch konzeptionelle Fehler gefährdet werden. Einen gewissen Schutz bieten die vom Berliner Datenschutzgesetz vorgeschriebene Durchführung einer Risikoanalyse und die darauf aufbauende Erstellung eines Sicherheitskonzeptes.

1.6 BBB-Premiumkarte – ein Schritt zum gläsernen Schwimmer?

2013 haben die Berliner Bäder-Betriebe (BBB) ein neues Produkt auf den Markt gebracht, das sich insbesondere an Stammkunden und Dauernutzer richtet: Die BBB-Premiumkarte.[12] Diese Chipkarte ermöglicht es, für einen festen Preis ein Jahr lang unbegrenzt oft in allen Frei-, Sommer- und Hallenbädern der BBB schwimmen zu gehen.

Dies klingt nach einem verlockenden Angebot für alle „Dauerschwimmer" in Berlin. Doch die Sache hat einen entscheidenden Haken: Bei jedem Einsatz der Chipkarte wird auch stets mit Datum und Uhrzeit gespeichert, wann der Kunde das betreffende Bad betreten und verlassen hat. Somit lassen sich problemlos umfangreiche Bewegungs- und Nutzungsprofile erstellen. Auf diesem Wege werden die Nutzer der BBB-Premiumkarte zu gläsernen Kunden.

Dieser Umstand wird jedoch gegenüber den Kunden nicht ausreichend transparent dargestellt. Er ist vielen wahrscheinlich nicht bekannt. So finden sich auf der Internetseite der BBB zwar zahlreiche Informationen zum Produkt,[13] die Datenschutzrisiken werden dort jedoch an keiner Stelle erwähnt. Lediglich in den „Allgemeinen Vertragsbedingungen für die Premiumkarte" findet sich eine Klausel, welche den Bäderbetrieben pauschal die Befugnis zur Erhebung und Verarbeitung von „Daten über die Nutzung von Bädern durch den Nutzer" einräumt.

12 http://www.berlinerbaeder.de/aktuelles/detail/premiumkarte-nutzen-sie-die-preisvorteile/
13 http://www.berlinerbaeder.de/fileadmin/user_upload/Premiumkarte_Infoflyer/Information-Premiumkarte_web.pdf

Das Unternehmen hat die umfangreiche Speicherung der Nutzungsdaten auf unsere Nachfrage damit begründet, dass einerseits der Missbrauch der Karte nach Verlust oder Diebstahl und andererseits eine Mehrfachnutzung durch Weitergabe im Freundes- oder Bekanntenkreis verhindert werden soll. Es ist nicht nachvollziehbar, wie diese Zwecke durch die Erstellung von Bewegungs- und Nutzungsprofilen erreicht werden sollen. Um eine Ersatzkarte zu erhalten, ist der Verlust einer Premiumkarte zu melden. Die Gültigkeit bzw. Sperrung kann im Kassensystem der BBB gespeichert werden. So kann eine gesperrte Karte bei ihrem unberechtigten Einsatz unmittelbar aus dem Verkehr gezogen werden.

Unberechtigte Mehrfachnutzungen können geeigneter durch Stichprobenkontrollen am Einlass festgestellt und verhindert werden. Soweit es um die statistische Erfassung der Auslastung der Berliner Bäder geht, kann dies auch mit allgemeineren Angaben erreicht werden. Aktuell untersuchen wir in einer umfangreichen Prüfung verschiedene Prozesse bei den BBB.

Die BBB-Premiumkarte mag ein attraktives Produkt für Stammkunden der BBB sein. Gleichwohl geht mit der noch immer zu umfangreichen Speicherung der Nutzungsdaten ein unnötig hohes Datenschutzrisiko für alle Besitzer der BBB-Premiumkarte einher. Darüber hinaus sind die Informationen der BBB gegenüber den Kundinnen und Kunden und potenziellen Interessenten intransparent und mangelhaft, da auf die Datenschutzrisiken nicht hingewiesen wird. Eine datensparsamere und gleichwohl für „Vielschwimmer" attraktive Alternative ist umzusetzen.

1.7 Umgang mit privater E-Mail in dienstlichen Postfächern

Eine Vielzahl von Beschäftigten in der Berliner Verwaltung verfügt mittlerweile über eine eigene dienstliche E-Mail-Adresse. Neben dem regulären herkömmlichen Posteingang in Papierform ist E-Mail zu einem wichtigen Kommunikationsmittel im dienstlichen Alltag aufgestiegen. Da liegt es nahe, nebenbei in der Pause die eine oder andere Mail für private Zwecke zu versenden.

Es stellt sich die Frage, ob die Nutzung des dienstlichen E-Mail-Postfachs für private Zwecke zulässig ist. Näheres regelt die Dienstvereinbarung über die Nutzung des Internet und anderer elektronischer Informations- und Kommunikationsdienste in der Berliner Verwaltung (Internet-DV) vom 21.02.2002.[14] Dort wird die private Nutzung von Internetdiensten, zu denen auch die E-Mail zählt, grundsätzlich verboten. Das bedeutet: Auch wenn in einer Behörde die private Nutzung vor Abschluss der Rahmendienstvereinbarung geduldet wurde (sog. betriebliche Übung), kommt diese nicht zum Tragen, wenn – wie hier – eine ausdrückliche Regelung besteht, die eine Privatnutzung untersagt.

Generell dürfen dienstliche E-Mails der Beschäftigten vom Dienstherrn zur Kenntnis genommen und somit gelesen werden. Nicht von einer dienstlichen Erforderlichkeit gedeckt ist eine nachträgliche Durchsicht sämtlicher empfangener und versandter E-Mails. Dies verstieße gegen den Verhältnismäßigkeitsgrundsatz.

Für den Fall der Abwesenheit kann eine Weiterleitung der E-Mails von Beschäftigten in Betracht kommen. Allerdings ist im Hinblick auf die schutzwürdigen Belange der Beschäftigten die Verwendung einer Abwesenheitsnotiz vorzuziehen. Dies kann auch durch den Dienstherrn veranlasst werden. Bei einer vorhersehbaren Abwesenheit ist ein automatisierter Hinweis des Beschäftigten auf seine Abwesenheit sowie auf seine Vertretung sinnvoll ebenso wie die Einrichtung einer Weiterleitung an die Vertretung, soweit erforderlich.

Das ist bei unvorhersehbarer Abwesenheit wie einer Erkrankung nicht möglich. Im Idealfall wird bereits im Vorfeld ein Zugriff der Vertretung auf das Postfach in Abstimmung mit dem Beschäftigten eingerichtet. Bei einer absehbaren kurzen Erkrankung ist je nach Einzelfall zu prüfen, ob ein Zugriff tatsächlich notwendig erscheint. Es sollte darüber hinaus in der Dienstvereinbarung ergänzend geregelt werden, wie der Zugriff bei Abwesenheit (ggf. durch Hinzuziehung des behördlichen Datenschutzbeauftragten, des Personalrates oder anderer Instanzen) erfolgt. Schließlich ist unabhängig davon nicht auszuschließen, dass E-Mails einer sog. Mischnutzung zuzuordnen sind, die neben beruflichen auch private Aspekte tangieren. Eine zwingende vorherige Einholung einer schriftlichen Einwilligung der

14 https://www.berlin.de/hpr/dienstvereinbarungen/artikel.299659.php

Beschäftigten ist bei einer allein beruflich vorgesehenen Nutzung rechtlich allerdings nicht vorgeschrieben.

Eine Öffnung von E-Mail-Postfächern ohne Wissen der Betroffenen für die gesamte Arbeitsgruppe unabhängig von Vertretungsregelungen ist grundsätzlich nicht zulässig.

Erkennbar private E-Mails im Postfach dürfen vom Dienstherrn nicht weiter zur Kenntnis genommen werden, sobald ihr nicht-dienstlicher Charakter erkannt wurde. Andernfalls besteht die Gefahr einer Verletzung des Post- und Fernmeldegeheimnisses.[15] Als privat erkannte E-Mails (z. B. anhand des Betreffs oder des Kommunikationspartners) dürfen inhaltlich nur vom vorgesehenen Empfänger (d.h. Postfachinhaber) gelesen werden. Das Zugriffsverbot für den Dienstherrn für diese Mails berührt jedoch nicht das grundsätzliche Nutzungsverbot des dienstlichen E-Mail-Postfachs für private Zwecke. Dienstrechtliche Konsequenzen für den Beschäftigten können die Folge sein.

Um diese Problematik zu umgehen, sollten private E-Mails ausschließlich über private E-Mail-Postfächer gesendet und empfangen werden. Es existieren diverse Anbieter entsprechender kostenfreier oder kostenpflichtiger Dienste, auf die in der Pause oder Freizeit mit privaten Geräten (Smartphones, Notebooks) zugegriffen werden kann. Auf einen entsprechenden Zugriff über dienstliche Geräte ist aber gemäß dem Verbot der Internet-DV zu verzichten.

Grundsätzlich darf der Dienstherr unter Wahrung der Verhältnismäßigkeit auf dienstliche E-Mails in Abwesenheit des Beschäftigten zugreifen. Sind einzelne E-Mails erkennbar privat, so dürfen diese nicht gelesen werden. Die private Nutzung des dienstlichen E-Mail-Postfachs kann dienstrechtliche Konsequenzen haben.

15 § 206 Strafgesetzbuch (StGB)

1.8 Umgang mit Datenträgern bei gemieteten IT-Geräten

Das Mieten oder Leasing von IT-Geräten mit höheren Anschaffungskosten wird auch in der Berliner Verwaltung seit längerem praktiziert. Geräte, die über einen nicht flüchtigen Langzeitspeicher wie Festplatten und sog. „Flashspeicher-Bausteine" verfügen, erzeugen beim bestimmungsgemäßen Gebrauch (z. B. Kopieren und Faxen) personenbezogene Daten. Diese Daten werden für einen unbestimmten Zeitraum auf diesen Speichern abgelegt.

Am Beispiel digitaler Kopiersysteme kann diese Problematik gut verdeutlicht werden. Die Vorteile dieser Geräte sind die Optionen, sie zu Netzwerkdruckern, Scannern oder sogar zu Faxgeräten aufzurüsten. Die sog. „Box"-Funktion bietet sogar eingeschränkte Serverfunktionalitäten an. In Sekretariaten sind multifunktionale Kopiersysteme kaum noch wegzudenken. Diese leistungsfähigen Geräte sind heutzutage im Netzwerk als zentrale Büro- oder Abteilungsdrucker vielseitiger und wirtschaftlicher als herkömmliche Drucker. Da diese Multifunktionssysteme auch ins behördeneigene Netzwerk integriert werden und sogar Verbindung zum Internet aufnehmen können, benötigen sie ähnliche Sicherheitsvorkehrungen wie PCs oder Server. Vor allem durch die Netzwerkfähigkeit können die Geräte zu einem Sicherheitsrisiko in Behörden und Unternehmen werden.

Datenschutzrisiken könnten z. B. bei der Rückgabe bzw. Entsorgung gemieteter Geräte an den Hersteller entstehen. Einige Hersteller reagieren darauf mit verschiedenen Ansätzen, z. B. statten sie ihre Produkte mit Funktionen zur Festplattenverschlüsselung aus. Demnach sollen die Daten verschlüsselt abgelegt und daher von Außenstehenden nicht zu entschlüsseln sein. Mittlerweile ist dieses Sicherheits-Feature als Option in den über die Rahmenverträge des ITDZ zu beziehenden Geräten verfügbar. Alle Kopien und gedruckte Dokumente werden im internen (Zwischen-)Speicher eines digitalen Kopiersystems abgelegt. Unklar sind dabei die Art und Dauer der Speicherung. Die Annahme, dass die Daten im internen (Zwischen-)Speicher abgelegt und je nach Größe eines weiteren zu druckenden Dokuments nach Bedarf beliebig überschrieben werden, konnte bisher nicht eindeutig bestätigt werden. Eine solche Lösung wäre auch unzureichend. Entsprechende Hinweise werden

in der Orientierungshilfe „Sicheres Löschen magnetischer Datenträger“ des Arbeitskreises Technik gegeben.[16]

Gemietete IT-Geräte werden im Rahmen der automatisierten Datenverarbeitung eingesetzt. Ihr Einsatz ist daher in die nach § 5 Abs. 3 BlnDSG erforderlichen Risikoanalysen und Sicherheitskonzepte einzubeziehen. Bei den mit Speichern ausgestatteten digitalen Systemen ist zu verhindern, dass die gespeicherten Daten von Unbefugten gelesen, verändert oder gelöscht werden können.

Normalerweise ist nicht festgelegt, wer diese Geräte in welcher Art nutzt. Bezugnehmend auf das Beispiel der digitalen Kopiergeräte darf jeder im Rahmen seiner Aufgabenerfüllung kopieren, sodass individuelle Berechtigungsprofile keinen Sinn machen. Deshalb dürfen beim normalen Kopieren keine Datenspeicherungen vorgenommen werden, die ohne einen erheblichen technischen Aufwand ausgelesen werden können. Die fortdauernde Speicherung darf nur im Einzelfall bewusst ausgelöst werden können, weil die Daten für spätere Vorgänge wiederverwendet werden sollen. Für eine differenzierte Regelung des Zugriffs auf gespeicherte Dokumente muss das System individuelle Lese- und Löschungsrechte für einzelne Dokumente ermöglichen und mit einem Authentisierungsverfahren (z. B. Kennung und Passwort, ID-Karte) die Berechtigungsprüfung zulassen. Der Systembetreiber bzw. die Systemverwaltung muss alle gespeicherten Informationen datenschutzgerecht löschen können.

Mittlerweile hat das Bundesamt für die Sicherheit in der Informationstechnik (BSI) im Rahmen des BSI-Grundschutzes mehrere Maßnahmebausteine erstellt und veröffentlicht. Als Beispiele sind der Baustein „M 2.167 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten“ und der Baustein „M 2.400 Sichere Außerbetriebnahme von Druckern, Kopierern und Multifunktionsgeräten“ zu nennen.

Die einsetzende Stelle hat bei Rückgabe sicherzustellen, dass die Löschung der in den Geräten enthaltenen Datenträger, wenn diese nicht hinreichend

16 http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/04/Orientierungshilfe_Sicheres_Loeschen_magnetischer_Datentraeger_AK_Technik_.pdf

verschlüsselt sind, datenschutzgerecht durchgeführt wird. In der Regel ist die Entsorgung über ein in Deutschland zertifiziertes Unternehmen ausreichend. Ein blindes Vertrauen auf die Verfahren der Hersteller, dessen Dienstleister sich in der Regel im Ausland befinden, reicht dagegen nicht aus. Bei dieser Vorgehensweise handelt es sich um eine unzulässige Datenübermittlung ins Ausland. Im Zweifel sind die Datenträger (auch kostenpflichtig) auszubauen und fachgerecht zu löschen bzw. zu entsorgen.

Beim Einsatz von gemieteten IT-Geräten mit nicht flüchtigen Datenspeichern sind die darauf verarbeiteten Daten im Regelfall zu verschlüsseln. Ist das nicht möglich, so ist bei der Rückgabe der Geräte darauf zu achten, dass die gespeicherten Daten rechtskonform gelöscht oder die Datenträger vernichtet werden.

2 Schwerpunkte

2.1 Durchbruch zu einem neuen Rechtsrahmen für Europa

2.1.1 Grundverordnung

Nach vier Jahren zäher Verhandlungen ist endlich ein Durchbruch bei der EU-Datenschutz-Grundverordnung gelungen. Wir hatten bereits in den vergangenen Jahren über das Reformprojekt berichtet.[17] Die neue Datenschutz-Grundverordnung soll die EU-Datenschutzrichtlinie von 1995 ablösen, die als veraltet gilt.

Anders als diese Richtlinie, die jeder Mitgliedstaat der EU in innerstaatliches Recht umsetzen musste, gilt die neue Verordnung unmittelbar. Das bedeutet, dass nach Ablauf der Übergangsfrist von zwei Jahren überall in der EU das gleiche Datenschutzrecht gilt. Dies ist zum einen von Vorteil für europaweit agierende Unternehmen, die sich nunmehr nur noch an ein einheitliches Datenschutzrecht halten müssen. Zum anderen wird verhindert, dass sich Unternehmen einen Standort suchen, an welchem die Datenschutzgesetze weniger streng sind. Hinzu kommt, dass die neue Datenschutz-Grundverordnung auch für außereuropäische Unternehmen verbindlich ist, die ihren Kundinnen und Kunden in der EU Waren und Dienstleistungen anbieten oder ihr Verhalten überwachen.[18]

Der Rechtsschutz der Bürgerinnen und Bürger wird zudem entscheidend gestärkt: Sie können sich nunmehr bei ihrer Datenschutzbehörde vor Ort über eine Datenschutzverletzung beschweren, auch wenn die datenverarbeitende Stelle ihren Sitz im Ausland hat.[19] Bisher mussten wir die Betroffenen bei solchen Beschwerden an die jeweils zuständige Datenschutzbehörde im Ausland

17 JB 2012, 14.1; JB 2013, 2.1; JB 2014, 11.1
18 Art. 3 EU-Datenschutz-Grundverordnung
19 Art. 73 EU-Datenschutz-Grundverordnung

verweisen. Nach der neuen Verordnung können wir gemeinsam mit der zuständigen Datenschutzbehörde den Fall aufklären und entsprechende Maßnahmen zum Schutz der Datenschutzrechte initiieren.[20]

Erfreulich ist außerdem, dass die bislang in Deutschland bestehende Trennung zwischen Regelungen für den öffentlichen und den nicht-öffentlichen Sektor grundsätzlich aufgehoben und dem europäischen Recht angepasst wurde.[21] Aufgrund der vielen Verflechtungen zwischen Behörden und Unternehmen bei der modernen Datenverarbeitung sind unterschiedliche Datenschutzniveaus nicht mehr zeitgemäß. Auswirkungen hat dies insbesondere auf den öffentlichen Bereich. Bislang konnten wir dort bei einer rechtswidrigen Datenverarbeitung lediglich Beanstandungen ohne unmittelbare Bindungswirkung aussprechen. Diese wurden zwar von der adressierten Behörde in der Regel zum Anlass genommen, die monierte Datenverarbeitungspraxis umzustellen. In einigen Fällen blieben die Empfehlungen aber unbeachtet.[22] Hier bringt die Verordnung eine wesentliche Verbesserung für den Rechtsschutz der Bürgerinnen und Bürger: Nach Inkrafttreten der Datenschutz-Grundverordnung können wir unmittelbar verbindliche Anordnungen nicht nur an Unternehmen, sondern auch an Behörden richten.

Im Vergleich zum deutschen Datenschutzrecht ist die Verordnung weniger detailliert und enthält an vielen Stellen Generalklauseln und unbestimmte Rechtsbegriffe. Dies kann von Vorteil sein, da das in vielen verschiedenen Gesetzen zersplitterte deutsche Datenschutzrecht für den Normadressaten oft schwer zu überschauen war. Allerdings bergen solche Generalklauseln oft eine große Rechtsunsicherheit, wie diese zu interpretieren sind. Um dem entgegenzuwirken, werden wir gemeinsam mit den anderen deutschen und europäischen Aufsichtsbehörden die vorgesehene zweijährige Übergangsfrist nutzen, um Interpretations- und Orientierungshilfen zu erstellen bzw. an die neue Rechtslage anzupassen. Dabei ist das erklärte Ziel des europäischen Gesetzgebers zugrunde zu legen, nicht hinter das Datenschutzniveau der bisherigen Datenschutzrichtlinie zurückzufallen. Die Interpretation der neuen Regeln darf nicht dazu führen, dass es im Ergebnis zu einer

20 Art. 54 a ff. EU-Datenschutz-Grundverordnung
21 Für den Bereich Polizei und Justiz gelten besondere Vorschriften, siehe 2.1.2.
22 Siehe z. B. 5.4, 5.7

Verschlechterung für den Grundrechtsschutz der betroffenen Bürgerinnen und Bürger kommt. Daran müssen sich auch die Gesetzgeber im Bund und in Berlin orientieren, wenn das Datenschutzrecht in Deutschland, soweit es nicht durch die Grundverordnung ersetzt wird, an den neuen Rechtsrahmen angepasst wird.

Eine wichtige Aufgabe für uns wird sein, die Zusammenarbeit mit den anderen europäischen Datenschutzaufsichtsbehörden im neuen Europäischen Datenschutzausschuss zu vertiefen und auszubauen, um eine gemeinsame und kohärente Umsetzung des europäischen Datenschutzrechts zu gewährleisten. Nur so können die in der Grundverordnung vorgesehenen europäischen Abstimmungsmechanismen effektiv zur grenzübergreifenden Durchsetzung der Datenschutzgrundrechte der Betroffenen beitragen.

Die neue Datenschutz-Grundverordnung bringt viele Vorteile mit sich. Sie berücksichtigt, dass moderne Datenverarbeitung nicht an Landesgrenzen haltmacht, und erweitert den Anwendungsbereich des Datenschutzrechts entsprechend. Die Auslegung unbestimmter Rechtsbegriffe und Generalklauseln darf nicht dazu führen, dass das Datenschutzniveau für die Bürgerinnen und Bürger sinkt. Um die Rechte der Betroffenen auch grenzüberschreitend zu schützen, ist nicht nur ein einheitlicher Rechtsrahmen, sondern auch eine intensive Zusammenarbeit der deutschen und europäischen Aufsichtsbehörden erforderlich.

2.1.2 Richtlinie im Bereich von Justiz und Inneres

Neben der EU-Datenschutz-Grundverordnung ist als zweites grundlegendes Regelungsinstrument die „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr“ (im Folgenden: JI-RL) beschlossen worden. Während der Entwurf der EU-Kommission und die jeweiligen Vorschläge des EU-Parlamentes und des Rates zur Grundverordnung in der Öffentlichkeit diskutiert wurden, fand der Entwurf zur JI-RL weniger Beachtung, obwohl die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hierzu zwei Entschließungen gefasst

hatte.[23] Anders als die Grundverordnung muss die JI-RL erst noch vom deutschen Gesetzgeber in nationales Recht umgesetzt werden, soweit dieses von der Richtlinie abweicht.

Die JI-RL ersetzt den bisher geltenden Rahmenbeschluss in diesem Bereich,[24] der lediglich den grenzüberschreitenden Datenverkehr betraf und in der Praxis zahlreiche Probleme mit sich brachte: Oftmals war bei der Datenerhebung noch nicht absehbar, ob es zu bestimmten personenbezogenen Daten in einer späteren Phase einen grenzüberschreitenden Austausch geben würde. Außerdem räumte der Rahmenbeschluss den Mitgliedstaaten bei der Umsetzung in nationales Recht einen großen Spielraum ein, was zu einem unterschiedlichen Datenschutzniveau in den Mitgliedstaaten führte. Bei bestimmten Datenkategorien war der Rahmenbeschluss zudem nicht anwendbar, weil es hierfür besondere Regelungen in eigenen Vertragswerken gab,[25] was zu einer weiteren Unübersichtlichkeit und zu Fehlerquellen bei der Verwendung der Daten führte.

Durch die JI-RL werden auch rein innerstaatliche Datenverarbeitungen reguliert, sodass eine stärkere Vergemeinschaftung erreicht wird. Allerdings ist der Lückenschluss nicht vollständig. Organe der Europäischen Union, aber auch Institutionen wie Europol und Eurojust werden nicht erfasst.

Inhalt ausgewählter Regelungsfelder

Ziele

Die JI-RL enthält das konfliktträchtige Ziel, die Grundrechte, Grundfreiheiten und Datenschutzrechte zu schützen und gleichzeitig ein hohes Maß an öffentlicher Sicherheit sowie den Austausch personenbezogener Daten zwischen den zuständigen Behörden in der EU zu gewährleisten.[26] Vor diesem Hintergrund ist zu begrüßen, dass eine gewisse Mindestharmonisierung in der JI-RL selbst festgeschrieben wurde.

23 Stellungnahme zur JI-RL vom 11. Juni 2012 sowie „Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen der Datenschutz-Richtlinie im Bereich von Justiz und Inneres“ vom 29. Oktober 2015

24 Rahmenbeschluss 2008/977/JI, ABl. EU Nr. L 350/60 vom 30. Dezember 2008

25 Z. B. DNA-Daten, die im Vertrag von Prüm behandelt wurden; siehe BGBl. I 2006, S. 1458 ff.

26 Art. 1 Nr. 2 JI-RL

Datenverarbeitung
So ist die Einwilligung der Betroffenen kein Rechtfertigungsgrund für die Datenverarbeitung, sodass Drucksituationen für die Betroffenen vermieden werden, da Datenerhebungen, -verarbeitungen und -nutzungen ausschließlich an gesetzlichen und damit objektiven Kriterien zu messen sind. Die Richtlinie selbst legt aber weitgehend nicht fest, welche Datenverarbeitungen erlaubt sein sollen. Sie setzt vielmehr Erlaubnisnormen im Unionsrecht oder im Recht der Mitgliedstaaten voraus. Für Letztere werden nur minimale inhaltliche Anforderungen in der JI-RL festgelegt, sodass zunächst von einem weiten Spielraum bei der Umsetzung für die Mitgliedstaaten ausgegangen werden könnte. Allerdings ist bei der (Nicht-)Ausfüllung dieses Spielraumes von den Mitgliedstaaten das unionsrechtliche Grundrecht auf Datenschutz nach Art. 8 der Grundrechte-Charta[27] zu berücksichtigen.

Betroffenenrechte
Die Kenntnis der Betroffenen darüber, welche ihrer personenbezogenen Daten von welcher Stelle verarbeitet werden, ist ein Kernelement des Rechts auf informationelle Selbstbestimmung. Da bei der Strafverfolgung Datenerhebungen und -verarbeitungen auch ohne Kenntnis der Betroffenen erfolgen können, sind diese auf die Benachrichtigung angewiesen. Ansonsten ist ein effektiver Rechtsschutz nicht möglich, da sie von der (heimlichen) Datenerhebung keine Kenntnis erhalten und so weitere Rechte nicht geltend machen können. Die JI-RL verpflichtet die Mitgliedstaaten, Informationspflichten mit detaillierten Inhaltsanforderungen zu schaffen.[28] Gleichzeitig sind aber auch vielfältige Ausnahmebestimmungen vorgesehen, die zu einer Aushöhlung der Betroffenenrechte führen können.[29] Anders als im bisherigen deutschen Recht darf die Benachrichtigung jedoch nicht mehr deshalb unterbleiben, weil die Betroffenen von den Maßnahmen nur unerheblich betroffen wurden und daher anzunehmen ist, dass sie kein Interesse an der Benachrichtigung haben.[30] Dies hat

27 Art. 8 Charta der Grundrechte der Europäischen Union (Grundrechte-Charta), ABl. EU Nr. C 83/389 vom 30. März 2010
28 Art. 10a JI-RL
29 So ist die Ausnahme, „zur Gewährleistung, dass behördliche oder gerichtliche Ermittlungen, Untersuchungen oder Verfahren nicht behindert werden", in Art. 10a Abs. 3 lit. a JI-RL sehr weit gefasst.
30 Siehe § 101 Abs. 4 Satz 4 StPO und BVerfGE 125, 260, 337

z. B. Auswirkungen auf Massenverfahren in Ermittlungsverfahren wie bei der Funkzellenabfrage.[31]

Keine verpflichtende Bestellung von behördlichen Datenschutzbeauftragten
Die Datenschutzkontrolle der Behörden wird bisher in Deutschland auch durch behördliche Datenschutzbeauftragte wahrgenommen. Häufig kann den Betroffenen bereits durch diese effektiv und schnell weitergeholfen werden. Leider ist es nicht gelungen, diese Institution als unverzichtbares Element für ein effektives Datenschutzregime in der JI-RL zu implementieren. Die JI-RL stellt den Mitgliedstaaten frei, ob sie die Schaffung eines behördlichen Datenschutzbeauftragten verpflichtend vorsehen möchten. Berlin sollte bei der Umsetzung der Richtlinie die bewährte Pflicht zur Bestellung behördlicher Datenschutzbeauftragter auch bei der Polizei und in der Strafjustiz beibehalten.

Datenexport in Drittstaaten
Datenübermittlungen an Behörden und Gerichte in Drittstaaten bedürfen einer Regelung, weil in diesen Staaten häufig geringe Anforderungen an die Verarbeitung gestellt werden und somit Auslandsaufenthalte mit Nachteilen für Betroffene verbunden sein können.

Die JI-RL erlaubt Übermittlungen von personenbezogenen Daten in Drittstaaten, wenn dies zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder zur Strafvollstreckung erforderlich ist und wenn weitere Anforderungen erfüllt werden. U. a. wird auch für diesen Bereich nunmehr die Möglichkeit vorgesehen, dass die Kommission verbindlich festlegen kann, ob das Datenschutzniveau für bestimmte Länder als „angemessen“ bezeichnet wird (Angemessenheitsbeschluss).[32] Die Angemessenheitsbeschlüsse, die auf der Grundlage der EU-Datenschutzrichtlinie von 1995 ergangen sind, gelten für den JI-Bereich nicht. Alternativ kann bei Nichtvorliegen eines solchen Beschlusses eine Übermittlung auf der Grundlage geeigneter Garantien oder weiterer Ausnahmevorschriften stattfinden. Solche Garantien können nur durch ein bilaterales Abkommen sichergestellt werden.

31 Siehe JB 2012, 2.1; JB 2013, 5.4
32 Art. 34 Abs. 1 JI-RL

Datenschutzaufsichtsbehörden
Die Aufsichtsbehörden sind nach der JI-RL als unabhängige Stellen ausgestaltet. Eine im Bereich von Polizei und Justiz zentrale Frage betrifft die Zuständigkeit von Datenschutzbehörden bei der Datenverarbeitung durch Gerichte im Rahmen ihrer gerichtlichen Tätigkeiten. Wir gehen weiterhin davon aus, dass der Ausschluss der Zuständigkeit der Aufsichtsbehörden sich nicht auf Akte der Exekutive bezieht, die nach nationalem Recht unter Beteiligung eines Richters zustande gekommen sind.[33] Die Tatsache, dass z. B. eine Telekommunikationsüberwachung nur auf richterliche Anordnung hin erfolgen darf, ändert nichts daran, dass die Durchführung dieser Maßnahme der Kontrolle durch den Datenschutzbeauftragten des Landes unterliegt.

Die JI-RL lässt die bisherige Ausgestaltung der aufsichtsbehördlichen Befugnisse im deutschen Recht weiterhin zu. Der deutsche Gesetzgeber sollte für eine wirksamere Durchsetzung der Grundrechte von Bürgerinnen und Bürgern die Möglichkeit vorsehen, dass die Datenschutzaufsichtsbehörden bei Verstößen von Behörden gegen das Datenschutzrecht eine gerichtliche Entscheidung erwirken können, wenn diese an ihrer Rechtsauffassung festhalten.

Auch bei der Umsetzung der Richtlinie für Justiz und Inneres in deutsches Recht darf das vorhandene Datenschutzniveau nicht abgesenkt werden. Möglichkeiten zu einer Verbesserung sollte der Gesetzgeber nutzen.

2.2 Große Liebe dank Big Data?

Im Sommer sorgte der Hackerangriff auf die kanadische Seitensprung-Plattform „Ashley Madison“ für Aufsehen. Spätestens die anschließenden Erpressungen der Nutzerinnen und Nutzer und die zum Teil tragischen Reaktionen machten deutlich, dass Dating-Portale über äußerst sensitive Daten verfügen. Ihr Bekanntwerden kann sogar existenzielle Auswirkungen auf das Leben der Betroffenen sowie ihr Umfeld haben. Wir haben im Berichtszeitraum

33 In Deutschland etwa im Hinblick auf Strafverfolgungsmaßnahmen, die einem Richtervorbehalt unterlegen haben.

gemeinsam mit anderen Datenschutzaufsichtsbehörden Dating-Portale und ihren Umgang mit den personenbezogenen Daten überprüft.

In einer koordinierten Prüfaktion mit den Datenschutzaufsichtsbehörden Baden-Württembergs, Bayerns und Hamburgs wurden bundesweit insgesamt 21 Portale einer datenschutzrechtlichen Prüfung unterzogen. Drei der geprüften Portale haben ihren Sitz in Berlin. Die Angebote richten sich an unterschiedliche Zielgruppen. So gibt es etwa Portale für Personen eines bestimmten Alters (z. B. 60+), Akademiker, Angehörige bestimmter Religionsgruppen oder spezifische Angebote je nach sexueller Ausrichtung.

Nutzerinnen und Nutzer von Dating-Portalen werden angehalten, umfangreiche und wahrheitsgemäße Angaben auch zu besonders intimen Bereichen ihres Lebens zu machen. Nur so könne der passende Partnervorschlag gemacht werden. Die Angaben reichen von der sexuellen Präferenz und erotischen Vorlieben über Bildungsniveau, Beruf und Einkommen bis hin zu Charaktereigenschaften, Einstellungen und Interessen, Rauch- und Trinkgewohnheiten, Fitnesslevel, Kinderwunsch und Religionsausübungspraxis. Zum Teil werden anhand ausführlicher Fragebögen explizit psychologische Persönlichkeitsprofile der Nutzerinnen und Nutzer erstellt.

Einen besonderen Fokus haben wir bei der Prüfung daher auf den Umfang der erhobenen Daten, die Umsetzung der Freiwilligkeit der Angaben, den Umgang mit den Daten sowie die Maßnahmen der Datensicherheit zur Verhinderung von Datenpannen gelegt. Die Prüfungen sind noch nicht vollständig abgeschlossen. Einzelne Verbesserungsmaßnahmen müssen mit den Betreibern noch erörtert werden. Zu den wichtigsten Feststellungen bei der Prüfung der Berliner Dating-Portale zählen bislang die folgenden Punkte:

Sensitive Angaben

Bereits mit der Frage, nach welchem Geschlecht die Nutzerinnen und Nutzer suchen, werden Angaben zur sexuellen Orientierung erhoben. Im Rahmen der Profilerstellung werden dann häufig noch weitere sensitive Daten beispielsweise über die Religionsausübung oder übermäßigen Alkoholkonsum abgefragt. Hierbei handelt es sich um besondere Arten personenbezogener Daten.[34]

34 § 3 Abs. 9 BDSG

Diese dürfen nur mit ausdrücklicher Einwilligung der Betroffenen verwendet werden.

Identifizierung und Altersverifikation

Portal-Betreiber fordern zum Teil für Zwecke der Identifizierung und Altersverifikation Kopien des Personalausweises der Nutzerinnen und Nutzer an. Das Anfordern einer Ausweiskopie kann allerdings lediglich in Zweifelsfällen zulässig sein, z. B. wenn bei einem personalisierten Account der Verdacht auf einen Identitätsdiebstahl aufgeklärt werden soll. Selbst in diesem Fall müssen aber zusätzlich die folgenden Voraussetzungen erfüllt sein:

- Eine Kopie wird nur von solchen Personalausweisen angefordert, die keine elektronische Identitätsfunktion (eID-Funktion) besitzen (alter Personalausweis).
- Die Betroffenen werden darauf hingewiesen, dass nicht benötigte Angaben geschwärzt werden können und die Kopien unverzüglich nach der Verifikation vernichtet werden.
- Wenn eine Identifikation oder Altersverifikation erforderlich ist, sollten Dating-Portale sicherstellen, dass die Betroffenen einen Personalausweis mit elektronischer Identitätsfunktion (eID-Funktion) einsetzen können.

Zugriff auf Kommunikationsinhalte

Wir haben festgestellt, dass alle Portalbetreiber Einblick in die Kommunikationsinhalte der Nutzerinnen und Nutzer nehmen. So wird der interne Nachrichtenaustausch zwischen den Nutzerinnen und Nutzern von automatischen Wortfiltern geprüft, die manuelle Prüfungen auslösen können, oder manuelle Prüfungen finden aufgrund von Beschwerden statt. Ein solches Vorgehen kann nur auf Grundlage einer ausdrücklichen Einwilligung der Betroffenen des Portals zulässig sein.

Transparenz

Die durch Datenschutzbestimmungen, allgemeine Geschäftsbedingungen, Nutzungsbedingungen und Einwilligungserklärungen erzielte Transparenz war im Allgemeinen nicht zufriedenstellend. Für die Nutzerinnen und Nutzer ist es schwierig, sich einen umfassenden Überblick über Umfang und Bedeutung der Datenverarbeitungen durch die Dating-Portale zu verschaffen und

einzuschätzen, was auf sie zukommt. Dies wäre jedoch vor der Anmeldung bei einem Portal wichtig, um selbstbestimmt über die Preisgabe von Daten zu entscheiden. Einige Portale bieten die Bildung von Persönlichkeitsprofilen und komplexe Matching-Verfahren zur Bewertung der Persönlichkeit und zur Unterbreitung von Partnervorschlägen an. Die Informationen für die Betroffenen sollten auf diese intensiven Datenverarbeitungen im besonderen Maße eingehen. Zudem muss zu jeder Zeit bei der Nutzung des Portals deutlich erkennbar sein, dass und welche Angaben freiwillig gemacht werden können.

Datensicherheit

Die Login-Verfahren sind teilweise unzureichend. Es wird meist nur ein als „unsicher" zu bewertendes Passwort gefordert, das keine besonderen Anforderungen erfüllen muss. Vor dem Hintergrund des Umfangs und der Sensitivität der im Profil gespeicherten Daten müssen sichere Passwörter und Anmeldeverfahren unterstützt werden, um die Gefahr des Missbrauchs zu minimieren.

Aufgrund des erhöhten Schutzbedarfs der Profildaten halten wir eine Zwei-Faktor-Authentifizierung zur Anmeldung in Dating-Portalen für erforderlich. Sofern ein Passwort als einer dieser Faktoren genutzt wird, hat der Diensteanbieter zu gewährleisten, dass es eine ausreichende Länge und Komplexität aufweist und mit einem wirksamen Hash-Verfahren beim Anbieter gespeichert wird. Zur Veranschaulichung der Passwortstärke können Passwortgütebalken o. Ä. eingesetzt werden. Generell ist zu gewährleisten, dass bei der Umsetzung der Passwort-Vergessen- bzw. Funktion des Zurücksetzens das Passwort der Nutzerinnen und Nutzer nicht im Klartext per E-Mail versendet wird.

Löschung

Keines der von uns geprüften Portale verfügte über ein zufriedenstellendes Löschkonzept. Wird ein Account durch die Nutzerinnen oder den Nutzer gelöscht, sind spätestens nach einem Jahr sämtliche personenbezogenen Daten der Betroffenen vollständig zu löschen bzw. zu sperren.

Betreiber von Dating-Portalen tragen besondere Verantwortung für den Schutz der sensitiven Daten ihrer Nutzerinnen und Nutzer. Datenpannen können existenzielle Folgen haben. Nutzerinnen und Nutzer sollten bei den Anbietern vor allem auf die Gewährleistung von Datensicherheit und Transparenz achten.

2.3 Vernetzte Fahrzeuge und moderne Verkehrstelematik – Chancen und Risiken

Die Digitalisierung unseres Lebens schreitet in den letzten Jahren noch schneller voran. Immer mehr Bereiche des täglichen Lebens werden heutzutage „vernetzt".[35] Diese Entwicklung erfasst auch den Verkehrsbereich. Es gibt inzwischen bereits erste Modelle intelligenter Anzeigen für Wanderbaustellen auf Autobahnen, die selbstständig in der Lage sind, dank Vernetzung ihre Informationen auch an andere Bereiche der Verkehrsinfrastruktur weiterzugeben und somit den Verkehrsfluss zu optimieren. Ebenso werden auch verschiedene neue Verfahren erprobt, mit denen der Autofahrer bereits unterwegs erkennen können soll, wo sich am Zielort freie Parkplätze befinden. Viele Anbieter arbeiten bereits am Verkehrsnetz der Zukunft, welches so viele Verkehrsinformationen wie möglich sammelt, analysiert, mit anderen Messstellen austauscht und auf Basis dieser gigantischen Datenmengen möglichst immer genauere Verkehrsprognosen liefern soll. Die Forschungsinstitute und Technikhersteller werben damit, durch diese Techniken zunehmend Staus vermeiden zu können und den Verkehr immer effizienter zu lenken, wodurch der Fahrer sein Ziel schneller erreicht und letztendlich u.a. auch der Schadstoffausstoß der Fahrzeuge sinken soll.

Parallel dazu verfolgen viele größere Städte den Trend sog. „Smart Cities", in denen die technischen Infrastrukturkomponenten der Stadt in der Lage sind, selbstständig untereinander Informationen auszutauschen, um Prozesse zu beschleunigen und effizienter zu gestalten. So sollen Ampeln selbstständig das Verkehrsgeschehen analysieren, um bei hohem Verkehrsaufkommen mehr „Grüne Welle"-Phasen zu ermöglichen. Busse und Bahnen im öffentlichen Nahverkehr sollen stärker am Bedarf der Kunden orientiert unterwegs sein, um bei hohem Fahrgastaufkommen mehr Verbindungen anzubieten, während in Zeiten schwacher Nachfrage das Angebot automatisch reduziert werden soll.

All diese Techniken erfassen im Lauf der letzten Jahre auch zunehmend einen Gegenstand, den viele Bürger sicherlich noch immer nur begrenzt mit Onlinefähigkeiten und Vernetzung in Verbindung bringen: Das Auto.

35 JB 2013, 2.4

Im selben Maße, wie die Vernetzung der Stadt- und Verkehrsinfrastruktur vorangetrieben wird, geschieht dies auch bei den Fahrzeugen selbst. Einige der neueren Funktionen werden Fahrern moderner Autos durchaus bekannt sein, denn Dienste wie z. B. das Surfen im Internet, der Abruf von E-Mails während der Fahrt oder der Zugriff auf Online-Radiostationen und Musikstreamingdienste sind ebenso wie die Nutzung von Online-Assistenzsystemen zur Unterstützung bei Fahrzeugproblemen bei vielen Herstellern bereits seit einigen Jahren verfügbar. Darüber hinaus ist es heutzutage für viele Fahrer bereits Standard, dass sich das Navigationsgerät dank Echtzeitinformationen aus dem Internet aktualisiert und eine optimierte Route berechnet. Mithilfe von „Event Data Recordern" können Unfälle dokumentiert und möglicherweise rekonstruiert werden.[36]

Hinzu kommt das zunehmende Angebot von Apps, welche speziell auf das Zusammenspiel zwischen dem Smartphone des Anwenders und dessen Auto abgestimmt sind. So lässt sich heutzutage nicht mehr nur das eigene E-Mail-Postfach mit dem Auto synchronisieren oder die Standheizung bequem per App vom Büro aus einschalten. Inzwischen können selbst der Ein- und Ausparkvorgang und sogar die Konfiguration einzelner Fahrwerkskomponenten bei manchen Herstellern komplett vom Endanwender über Apps gesteuert werden.

Ein weiterer Schritt ist die Vernetzung von Fahrzeugen untereinander. Durch sog. C2C- (Car-to-Car) und C2X-Dienste (Car-to-Infrastructure) werden moderne Autos zukünftig in der Lage sein, miteinander zu kommunizieren und Daten auszutauschen. Ziel dieser Techniken ist es, dass entsprechend konfigurierte Fahrzeuge den Fahrer frühzeitig auf Gefahrensituationen und Verkehrsbehinderungen hinweisen können, um die Sicherheit im Straßenverkehr zu erhöhen und gleichzeitig den Verkehrsfluss zu verbessern. So kann z. B. ein vorausfahrendes Auto nachfolgende Fahrzeuge vor einem Stau oder Glatteis warnen. Ebenso ist es möglich, dass Fahrzeuge Hinweise zu Unfällen und Baustellen austauschen, welche dem Fahrer dann im Armaturenbrett oder direkt als Projektion auf der Windschutzscheibe angezeigt werden.

36 Siehe dazu die Empfehlungen der sog. Berlin Group: Datenaufzeichnung in Fahrzeugen (Event Data Recording – EDR): Fragestellungen zu Datenschutz und zum Schutz der Privatsphäre für Regierungen und Hersteller, Dokumentenband 2011, S. 117

Die entsprechenden C2X-Techniken werden bereits seit rund zehn Jahren erforscht. Demnächst werden nun vermutlich erstmals Fahrzeuge auf den Markt kommen, die der Kunde auf Wunsch auch mit C2X-Zusatzdiensten nutzen kann. Ungeklärt ist jedoch in weiten Teilen noch die Frage, wer wann und in welchem Umfang Zugriff auf die Daten der Fahrzeugnutzer und -insassen erhält. Ebenso ist bisher nicht eindeutig geregelt, welche der beteiligten Institutionen die verantwortliche Stelle gegenüber dem Fahrzeughalter ist, sofern dieser eine Auskunft über die erhobenen und gespeicherten Daten verlangt oder es zum Schadensfall (z. B. durch Missbrauch der Daten) kommt.

Ein weiteres mögliches Nutzungsszenario im Bereich der C2X-Kommunikation stellen die Erfassung und Abrechnung von Mautdaten dar. So könnte das System z. B. für die Übertragung von Mautdaten und zur Fahrzeugerfassung an Mautstellen eingesetzt werden. Sollte sich dies technisch realisieren lassen, wäre es möglich, die dann aufgebaute C2X-Infrastruktur anstelle der heute üblichen Mautboxen zu nutzen. Dieser Ansatz wird zusätzlich auch durch das EU-Projekt „eCall“ weiter vorangetrieben. Ab März 2018 soll europaweit ein einheitliches Notrufsystem namens eCall[37] eingeführt werden.[38] Das System muss dann verpflichtend in alle neuen Pkw-Modelle und leichten Nutzfahrzeuge eingebaut werden. Im Fahrzeug montierte Geräte sollen schwere Verkehrsunfälle automatisch an die einheitliche europäische Notrufnummer 112 melden und durch die schneller eingeleiteten Rettungsmaßnahmen helfen, die Zahl der Verkehrstoten zu senken und die Schwere von Verletzungen im Straßenverkehr zu reduzieren. Zusammen mit der ggf. durch eCall eingeführten GSM-basierten Infrastruktur im Fahrzeug sind ebenfalls viele neue Anwendungen im Bereich der Mauterfassung und -abrechnung möglich. Um den Schutz der Privatsphäre der Fahrzeuginsassen zu gewährleisten, ist das System so konzipiert, dass es nur bei schweren Unfällen einen automatischen Notruf über das Mobilfunknetz auslöst. Solange das Fahrzeug unfallfrei im Verkehr unterwegs ist, soll sich das System lediglich in einem Wartemodus (Schlafmodus) befinden und keine Daten – insbesondere keine Bewegungsprofile – aufzeichnen.

Durch die zunehmende Vernetzung von Fahrzeugen ist nicht nur der Schutz der persönlichen Daten des Fahrers und mitunter sogar der weiteren

37 Kurzform für emergency call
38 Siehe JB 2013, 4.1

Fahrzeuginsassen gefährdet. Auch die generelle Sicherheit bei den datenverarbeitenden IT-Systemen gerät zunehmend in das Visier von Kriminellen. Entsprechende Beispiele von kritischen Eingriffen in die Fahrzeugtechnik gab es bereits mehrfach in der Vergangenheit. Bisher handelte es sich hierbei glücklicherweise stets um Angriffe von Hackern, die explizit dazu gedacht waren, Schwachstellen aufzudecken und diese den Herstellern zu melden. Je weiter die Digitalisierung unseres Alltags und somit die Vernetzung im Fahrzeugbereich voranschreiten, desto größer ist jedoch die Gefahr, dass es eines Tages zu bewusst geplanten Angriffen von Kriminellen auf die Fahrzeugtechnik kommt, welche im Extremfall zu einer Gefahr für Leib und Leben werden können.

Die zunehmende Digitalisierung von Kraftfahrzeugen kann sowohl die Verkehrssicherheit erhöhen als auch den persönlichen Komfort beim Autofahren steigern. Gleichzeitig darf nicht außer Acht gelassen werden, dass durch neue technische Möglichkeiten neue Risiken entstehen.

2.4 Bestimmung und Begrenzung der Risiken von Datenverarbeitung

Aus der Praxis

Der Bundestag gehackt. Kreditkartendaten gestohlen. Rechenzentrum fällt durch fehlerhafte Notstromversorgung aus. Dies sind alles Risiken, die sich realisiert haben. Damit lohnt sich eine eingehendere Betrachtung solcher Risiken.

Für das Datenschutzrecht ist jede automatisierte Verarbeitung personenbezogener Daten prinzipiell riskant. Allerdings sind die Risiken differenziert zu bewerten. Das Berliner Datenschutzgesetz (BlnDSG) fordert deshalb,[39] dass vor einer Entscheidung über den Einsatz oder eine wesentliche Änderung der automatisierten Datenverarbeitung die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse und eines Sicherheitskonzeptes zu ermitteln sind.

39 § 5 Abs. 3 BlnDSG

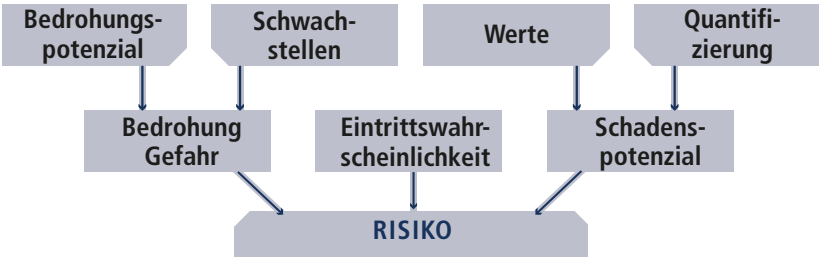
Einordnung von „Risiko“

Der (Online-)Duden definiert „Risiko“ als möglichen negativen Ausgang bei einer Unternehmung, mit dem Nachteile, Verluste und Schäden verbunden sind bzw. als mit einem Vorhaben, Unternehmen o. Ä. verbundenes Wagnis.[40]

Wirtschaftlich beinhaltet eine Investition die Möglichkeit des Verlustes, aber auch die (erhoffte) Möglichkeit eines Gewinns. Wird die Chance mit einbezogen, dann spricht man vom entscheidungsorientierten Risikoansatz, werden nur die negativen Auswirkungen betrachtet, so ist dies der ausfallorientierte Risikoansatz. Auch wenn in letzter Zeit der Chancen-Aspekt an Bedeutung gewinnt, so wird beim Informationssicherheits-Risiko (IT-Risiko) in der Regel der ausfallorientierte Ansatz genutzt. In der Norm DIN ISO/IEC 27000:2011[41] wird das IT-Risiko als „Möglichkeit, dass eine vorhandene Bedrohung die eine Schwachstelle eines Wertes oder einer Gruppe von Werten ausnutzt und dadurch der Institution Schaden zufügen könnte“, definiert.

So wie es unterschiedliche Definitionen von „Risiko“ gibt, so gibt es auch für die Herleitung unterschiedliche Ansätze. Ein in der Literatur häufig aufgeführter quantitativer Ansatz beruht auf der Formel „Risiko = Schadenshöhe × Eintrittswahrscheinlichkeit“. Liegen konkrete Zahlenwerte vor, so kann ein Wert ermittelt werden, der eine Einordnung ermöglicht.

Ein anderer Erklärungsansatz lässt grundsätzliche Betrachtungen für die Ermittlung und die Einordnung des Risikos zu:[42]



40 http://www.duden.de/rechtschreibung/Risiko (Stand: 7. Dezember 2015)
41 Deutsche Version der internationalen Norm ISO/IEC 27000:2009
42 Claudia Eckert, „IT-Sicherheit: Konzepte – Verfahren – Protokolle“, 7. Auflage, Oldenburg Verlag, München 2012

Die unmittelbaren Einflussfaktoren für das Risiko sind die Bedrohung oder Gefahr, die Eintrittswahrscheinlichkeit und das Schadenspotenzial. Sind alle Faktoren hoch, so ist von einem großen Risiko auszugehen. Interessant ist die weitere Betrachtung der Faktoren. Um das Schadenspotenzial ermitteln zu können, müssen die Werte, also die zu schützenden Objekte wie Geschäftsprozesse, Daten, technische Einrichtungen, Beschäftigte oder Reputation mit ihrer quantifizierten Bedeutung wie z. B. Geldwert bestimmt werden. Für die Bedrohung oder Gefahr müssen das Bedrohungspotenzial und die Schwachstellen ermittelt werden. Liegen Schwachstellen vor, so ist deren Relevanz und das Bedrohungspotenzial einzuschätzen. Betrachtet man z. B. Bedrohungen oder Gefahren, die aus Vorsatz entstehen, dann ist das Angreifermodell ein wichtiger Faktor. Dies betrifft u.a. die Motivation wie z. B. Gewinnstreben, Aufmerksamkeit, Spionage und Rache, die Fähigkeiten wie Kenntnisse, Fertigkeiten und Erfahrung und die Ressourcen wie Zeit, Finanzen und Personal. Gibt es Personen oder Organisationen, die ein Interesse daran haben, die Schwachstelle auszunutzen? Handelt es sich um eine Schwachstelle, die auch von einem sog. Skript-Kiddy, also Personen mit geringem IT-Wissen, mit einem vorgefertigten Angriffswerkzeug mit nur geringen Kenntnissen in kurzer Zeit kostengünstig ausgenutzt werden kann oder muss dafür erheblicher Aufwand betrieben werden, für den Experten und sonstige erhebliche Mittel benötigt werden, was nur von Staaten oder großen kriminellen Organisationen realisiert werden kann? Die Bestimmung der Eintrittswahrscheinlichkeit stellt sich häufig als schwierig heraus. Die Wahrscheinlichkeit für das Einschlagen eines Blitzes in ein Rechenzentrumsgebäude ist mittels Statistiken der Blitzschlaghäufigkeiten am jeweiligen Standort gut bestimmbar. Das Auftreten eines Zero-Day-Exploits, d.h. einer Schwachstelle, die erst kürzlich bekannt wurde, ist dagegen statistisch wesentlich schwieriger zu fassen.

Die Schwierigkeit der quantitativen Bestimmung von Risiken eines Systems führt zur verbreiteten Nutzung qualitativer Ansätze (z. B. groß, mittel, klein) bzw. zu einer Vermeidung der unmittelbaren Wahrscheinlichkeitsbetrachtung, wie es das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem Grundschutzansatz vorschlägt.

Risikomanagement

Die vorangegangenen Betrachtungen zeigen die Komplexität des Risikobegriffs. Da auch der Umgang mit Risiken nicht minder komplex ist, wurden

Risikomanagement-Methoden entwickelt, die zudem im Informationssicherheitsmanagement benötigt werden.

Viele dieser Methoden sind in ihrem Aufbau und den grundsätzlichen Schritten ähnlich. Das liegt an der Sinnhaftigkeit der Schritte und an der zunehmenden Anlehnung von Informationssicherheits-/Risikomanagement-Methoden und -normen an die 27000-Reihe der ISO/IEC (International Organization for Standardization) zur IT-Sicherheit.[43] Für das Management von Informationsrisiken werden hier u.a. die Risikomanagement-Methoden spezifiziert.[44] Allgemeinere Aspekte zum Risikomanagement sind in der ISO 31000 standardisiert.

Im Rahmen eines Risikomanagements haben sich folgende Schritte bewährt:[45]

- Festlegung des Kontextes (Context Establishment)
- Risiko-Beurteilung (Risk Assessment)
  - Risiko-Identifikation (Risk Identification)
  - Risiko-Analyse (Risk Analysis)
  - Risiko-Bewertung (Risk Evaluation)
- Risiko-Behandlung (Risk Treatment)
- Risiko-Akzeptanz (Risk Acceptance)

sowie die auf allen Ebenen flankierenden Schritte:

- Risiko-Kommunikation und -Beratung (Risk Communication and Consultation)
- Risiko-Überwachung und -Überprüfung (Risk Monitoring and Review)

Diese Schritte können vereinfacht wie folgt beschrieben werden:

In der Festlegung des Kontextes werden relevante Rahmenbedingungen abgeleitet. U. a. wird der zu betrachtende Ausschnitt wie z. B. ein Teil oder ein

43 Dies gilt ausdrücklich auch für die BSI Standards 100-x.
44 ISO/IEC 27005
45 Nach ISO/IEC 27005 frei übersetzt

ganzes Unternehmen oder ein IT-Verbund festgelegt. Weiterhin wird die maximale Größe des übernehmbaren Risikos (Risiko-Affinität) definiert.

Die Risiko-Identifikation ermittelt alle zu schützenden Werte wie z. B. Geschäftsprozesse, Bedrohungen (Art und Quelle), bestehende und bereits geplante Maßnahmen, Schwachstellen und mögliche Konsequenzen von Sicherheitsvorfällen. Die Risiko-Analyse kann qualitativ und quantitativ oder als Kombination beider Ansätze ausgeführt werden. Wie bereits oben erwähnt, wird aus Komplexitätsgründen häufig der qualitative Ansatz gewählt. Auch die Analysetiefe kann den Randbedingungen angepasst werden. Es werden mögliche Auswirkungen, Eintrittswahrscheinlichkeiten und Risikohöhen untersucht. Die Risiko-Bewertung liefert das Ergebnis der Risiko-Beurteilung, eine Liste mit nach Priorität geordneten Risiken. Nach der Risiko-Beurteilung wird überprüft, ob dieser Schritt zufriedenstellend verlaufen ist. Sollte dies der Fall sein, folgt die Risiko-Behandlung. Sonst wird erneut mit der Festlegung des Kontextes begonnen.

Mit der Risiko-Behandlung werden Möglichkeiten des Umgangs mit den ermittelten Risiken festgelegt. Bei einem ausfallorientierten Ansatz bedeutet dies, dass man nur von den negativen Auswirkungen des Risikos ausgeht.

Daraus resultieren die vier Behandlungsansätze[46]

- Vermeidung (Avoidance)
- Reduktion (Modification)
- Transfer (Sharing)
- Übernahme (Retention)

Die zu einem Risiko führenden Umstände werden beim ersten Ansatz vermieden. So kann ein risikobehafteter Prozessschritt gegen einen sichereren ausgetauscht werden. Bei der Risiko-Reduktion wird das Risiko mittels Maßnahmen auf einen akzeptablen Wert gesenkt. Beim Risiko-Transfer wird das Risiko an eine andere Organisation ausgelagert. So können Risiken versichert oder z. B. die Gewährleistung der Rechenzentrumsverfügbarkeit durch Outsourcing

46 Die deutschen Bezeichnungen entstammen dem BSI Standard 100-3.

an einen Betreiber übertragen werden. Bei der Risiko-Übernahme wird das Risiko getragen. Dabei darf die maximale Größe des übernehmbaren Risikos nicht überschritten werden. Das Ergebnis ist ein Plan für den Umgang mit den Risiken und die Restrisiken.

Sollte das Ergebnis nicht akzeptabel sein, wird der Schritt der Risiko-Behandlung wiederholt oder erneut mit der Festlegung des Kontextes begonnen. Im positiven Fall wird zum Schritt Risiko-Akzeptanz weitergegangen.

Im Schritt der Risiko-Akzeptanz muss sich das verantwortliche Management mit den Restrisiken befassen und diese bewusst zur Kenntnis nehmen. Dies gilt insbesondere für den Fall, dass die Restrisiken eigentlich die max. Größe des definierten übernehmbaren Risikos überschreiten. Das Ergebnis ist schriftlich zu fixieren.

Die Schritte der Risiko-Kommunikation und -Beratung sowie Risiko-Überwachung und -Überprüfung dienen u.a. der Transparenz des Risikomanagement-Prozesses und der Qualitätssicherung desselben.

Nach Abschluss dieses Prozesses ist ein Risikomanagement-Team eingesetzt. Innerhalb der gewählten Grenzen sind die relevanten Geschäftsprozesse und weiteren Werte bekannt. Die dazugehörigen Schadensszenarien mit ihren Eintrittswahrscheinlichkeiten haben zu einer priorisierten Liste von Risiken geführt. Daraus wurde ein Plan für den Umgang mit den Risiken abgeleitet, und Restrisiken sind eindeutig bekannt. Der nun transparente Status ermöglicht einen verantwortungsvollen Umgang mit den Risiken. Besonders wichtig ist die durchgehende Dokumentation des gesamten Prozesses, sodass auch Außenstehende alle Schritte und Entscheidungen nachvollziehen können.

Die beste Risikomanagement-Methode muss jede Organisation individuell ermitteln. Auch der qualitative Ansatz des BSI hat seine Vorteile. So ist insbesondere durch den Einsatz der Grundschutzkataloge eine gute Vergleichbarkeit von Ergebnissen gegeben, wobei die Grundschutzkataloge auch für Risikomanagement-Prozesse nach ISO/IEC 27005 bzw. Informationssicherheitsmanagement nach ISO/IEC 27001 verwendet werden können.

2.5 Risiken werden real: Datenlecks

Aus der Praxis

Durch öffentlichkeitswirksame Hackerangriffe ist das Thema IT-Sicherheit 2015 stärker in den Fokus der Öffentlichkeit gerückt. Die Konsequenzen solcher Angriffe für die Nutzerinnen und Nutzer sind im Fall des kanadischen Seitensprungportals „Ashley Madison“[47] besonders offenbar geworden. Auch in Berlin mehren sich die Fälle, in denen große Datenbanken das Ziel von Hackern werden, die versuchen, die betroffenen Unternehmen mit den gestohlenen Datensätzen oder der Veröffentlichung des Datenhacks zu erpressen. Jedenfalls bei den Unternehmen, die die Betroffenen über den „Datenabfluss“ unterrichten, stellt das Drohen mit Veröffentlichung kein taugliches Erpressungsinstrument mehr dar.

Zu diesen Fällen zählt auch der Hackerangriff auf die Webseite eines Theaters. Durch eine sog. „SQL-Injection“, d.h. eine Übernahme der Datenbank, wurden mehr als 17.000 Datensätze mit Kreditkarten- und Bankdaten erlangt, die die Kundinnen und Kunden bei der Bestellung von Theater-Tickets angegeben hatten. Nach dem Angriff wurde das Theater von dem mutmaßlichen Hacker per E-Mail zur Zahlung von sog. Bitcoins (einer digitalen Währung) aufgefordert. Das Verfahren ist bei uns noch nicht abgeschlossen. Unabhängig von dem Hackerangriff haben wir bereits jetzt erhebliche Mängel bei der technisch-organisatorischen Absicherung der Daten festgestellt. So waren sowohl die Zahlungs- als auch die Login-Daten (Benutzernamen und Passwörter) im Klartext in der Datenbank abgelegt.

Ebenfalls betroffen von einem Hackerangriff war ein Webhosting-Unternehmen mit Nutzerinnen und Nutzern im gesamten Bundesgebiet. Durch den Angriff auf das interne System wurden sowohl Bestandsdaten (z. B. Zahlungsdaten) als auch Zugangsdaten (Benutzernamen und Passwörter) der Kundinnen und Kunden erbeutet. Mit den Zugangsdaten war der Weg frei zu den beim Hoster abgelegten Inhalten der Betroffenen. Auch dieses Unternehmen erhielt eine E-Mail mit der Forderung, Bitcoins zu bezahlen. Sowohl die Betroffenen als auch wir als Aufsichtsbehörde wurden durch das Unternehmen erst spät informiert: Ihm war der Hackerangriff länger als ein Monat bekannt, bevor die Unterrichtung erfolgte. Auch dieses Verfahren ist noch nicht abgeschlossen.

47 Siehe 2.2

Der Schwerpunkt der Meldungen über eine unrechtmäßige Kenntniserlangung von Daten durch Dritte[48] liegt nach wie vor im nicht-öffentlichen Bereich. Von der Versendung von Partei-E-Mails an einen offenen Verteiler bis zum Diebstahl des Laptops eines Psychiaters war die Bandbreite der Vorfälle groß. Eine Meldung erhielten wir von einem großen Unternehmen der Chemiebranche: Eine Mitarbeiterin der Personalabteilung nutzte die Bankdaten einer Kollegin für private Einkäufe im Internet und legte mit den Daten sogar ein Konto bei einem Zahlungsdienstleister an. Als Mitarbeiterin des Personalbereiches hatte die Beschäftigte zwar berechtigten Zugriff auf die Daten. Die Nutzung der Informationen hingegen war missbräuchlich. In der Regel können organisatorische Maßnahmen wie die Verpflichtung der Beschäftigten, das Datengeheimnis zu wahren,[49] das Risiko von „Innenangriffen" verringern. In diesem Fall konnte der Missbrauch dadurch allerdings nicht verhindert werden.

Im öffentlichen Bereich erfolgten nur wenige Meldungen. Durch die Presse ging das Rückmeldeverfahren der Technischen Universität Berlin. Die Versendung der Rückmeldeinformationen per E-Mail war fehlerhaft, sodass die Studierenden nicht nur die eigenen Rückmeldeinformationen erhielten, sondern auch sämtliche Rückmeldeinformationen, die an die jeweiligen Vorgängerinnen oder Vorgänger im Versendeprozess gesendet worden waren. Nach ca. 1.800 versendeten E-Mails fiel der Missstand auf und der Prozess wurde abgebrochen. In den meisten Fällen waren ausschließlich die Anschriften der Studierenden in den Rückmeldeinformationen enthalten. Zum Teil enthielten die Anschreiben allerdings auch individuelle Studiumshinweise z. B. zu fehlenden Nachweisen oder Exmatrikulationen. Die Betroffenen wurden in einem abgestuften Verfahren benachrichtigt. Alle Studierenden sind nach dem Vorfall erneut auf die erforderliche Rückmeldung hingewiesen worden. Auf unsere Anregung hin wurden dabei keine persönlichen Informationen versendet. Vielmehr wurden die Studierenden aufgefordert, sich in das Studierendenportal einzuloggen und in ihren persönlichen Konten nachzusehen, was für die Rückmeldung erforderlich ist.

48 Informationspflichten nach § 42 a BDSG, § 15 a TMG, § 83 a SGB X, § 18 a BlnDSG
49 § 5 BDSG

Die Fälle zeigen zum Teil eklatant, wie wichtig es ist, aktuelle Software einzusetzen, die ständig auf bekannte Sicherheitsmängel überprüft und entsprechend „gepatcht" (geflickt) wird. Die Folgen eines Angriffs auf die Systeme können dadurch deutlich abgemildert oder gar verhindert werden. Gegen das Auslesen von Daten bei Verlust der Hardware, z. B. Diebstahl eines Arztrechners, helfen Verschlüsselungsmaßnahmen, die mit einfachen Mitteln umgesetzt werden können.

2.6 Datenschutz made in Berlin

Berlin „hat europaweit die meisten Start Ups".[50] In unserer Praxis haben wir regelmäßig mit ihnen zu tun. Mehrheitlich geht es um Beratungen zu datenschutzrechtlichen Fragen. Damit haben sich die neu gegründeten Unternehmen oft nicht beschäftigt. So gab es vor der ersten Beschwerde noch keine Auskunftsersuchen von Kunden, weswegen das erste Auskunftsersuchen nicht oder unvollständig beantwortet wurde. Häufig wird auch die Frage nach dem Löschkonzept dahingehend beantwortet, dass das Unternehmen noch nicht lang genug existiere, als dass man in die Verlegenheit komme, Daten löschen zu müssen. Diese Annahme ist nicht zutreffend: Personenbezogene Daten sind zu löschen, sobald sie nicht mehr erforderlich sind. Anderes gilt nur, wenn die Aufbewahrung gesetzlich vorgeschrieben ist, wie etwa im Falle von steuerrechtlichen Aufbewahrungsfristen. Aufbewahrungspflichtige Daten unterliegen einer engen Zweckbindung, müssen daher u. U. datenschutzrechtlich gesperrt, d.h. aus den operativen Systemen entfernt werden.

Erfreulich ist aber, dass eine ganze Reihe von Start Up-Unternehmen den Schutz der Privatsphäre zu ihrem Geschäftsmodell gemacht hat. Bei fünf Diensten, die innovative Konzepte verfolgen, haben wir uns die Außendarstellung und Funktionalitäten angeschaut:

Bei **Hoccer** handelt es sich um einen Messaging-Dienst für Smartphones, der unabhängig von Telefonnummern funktioniert. Dies hat den Vorteil, dass

50 So der Senator für Finanzen, Dr. Kollatz-Ahnen, SZ vom 31. Dezember 2015/1. Januar 2016, S. 6

Nutzer ihre Telefonnummer nicht herausgeben müssen und insbesondere keine datenschutzrechtlich besonders problematische Funktion zum Hochladen des gesamten Telefonbuches angeboten werden muss. Da das Finden der Chatpartner so schwieriger ist, gibt es eine Funktion, die andere Hoccer-Nutzer in der Nähe anzeigt, wenn sie die Funktion ebenfalls eingeschaltet haben. Die dafür notwendige Standortbestimmung beschränkt sich auf diese Augenblicke.

Selbstverständlich werden die übermittelten Daten per Ende-zu-Ende-Verschlüsselung geschützt. Die Software ist Open-Source und der Server, bei dem trotz der Verschlüsselung prinzipiell noch (pseudonyme) Verbindungsdaten anfallen, steht in Deutschland. Leider ist der Dienst noch nicht sehr verbreitet.

Posteo (posteo.de) ist ein Web-E-Mail-Dienst mit den üblichen Funktionen. Im Unterschied zu anderen Webmailern ist die Nutzung kostenpflichtig, dafür wird auf jegliche Identifizierungsdaten und auf die Analyse des Nutzungsverhaltens oder gar der Inhalte der Nachrichten verzichtet. Dies beginnt damit, dass die Nutzenden ihre Postfächer unter Pseudonym anlegen: Es werden abgesehen von der gewünschten E-Mail-Adresse und einem Passwort keinerlei Daten verpflichtend erhoben. Auch die Prepaid-Bezahlung kann per Bareinzahlung vollständig anonym erfolgen. Wählt man personenbezogene Zahlverfahren, wird zumindest die über einen Code hergestellte Verknüpfung zum E-Mail-Postfach unmittelbar nach Zahlungseingang gelöscht.

Neben der konsequenten Umsetzung aller Möglichkeiten der Transportverschlüsselung beim Versenden und Empfangen der E-Mails sowie beim Zugriff auf die Weboberfläche wird auch eine optionale Ende-zu-Ende-Verschlüsselung mit PGP und S/MIME unterstützt. Eine Besonderheit ist die Funktion zum Grund-Verschlüsseln von Postfachinhalt und Adressbuch: Auf einfache Weise lässt sich dafür sorgen, dass selbst unverschlüsselt empfangene E-Mails verschlüsselt gespeichert werden. Im Gegensatz zu der Verschlüsselung bei PGP und S/MIME werden auch die Verkehrsdaten im E-Mail-Kopf verschlüsselt. Die Entschlüsselung erfolgt – transparent im Hintergrund – nur in dem Augenblick, in dem die jeweilige E-Mail abgerufen wird. Bei Nutzung dieser Funktion ist die Wahl eines sicheren und längeren Passwortes besonders wichtig.

Mynigma (mynigma.org) hingegen ist ein Ansatz, den Einsatz von Ende-zu-Ende-Verschlüsselung bei E-Mails zu erhöhen, indem der Schlüsselaustausch vereinfacht wird. Dies geschieht, indem mit der ersten E-Mail der öffentliche Schlüssel automatisch mitgeschickt wird. Ein solches Modell nennt sich „Trust on first use", d.h. man vertraut darauf, dass die erste Kommunikation unmanipuliert erfolgt. Alle folgenden E-Mails werden verschlüsselt und signiert übertragen. Um Angriffe auf die erste E-Mail zu erkennen, kann man optional den Fingerprint des ausgetauschten Schlüssels vergleichen.

Neben dem diskussionswürdigen Sicherheitsmodell, welches man eigentlich nur als zusätzliches Sicherheitsfeature, z. B. neben einer Zertifizierungsinfrastruktur einsetzt, stellt hier die Anforderung, dass beide Kommunikationspartner einen E-Mail-Client verwenden müssen, der entsprechende Erweiterungen enthält, ein praktisches Problem dar.

Androlyzer ist eine für Android-Smartphones verfügbare App, die in der Lage ist, den Programmcode anderer Apps zu analysieren. Dadurch wird auf möglicherweise kritische Aspekte hingewiesen. Dies können umfangreich eingeräumte Zugriffsrechte auf z. B. sensitive Daten, GeräteIDs, Kontaktdaten oder Fotos sowie auf durch Sensoren wie etwa Kamera, GPS (Standort) oder Mikrofon erhobene Daten sein. Auch Funktionen wie die Verwendung von Bibliotheken werden festgestellt, die bekannt für den Einsatz von Tracking oder gar Spionagetechniken sind (z. B. Bibliotheken für verhaltensbasierte Werbung). Zudem erfolgt eine Analyse des Programmablaufs, sodass z. B. erkannt werden kann, wenn sensitive Daten erhoben werden, um diese an Server des Unternehmens oder Dritte zu übermitteln. Trotz Markierung in Ampelfarben erfordert die Auswertung erhebliches Fachwissen, zumal manche Funktionen durchaus einen vom Nutzer erwünschten Zweck erfüllen können. Auf dem Webangebot (androlyzer.com) sind die Ergebnisse bereits durchgeführter Analysen einsehbar. Bei iOS-Geräten erhalten installierte Apps keine Rechte, um auf den Programmcode anderer Apps zuzugreifen. Für unmanipulierte iOS-Geräte ist Androlyzer daher nicht realisierbar.

Bei **Whispeer** (whispeer.de) handelt es sich um ein soziales Netzwerk, das besonderes Augenmerk darauf legt, Profilinhalte nur bestimmten Gruppen von Nutzern (Kreisen) zugänglich zu machen. Nutzer können frei definieren, für wen ein bestimmter Inhalt zugänglich sein soll. Erreicht wird dies durch

Verschlüsselungsverfahren. Selbst für den Betreiber des Dienstes bleiben all jene Inhalte verborgen, die nicht vom Nutzer für alle Nutzer des sozialen Netzwerkes zugänglich festgelegt wurden. Dabei erfolgt die Ver- und Entschlüsselung bereits im jeweiligen Browser, also bereits vor dem Hochladen der Inhalte auf die Server bzw. nach dem Herunterladen. Bei dem eingesetzten Verfahren handelt es sich um eine relativ bekannte, auf Javascript basierende Open-Source-Kryptobibliothek. Die Kryptografie arbeitet transparent im Hintergrund, sodass das Netzwerk ebenso leicht zu nutzen ist wie andere soziale Netzwerke.

Die Nutzung unter Pseudonym wird nicht nur ermöglicht,[51] sie ist sogar voreingestellt. Alle weiteren Profilinhalte sind frei gestaltbar, und der Zugriff kann differenziert auf bestimmte Nutzergruppen beschränkt werden. Die Server des Angebotes befinden sich ausschließlich in Deutschland, und die Datenübertragung erfolgt SSL-verschlüsselt mit sicheren Algorithmen. Die Informationen zum Datenschutz sind hingegen ergänzungsbedürftig. Insbesondere sollte dargestellt werden, ob bzw. in welchem Umfang eine Protokollierung der Verkehrsdaten erfolgt.

Die Angebote zeigen beispielhaft, dass es möglich ist, jede Art von Diensten so zu gestalten, dass sie die Privatsphäre der Nutzer besonders gut schützen, wenn man bereits bei der Konzeption Datenschutzaspekte nicht nur berücksichtigt, sondern zu einem wesentlichen Aspekt des Produktes macht. Insbesondere Datenminimierung und der konsequente Einsatz von Verschlüsselung sind ein entscheidendes Werkzeug.

Datenschutz ist durchaus ein erfolgreiches Verkaufsargument, wie das Beispiel Posteo zeigt. Aber auch die anderen Geschäftsideen machen deutlich, dass in der europäischen „Start Up-Hauptstadt Berlin" der Datenschutz innovationsfördernd wirkt.

51 § 13 Abs. 6 Telemediengesetz

3 Inneres und Sport

3.1 Steinige Prüfung bei den Gemeinsamen Terrorabwehrzentren

Im letzten Jahr berichteten wir über unsere begonnene Kontrolle im Gemeinsamen Terrorismusabwehrzentrum (GTAZ) und im Gemeinsamen Extremismus- und Terrorismusabwehrzentrum (GETZ), in dem neben 38 anderen Sicherheitsbehörden des Bundes und der Länder auch die Berliner Verfassungsschutzbehörde und das Landeskriminalamt vertreten sind.[52] Neben den genannten Schwierigkeiten mit der Auswertung der Protokolle mussten wir nun elf Monate auf die Übersendung der notwendigen Zusammenarbeitsrichtlinie im Bereich der Nachrichtendienste warten. Die Prüfung konnte daher noch nicht abgeschlossen werden. Die vorstehend genannte Verwaltungsvorschrift enthält für die beteiligten Dienste maßgebliche Regelungen zum Informationsaustausch, die faktisch die beteiligten Stellen ebenso binden wie die gesetzlichen Regelungen zur Datenübermittlung. Inwieweit allerdings eine Verwaltungsvorschrift und die allgemeinen Übermittlungsbefugnisse als Rechtsgrundlagen für den Informationsaustausch im GTAZ und im GETZ ausreichen, wird noch zu prüfen sein.

Die Begleitumstände zur Übersendung der Richtlinie gestalteten sich folgendermaßen: Nachdem wir die Verfassungsschutzbehörde im August 2014 aufgefordert hatten, uns die als Verschlusssache eingestuften Vorschriften zu übersenden, wandte sich diese an die Innenministerkonferenz (IMK) mit der Bitte, das hierfür erforderliche Freigabeverfahren einzuleiten. Die Verfassungsschutzbehörde sah sich nicht in der Lage, eigenständig zu entscheiden, ob bzw. in welcher Form uns diese Vorschrift zur Verfügung gestellt werden konnte.

Im Dezember 2014 mahnten nicht nur wir und der Vorsitzende der Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Übersendung der Zusammenarbeitsrichtlinie unter Hinweis auf die im Bundesdatenschutz- und

52 JB 2014, 2.3

den Ländergesetzen geregelte Unterstützungspflicht öffentlicher Stellen an. Inzwischen hatten weitere Aufsichtsbehörden um die Übersendung dieser Vorschrift für ihre Kontrolltätigkeit im Bereich der Nachrichtendienste gebeten. Eine unverzügliche Übersendung erfolgte jedoch auch weiterhin nicht. Das bei der IMK eingeleitete Freigabeverfahren war ausgesetzt worden, weil diese eine grundsätzliche Klärung der Frage des Umgangs mit Herausgabeverlangen zu ihren Dokumenten anstrebte. Im Zuge dessen beauftragte die IMK einen Gutachter, der die Frage klären sollte, wie Herausgabe- und Auskunftspflichten gegenüber Parlamentsabgeordneten, Privaten sowie Datenschutzbeauftragten hinsichtlich nicht freigegebener Beschlüsse und Berichte der IMK rechtlich zu bewerten sind, da die informatorische Rechtsstellung der IMK bislang ungeklärt war.[53] Naturgemäß beschäftigte sich das Gutachten daher mit Ansprüchen nach den Informationsfreiheitsgesetzen, die für unsere vorliegende Kontrolle jedoch nicht relevant waren.[54] Zudem sind unsere Befugnisse bei einer Kontrolle bereits gesetzlich geregelt. Der Gutachter konnte daher nur auf diese gesetzliche Regelung verweisen.[55]

Weder sollte mit unserer Aufforderung, die Vorschrift zu übersenden, eine Aufhebung der Einstufung als Verschlusssache, noch das berechtigte Anliegen der IMK unterlaufen werden, selbst zu entscheiden, inwieweit sie einzelne Beschlüsse von der Veröffentlichung ausnimmt. Bei einer solchen Kontrolltätigkeit ist es eine Selbstverständlichkeit, dass Regelungen zur Verschlusssachenanweisung von uns strikt beachtet werden.

Das fast einjährige Warten auf eine für unsere Kontrolltätigkeit erforderliche Vorschrift ist nicht hinnehmbar und widerspricht der im Gesetz geregelten Unterstützungspflicht.[56]

53 Gutachten von Prof. Dr. Mario Martini im Auftrag der Innenministerkonferenz vom 10. März 2015: Die Innenministerkonferenz als Gegenstand des Informationsrechts

54 § 38 Gesetz über den Verfassungsschutz in Berlin i.V. m. § 28 Abs. 1 BlnDSG

55 Martini, a. a. O., S. 132, Fn. 833

56 § 28 BlnDSG

3.2 Übersichtsaufnahmen durch die Polizei bei Demonstrationen

Aus der Praxis

2013 wurde eine Rechtsgrundlage für die Anfertigung von polizeilichen Übersichtsaufnahmen bei Versammlungen unter freiem Himmel und Aufzügen geschaffen.[57] Diese Regelung hat der Verfassungsgerichtshof des Landes Berlin für verfassungskonform erklärt.[58] Allerdings betonte er, es müsse bei der Anwendung der Norm insbesondere gewährleistet sein, dass Übersichtsaufnahmen und individualisierte Aufnahmen von getrenntem Personal mit unterschiedlicher Technik angefertigt und regelmäßige Schulungen der eingesetzten Beamtinnen und Beamten durchgeführt werden.[59]

Wir haben anlässlich der Demonstrationen am 1. Mai die praktische Umsetzung der neuen Bestimmung sowie der diesbezüglichen Hinweise des Verfassungsgerichtshofs vor Ort kontrolliert. Hierzu haben wir das Lagezentrum sowie die zentrale Stelle für Videoaufzeichnungen beim Polizeipräsidenten besichtigt und den Einsatz einer stationären Kamera überprüft. Ein Verstoß gegen datenschutzrechtliche Vorgaben wurde nicht festgestellt.

Die Durchführung von Übersichtsaufnahmen durch die Polizei erfolgte sehr restriktiv. Die Aufnahmen wurden in vier Fällen vom Polizeiführer aufgrund der Größe der Versammlung und der damit verbundenen Unübersichtlichkeit zur polizeilichen Lagebeurteilung angeordnet und entsprechend dokumentiert. Die Versammlungsleitung wurde nach Aussage der Polizei bereits im Kooperationsgespräch über die Möglichkeit der Durchführung von Übersichtsaufnahmen informiert und vor Beginn der Maßnahmen über den tatsächlichen Einsatz nochmals persönlich durch eine Verbindungskraft der Polizei in Kenntnis gesetzt. Gleichzeitig wurde die Durchführung der Übersichtsaufnahmen via Twitter bekannt gegeben.

Die kontrollierte stationäre Kamera enthielt kein Speichermedium und war außerhalb der Durchführung der Übersichtsaufnahmen deutlich sichtbar zu

57 § 1 Abs. 2 des Gesetzes über Aufnahmen und Aufzeichnungen von Bild und Ton bei Versammlungen unter freiem Himmel und Aufzügen; siehe JB 2013, 3.5
58 VerfGH Berlin, Urteil vom 11. April 2014, 129/13
59 a.a.O., Rn. 63

Boden gesenkt. Ein Heranzoomen der Umgebung war mit der Kamera zwar technisch, jedoch aufgrund des Aufstellungsortes praktisch schwer möglich und wurde nach unserer Kenntnis auch nicht durchgeführt. Das geprüfte Kamerateam trug Warnwesten in Leuchtfarben. Für die Übersichtsaufnahmen und die individualisierten Aufnahmen waren verschiedene Teams mit jeweils eigener Kameraausrüstung zuständig. Nach Auskunft der Polizei sind die eingesetzten Dienstkräfte hoch spezialisiert und kennen ihren Einsatzbereich seit Jahren sehr genau. Zur Anfertigung von Übersichtsaufnahmen bei Demonstrationen habe eine gesonderte Schulung stattgefunden. Darüber hinaus besteht eine detaillierte Handlungsanleitung zur Regelung solcher Maßnahmen.

Nach Abschluss unserer Prüfung empfahlen wir der Polizei, aus Gründen der Transparenz bei Übersichtsaufnahmen, die über einen längeren Zeitraum erfolgen, die Versammlungsleitung in regelmäßigen Abständen über die Fortdauer der jeweiligen Maßnahme bzw. deren Beendigung zu informieren. Zudem sollte die Versammlungsleitung von jeder einzelnen Anordnung einer Maßnahme in Kenntnis gesetzt werden und eine entsprechende Dokumentation auf dem Formblatt erfolgen. Weiterhin sollte zur besseren Nachvollziehbarkeit die Uhrzeit der Veröffentlichung der Anordnungen von Übersichtsaufnahmen im Internet ebenfalls dokumentiert werden. Die Polizei kam unseren Empfehlungen nach.

Die Anfertigung von polizeilichen Übersichtsaufnahmen bei Demonstrationen stellt eine erheblich Beschränkung des Grundrechts auf Versammlungsfreiheit dar und ist nur in einem eng begrenzten Rahmen zulässig. Die festgestellte Praxis entspricht den gesetzlichen Vorgaben.

3.3 Polizeiliche Auskunftsersuchen per unverschlüsselter E-Mail

Ein E-Mail-Anbieter teilte uns mit, dass das Landeskriminalamt 2014 ein Ersuchen um Bestandsdatenauskunft,[60] das personenbezogene Daten enthielt, per unverschlüsselter E-Mail an ihn gerichtet habe, und bat um

60 § 100j Strafprozessordnung (StPO) i.V. m. § 113 Telekommunikationsgesetz (TKG)

Unterstützung beim Durchsetzen der Einhaltung der datenschutzrechtlichen Vorgaben bei manuellen Auskunftsersuchen dieser Art durch die Polizei.

Das Auskunftsersuchen sei zunächst an das allgemeine Support-Postfach gesendet worden. Später sei es zusätzlich an die für solche Anfragen bestimmte E-Mail-Adresse übermittelt worden, auf die nur die hierfür zuständigen Beschäftigten Zugriff haben. In beiden Fällen sei die Nachricht nicht verschlüsselt gewesen, obwohl der E-Mail-Anbieter öffentliche Schlüssel für die Verschlüsselungsverfahren S/MIME und PGP auf seiner Webseite u.a. im Impressum bereitstelle.

Wir haben die Eingabe zum Anlass genommen, die generelle Praxis polizeilicher Auskunftsersuchen an Telekommunikationsanbieter zu kontrollieren, und die Polizei hierzu um Stellungnahme gebeten. Die Polizei teilte uns mit, dass es neben allgemeinen polizeiinternen Vorschriften zur Nutzung von Informationstechnik und zum Schutz personenbezogener Daten mit Vorgaben zur Verschlüsselung von E-Mails spezielle Arbeitshinweise zur Bestandsdatenauskunft gibt, die die gesetzlichen Bestimmungen näher erläutern und Regeln zur praktischen Durchführung von Auskunftsersuchen enthalten.

Entsprechend unserer Empfehlung wurden diese Arbeitshinweise durch die hervorgehobene Information ergänzt, dass Auskunftsersuchen per E-Mail, die Bestandsdaten betreffen, ausnahmslos verschlüsselt werden müssen. Auf unsere Bitte hin wurde zudem die zuständige Abteilung des Landeskriminalamtes darüber informiert, dass der betroffene E-Mail-Anbieter eine spezielle E-Mail-Adresse für Meldungen von Verdacht auf Missbrauch eingerichtet hat, die auch für polizeiliche Auskunftsersuchen genutzt werden soll.

Es ist lobenswert, wenn E-Mail-Anbieter technische und organisatorische Voraussetzungen schaffen, die es der Polizei erlauben, möglichst unkompliziert und gleichzeitig datenschutzgerecht ihrer Ermittlungstätigkeit nachzugehen. Umso wichtiger ist es, dass die Polizei durch Nutzung dieser Einrichtungen das Engagement solcher E-Mail-Anbieter unterstützt.

3.4 Entwurf eines Anti-Doping-Gesetzes

Die Bundesregierung hat im Frühjahr den Entwurf eines Gesetzes zur Bekämpfung von Doping im Sport (Anti-Doping-Gesetz) vorgelegt.[61] Der Entwurf ist im Dezember in Kraft getreten.[62] Mit dem Gesetz wird der Zweck verfolgt, den Einsatz von Dopingmitteln und -methoden im Sport zu bekämpfen, um die Gesundheit der Sportlerinnen und Sportler zu unterstützen, die Fairness und Chancengleichheit bei Sportwettbewerben zu sichern und damit zur Erhaltung der Integrität des Sports beizutragen. Das Gesetz enthält eine Vielzahl datenschutzrechtlicher Vorschriften, mit denen die informationellen Maßnahmen bei der Durchführung von Doping-Kontrollen auf eine gesetzliche Grundlage gestellt werden.

Wir haben in einer gemeinsamen Stellungnahme mit den Datenschutzaufsichtsbehörden von Mecklenburg-Vorpommern, Rheinland-Pfalz und Schleswig-Holstein gegenüber dem Gesetzgeber deutlich gemacht, dass wir den vom Bundeskabinett beschlossenen Entwurf für verfassungswidrig halten.

Es ist zwar zu befürworten, dass die erheblichen Eingriffe in das Recht auf informationelle Selbstbestimmung nicht mehr durch eine Einwilligung der Sportlerinnen und Sportler legitimiert werden sollen. Zu kritisieren ist jedoch, dass der Gesetzgeber bezüglich der Verarbeitung personenbezogener Daten lediglich auf das „Dopingkontrollsystem“ verweist und die Ausgestaltung dieses Systems vollständig nichtstaatlichen Organisationen wie NADA[63] und WADA[64] überlässt. Hier steht der Gesetzgeber noch immer in der Pflicht, selbst Regelungen zu treffen. Es fehlt eine strenge Zweckbindung der erhobenen Gesundheitsdaten und anderer sensitiver Daten. Auch fehlt es an der notwendigen Transparenz für die Betroffenen. Auskunfts-, Berichtigungs-, Benachrichtigungs- und Widerspruchsrechte für die Betroffenen sind ebenfalls nicht vorgesehen.

Die Notwendigkeit eines internationalen „Dopingkontrollsystems“ wird auch von den Datenschutzaufsichtsbehörden anerkannt. Allerdings muss es das Recht

61 BT-Drs. 18/4898 vom 13. Mai 2015
62 BGBl. I, S. 2210
63 Nationale Anti Doping Agentur Deutschland
64 Welt-Anti-Doping-Agentur

der Sportlerinnen und Sportler auf informationelle Selbstbestimmung wahren. Wir haben die gemeinsame Stellungnahme dem Senator für Inneres und Sport zur Kenntnis gegeben und ihn gebeten, unsere datenschutzrechtlichen Kritikpunkte in das weitere Gesetzgebungsverfahren im Bundesrat einzubringen. Auch wenn unsere Kritik von der Senatsverwaltung für Inneres und Sport nicht in allen Punkten geteilt wurde, so war es positiv, dass unser Hinweis auf eine fehlende gesetzliche Regelung der Datenübermittlung von der NADA an die Strafverfolgungsbehörden im Bundesrat aufgegriffen wurde und immerhin Eingang in die Stellungnahme des Bundesrates gefunden hat. Das verabschiedete Gesetz verzichtet allerdings auf die notwendige Übermittlungsbefugnis.

Leider hat es der Bundesgesetzgeber versäumt, bei der Verabschiedung des dem Schutze der Sportlerinnen und Sportler dienenden Anti-Doping-Gesetzes deren Datenschutzrechte ausreichend zu berücksichtigen.

4 Justiz und Verbraucherschutz

4.1 Vorratsdatenspeicherung – eine unendliche Geschichte?

Im April 2014 hatte der Europäische Gerichtshof (EuGH) die Richtlinie zur Vorratsdatenspeicherung[65] mit der Begründung für ungültig erklärt, dass sie einen Eingriff in die Grundrechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten ermöglicht, der von großem Ausmaß und als besonders schwerwiegend anzusehen ist und sich nicht auf das absolut Notwendige beschränkt.[66] Bereits 2010 hatte das Bundesverfassungsgericht das deutsche Gesetz zur Umsetzung der Richtlinie zur Vorratsdatenspeicherung für verfassungswidrig erklärt.[67]

Beide Urteile hielten den deutschen Gesetzgeber nicht davon ab, im Oktober 2015 erneut ein Gesetz zu beschließen, das die anlasslose Speicherung sämtlicher Verkehrsdaten zu Zwecken der Strafverfolgung und der Gefahrenabwehr erlaubt.[68] Bereits im Gesetzgebungsverfahren haben wir gegenüber dem Senator für Justiz und Verbraucherschutz Stellung zum geplanten Gesetz genommen und ihn gebeten, unsere Ausführungen bei der Beratung über das Gesetz im Bundesrat zu berücksichtigen.

Unabhängig von der im Hinblick auf die beiden Gerichtsentscheidungen generell zu stellenden Frage der Grundrechtskonformität der Vorratsdatenspeicherung wirft das inzwischen in Kraft getretene Gesetz folgende Probleme auf:

- Der Schutz der Berufsgeheimnisträger ist nicht gewährleistet. Davon ist auch der Berliner Beauftragte für Datenschutz und Informationsfreiheit betroffen, denn Daten über alle Anrufer in seiner Dienststelle müssen auf Vorrat bei

65 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. EU L 105/54

66 EuGH, Urteil vom 8. April 2014, C-293/12 und C-594/12, Rn. 37, 52 ff.

67 BVerfG, Urteil vom 2. März 2010, 1 BvR 256/08; siehe auch JB 2010, 13.1

68 Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, BGBl. I, S. 2218

den Telefongesellschaften gespeichert werden. Das vorgesehene Abruf- und Verwertungsverbot stellt keine Alternative zum vollständigen Verzicht auf die Speicherung von Verkehrsdaten von Berufsgeheimnisträgern dar.

- Das Bundesverfassungsgericht hat betont, dass die Schaffung vorsorglicher anlassloser Datensammlungen eine Ausnahme bleiben muss und in Verbindung mit anderen vorhandenen Dateien nicht „zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger" führen darf.[69] Das Gesetz entspricht insbesondere hinsichtlich der Überwachung der Internetnutzung nicht diesen Vorgaben. Allein die umfassende Verpflichtung zur Speicherung von IP-Adressen führt zu einer großen Datensammlung, die zusammen mit anderen staatlichen Zugriffsmöglichkeiten auf IP-Adressen[70] eine umfangreiche Überwachung ermöglichen.
- Die Neuregelung der Funkzellenabfragen in § 100g Abs. 3 Strafprozessordnung (StPO) wurde nicht dazu genutzt, den Einsatz solcher Maßnahmen gemessen an deren großer Eingriffstiefe und Streubreite zu begrenzen. Insbesondere wurde der Anwendungsbereich für Funkzellenabfragen nicht auf die in § 100a Abs. 2 StPO benannten Straftaten beschränkt.[71]

Das neue Gesetz räumt die erheblichen verfassungsrechtlichen Bedenken gegen die Vorratsdatenspeicherung nicht aus. Es bleibt abzuwarten, ob die Neuregelung der gerichtlichen Überprüfung standhalten wird, die aufgrund der bereits erhobenen Verfassungsbeschwerden zu erwarten ist.

4.2 Gesetz zur Weiterentwicklung des Berliner Justizvollzugs

Seit der Föderalismusreform im Jahr 2006 sind die Länder für die Strafvollzugsgesetzgebung zuständig und können das bisherige Strafvollzugsgesetz des Bundes durch eigene Regelungen ersetzen. Die Senatsverwaltung für Justiz und Verbraucherschutz legte in diesem Zusammenhang den Entwurf

69 BVerfG, a. a. O., Rn. 218

70 U. a. aufgrund von Regelungen des Bundeskriminalamtsgesetzes (BKAG) und des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

71 Zur Notwendigkeit des restriktiven Umgangs mit Funkzellenabfragen siehe auch JB 2012, 2.1

eines Gesetzes zur Weiterentwicklung des Berliner Justizvollzugs[72] vor, zu dem uns frühzeitig Gelegenheit zur Stellungnahme gegeben wurde.

Der Strafvollzug soll nun noch konsequenter am Resozialisierungsgedanken ausgerichtet werden, was eine verstärkte Zusammenarbeit verschiedener Stellen und eine damit einhergehende Übermittlung personenbezogener Daten bedingt. Diese Übermittlung ist verfassungsrechtlich zulässig, soweit die Daten für die Erfüllung der Aufgaben der jeweiligen Stelle erforderlich sind. In den geplanten Regelungen spiegelt sich das Erforderlichkeitsprinzip bislang jedoch nicht hinreichend wider. Wie bereits im 2013 verabschiedeten Gesetz über den Vollzug der Sicherungsverwahrung[73] wird die Verarbeitung personenbezogener Daten oft lediglich von der Zweckmäßigkeit abhängig gemacht; auch ist aus den Vorschriften nicht ersichtlich, für welche Stellen sie gelten sollen. Wir haben darauf hingewiesen, dass zur Wahrung der Verfassungskonformität im geplanten Gesetz verdeutlicht werden sollte, welche personenbezogenen Daten durch welche konkreten Stellen in welchem Umfang verarbeitet werden dürfen.

Der Entwurf soll es den Justizvollzugsanstalten erlauben, sämtlichen Schriftwechsel der Gefangenen zu überwachen, soweit dies wegen einer Gefährdung der Erreichung des Vollzugsziels oder aus Gründen der Sicherheit erforderlich ist.[74] Diese Vorschrift ist in der derzeitigen Form verfassungsrechtlich bedenklich. Die Rechtsprechung lässt eine inhaltliche Überwachung des Schriftwechsels bei einer Justizvollzugsanstalt höchster Sicherheitsstufe generell aus Gründen der Sicherheit und Ordnung der Anstalt mit der Begründung zu, dass besonders gefährliche Gefangene nicht überwachte Mitgefangene unter Druck setzen könnten, um über deren ein- und ausgehende Post sicherheitsgefährdende Kontakte nach außen herzustellen.[75] Gründe der Sicherheit und Ordnung in Justizvollzugsanstalten geringerer Sicherheitsstufen sowie die Gefährdung der Erreichung des Vollzugsziels einzelner Gefangener in Justizvollzugsanstalten jeder Sicherheitsstufe rechtfertigen hingegen keinen solchen schwerwiegenden Eingriff in das grundrechtlich geschützte Brief- und

72 Abghs.-Drs. 17/2442
73 Siehe JB 2013, 5.1
74 § 37 Abs. 1 StVollzG-E
75 BVerfGE, Nichtannahmebeschluss vom 22. Oktober 2003, 2 BvR 345/03, Rn. 7 - zitiert nach juris

Postgeheimnis, wie sie die allgemeine Überwachung des Schriftwechsels darstellt. Wir haben daher empfohlen, im Gesetz vorzusehen, dass der Schriftwechsel nur im Einzelfall überwacht werden darf, soweit dies zur Erreichung des Vollzugsziels oder aus Gründen der Sicherheit und Ordnung der Anstalt erforderlich ist. Eine allgemeine Kontrolle des Schriftwechsels darf nur in Anstalten höchster Sicherheitsstufe erlaubt werden, soweit dies aus Gründen der Sicherheit und Ordnung der Anstalt erforderlich ist.

Unsere Empfehlungen wurden u. a. in diesem Punkt bislang nicht berücksichtigt. Wir konnten jedoch einige andere Klarstellungen und Konkretisierungen im Gesetzentwurf hinsichtlich der Zulässigkeit der Datenübermittlung durch die Justizvollzugsanstalten an externe Stellen bewirken.

Das Gesetz zur Weiterentwicklung des Berliner Justizvollzugs bleibt im jetzigen Entwurfsstadium hinter den guten datenschutzrechtlichen Ansätzen im Justizvollzugsdatenschutzgesetz zurück[76] und sollte insbesondere im Hinblick auf den Erforderlichkeitsgrundsatz dringend nachgebessert werden.

4.3 Mithören von Gefangenentelefonaten

Aus der Praxis

Nach dem derzeit noch für den Berliner Strafvollzug geltenden[77] Bundesgesetz über den Vollzug der Freiheitsstrafe und der freiheitsentziehenden Maßregeln der Besserung und Sicherung[78] dürfen Telefonate von Gefangenen überwacht werden, soweit es aus Gründen der Behandlung oder der Sicherheit oder Ordnung der Anstalt erforderlich ist und es sich nicht um Telefonate mit dem Verteidiger sowie sog. Petitionsstellen[79] handelt.[80] Über eine beabsichtigte Überwachung sind die Gesprächsteilnehmerinnen und -teilnehmer vorab zu informieren.[81]

76 Siehe JB 2011, 2.2.3
77 Siehe 4.2
78 Strafvollzugsgesetz (StVollzG)
79 Dazu zählt auch die Behörde der Berliner Beauftragten für Datenschutz und Informationsfreiheit.
80 § 32 Satz 2 i.V. m. § 29 StVollzG
81 § 32 Satz 3, 4 StVollzG

Hierbei ist auf den konkreten Einzelfall abzustellen. Ein allgemeiner Hinweis auf eine mögliche Überwachung vor jedem Gefangenentelefonat ist unzulässig. Er würde die Gesprächsteilnehmenden verunsichern und insoweit unnötig in ihrer informationellen Selbstbestimmung einschränken. Besonders problematisch wirkt sich dies auf Telefonate zwischen Gefangenen und ihren Verteidigerinnen und Verteidigern aus.

Wir haben geprüft, ob in den Justizvollzugsanstalten (JVA) solche allgemeinen Ansagen bei den Gefangenentelefonaten verwendet werden. Es stellte sich dabei heraus, dass lediglich die JVA für Frauen eine generelle Bandansage zur Telefonüberwachung eingerichtet hatte. Auf unseren rechtlichen Hinweis hin, dass solche Mitteilungen nur bei einer tatsächlich durchgeführten Überwachung erfolgen dürfen, stellte die JVA für Frauen ihre bisherige Praxis unverzüglich um.

Eine Datenverarbeitung ist nur dann transparent, wenn deutlich wird, in welcher Form sie stattfindet, was sie beinhaltet und wann sie genau durchgeführt wird. Anderenfalls können Betroffenenrechte nicht wirksam wahrgenommen werden.

4.4 Mangelhafte Anonymisierung bei Veröffentlichung einer Gerichtsentscheidung

Eine Petentin hat sich an uns gewandt und sich über die nicht ausreichend anonymisierte Veröffentlichung eines Gerichtsbeschlusses durch das Kammergericht beschwert. Sie wurde hierauf durch eine Bekannte aufmerksam gemacht, die diese Entscheidung zufällig gelesen hatte und trotz geschwärzter Namen der Prozessbeteiligten die Petentin aufgrund detaillierter Orts- und Zeitangaben sofort wiedererkannte.

Der Beschluss wurde in der vom Kammergericht herausgegebenen Form von mehreren Gerichtsentscheidungsdatenbanken im Internet veröffentlicht. Mit wenigen Angaben aus dem Lebenslauf der Petentin war es möglich, über eine Internetsuchmaschine auf den Beschluss aufmerksam zu werden und so an sensitive Daten der Petentin wie beispielsweise Angaben zur Gesundheit zu

gelangen. Die Petentin befürchtete durch diese Erkennbarkeit große berufliche und private Nachteile.

Wir teilten dem Kammergericht umgehend mit, dass die Veröffentlichung in der beschriebenen Form unzulässig sei, und forderten es auf, die Löschung der Entscheidung zu veranlassen. Das Kammergericht kam dieser Aufforderung nach und bewirkte, dass die betreffenden Datenbanken nunmehr eine ausreichend anonymisierte Version des Beschlusses veröffentlichen bzw. vollständig auf dessen Veröffentlichung verzichten.

Das Kammergericht erklärte, dass eine vollständige Anonymisierung seiner Entscheidungen selbstverständlicher Standard sei und mittels eines Formblattes unter Berücksichtigung des Vier-Augen-Prinzips erfolge. Es handele sich vorliegend um einen bedauerlichen Ausnahmefall. Obwohl bereits über tausend Entscheidungen veröffentlicht worden seien, seien bislang keine Fehler bei der Anonymisierung entdeckt worden.

Das Anonymisieren von Dokumenten erfordert eine sorgfältige Arbeitsweise, da nicht nur direkte Identifikationsmerkmale wie Namen und Adressen, sondern jegliche Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person unkenntlich gemacht werden müssen.[82]

4.5 Auskunftspflicht von Rechtsanwältinnen und Rechtsanwälten

Rechtsanwältinnen und Rechtsanwälte geben uns gegenüber immer wieder an, aufgrund eines Mandatsverhältnisses und der sich daraus abzuleitenden Pflicht zur Verschwiegenheit[83] nicht zur Auskunft nach dem BDSG verpflichtet zu sein.

Aus der Praxis

82 § 4 Abs. 3 Nr. 7 BlnDSG
83 § 43 a Abs. 2 BRAO

Grundsätzlich ist jede unserer Kontrolle unterliegende Stelle zur Auskunft verpflichtet.[84] Eine Rechtsanwältin oder ein Rechtsanwalt kann gegenüber der Aufsichtsbehörde die Auskunft nur dann verweigern, wenn diese die Anwältin oder den Anwalt der Gefahr strafgerichtlicher Verfolgung aussetzen würde.[85] Eine solche Gefahr droht nicht, wenn eine Einwilligung der Mandantin oder des Mandanten in die Auskunftserteilung vorliegt. Dies ist der Fall, wenn die Betroffenen eine Eingabe bei uns einreichen, die das anwaltliche Verhältnis betrifft.

Darüber hinaus wäre eine strafrechtliche Verfolgung nur bei unbefugter Weitergabe von Informationen aus dem Mandatsverhältnis möglich.[86] Dies ist uns gegenüber nur denkbar, wenn keine Pflicht zur Auskunft besteht. Hierzu gibt es unterschiedliche Gerichtsentscheidungen. Das Kammergericht hat 2010 zwar beschlossen, dass Rechtsanwälte der Datenschutzbehörde keine Auskunft erteilen müssen, sofern sie sich auf die Schweigepflicht berufen können.[87] Im darauffolgenden Jahr hat allerdings das Bundesverwaltungsgericht festgestellt, dass nach der Bundesordnung für Rechtsanwälte (BORA) die Pflicht zur Verschwiegenheit gegenüber einer Aufsichtsbehörde (der Bundesanstalt für Finanzdienstleistungen) nicht gilt,[88] wenn andere Rechtsvorschriften Ausnahmen zulassen.[89] Dies seien solche, die die Schweigepflicht des Rechtsanwalts ausdrücklich einschränken. Dazu gehören auch nicht-berufsspezifische Regelungen. Auskunftspflichten, die das Gesetz jedermann oder eine nicht nach dem Beruf abgegrenzten Gruppe auferlegt, treffen grundsätzlich auch Rechtsanwältinnen und Rechtsanwälte.

Unsere Behörde hat eine Pflicht zur Verschwiegenheit über die ihr amtlich bekannt gewordenen Angelegenheiten.[90] Es ist selbstverständlich, dass durch die Auskunft möglicherweise gewonnene Erkenntnisse nicht der Gegenseite als potenziellem Streitgegner zugänglich gemacht werden. Die gesetzlich

84 § 38 Abs. 3 Satz 1 BDSG
85 § 38 Abs. 3 Satz 2 BDSG
86 § 203 StGB
87 Kammergericht Berlin, Beschluss vom 20. August 2010, 1 Ws (B) 51/07 – 2 Ss 23/07 – (AG Berlin-Tiergarten)
88 § 59 b Abs. 2 Nr. 1 Buchst. c BRAO i.V. m. § 2 Abs. 3 BORA
89 BVerwG, Urteil vom 13. Dezember 2011, 8 C 24/10
90 § 23 BlnDSG

intendierte Prüfung zur datenschutzkonformen Arbeitsweise der Anwaltschaft würde durch den generellen Ausschluss unter Berufung auf eine Schweigepflicht jedoch unterlaufen. Es reicht nicht aus, sich allein auf die anwaltliche Verschwiegenheit zu berufen. Eine Informationserteilung an die Aufsichtsbehörden ist daher nicht per se unbefugt im Sinne des Strafgesetzbuches.

Rechtsanwältinnen und Rechtsanwälte sind gegenüber der Aufsichtsbehörde grundsätzlich auskunftspflichtig.

4.6 Projekt „Smarte Bürger"

Wir haben uns beratend am Projekt „Smarte Bürger – Verbraucherschutz in der digitalen Welt"[91] der Technologiestiftung Berlin, der Senatsverwaltung für Justiz und Verbraucherschutz und der Open Knowledge Foundation Deutschland beteiligt.

Ziel des Projektes ist es, Bürgerinnen und Bürger im Rahmen einer Informationskampagne über Verbraucherschutz im Web und mobilen Internet zu informieren. Wir wurden hierfür bezüglich der Datenschutzaspekte des Verbraucherschutzes hinzugezogen und konnten mit einigen Vorschlägen über zu behandelnde Themen zum Erfolg der Kampagne beitragen.

Sie besteht in erster Linie aus einem interaktiven Parcours, der reale und digitale Welt spielerisch verbinden soll. Hierzu können auf der Webseite smarte-buerger.de zum Download bereitgestellte Plakate ausgedruckt und auf einem Spielfeld – z. B. im Klassenraum oder auch in einem Garten – aufgestellt werden. Gespielt wird der interaktive Parcours mithilfe einer Webapp, eines auf mobile Displays angepassten Webangebots, das einer Smartphone-App ähnelt. Die Nutzenden können die Stationen des Parcours grundsätzlich parallel und in beliebiger Anzahl ohne eine Anleitung durchlaufen, da die Plakate bzw. die zugehörigen Teile der App an den jeweiligen Stationen die notwendigen Informationen für die jeweils durchzuführenden Aufgaben bereitstellen.

91 www.smarte-buerger.de

Zu den zu lösenden Aufgaben gehört z. B. die Installation einer App, wobei eine Reihe von Rechten eingefordert wird. Je nach Reaktion des Nutzers erhält dieser im Anschluss eine Auswertung aus Datenschutzsicht. Es wird verdeutlicht, dass man immer kritisch prüfen sollte, ob eine App tatsächlich die jeweils eingeforderten Rechte benötigt. Falls man nicht davon überzeugt ist, sollte man das jeweilige Recht verweigern bzw. ganz auf die Installation der App verzichten.

Die weiteren Stationen beschäftigen sich mit der Problematik, dass Nutzende von Online-Diensten oder sozialen Netzwerken leicht die Kontrolle und u. U. auch ihre Rechte an zur Verfügung gestellten Inhalten wie z. B. Texten, Bildern und Videos verlieren können. Zudem geht es um die Praxis von Online-Shops, mithilfe von Auskunfteien und anderen Informationen – z. B. aus sozialen Netzwerken oder durch Auswertung der Art des verwendeten Endgerätes (teuer oder billig) – die Kreditwürdigkeit und Zahlungsfähigkeit von Kunden zu bewerten und daraufhin u. U. schlechtere Konditionen anzubieten oder gar bestimmte Angebote zu verweigern.[92] Eine weitere Station befasst sich mit den möglichen Auswirkungen des sog. Offline-Trackings.[93] Hierbei werden mit verschiedenen Techniken die Aufenthaltsorte der Nutzenden (z. B. in einem Geschäft) ausgewertet und zur gezielten Werbeansprache verwendet.

Neben dem Parcours wird ein Quiz zu Verbraucher- und Datenschutzthemen mit Bezug zu neuen Medien und Online-Diensten angeboten. Zusätzlich existiert eine Sammlung von Tipps zum Selbstdatenschutz.

Ein Ziel unserer Arbeit ist die Information und die Sensibilisierung der Bürgerinnen und Bürger in Datenschutzfragen. Eine Möglichkeit unserer Öffentlichkeitsarbeit stellt die Beratung bei Projekten wie der Informationskampagne „Smarte Bürger“ dar.

92 Siehe dazu JB 2014, 9.2.2
93 Siehe dazu 11.8.2

5 Stadtentwicklung, Verkehr und Tourismus

5.1 Besserer Schutz von Eigentümerdaten

Aus der Praxis

2013 haben wir darüber berichtet, dass wir vielen Beschwerden wegen unerwünschter Werbepost von Maklern nachgehen mussten.[94] Diese hatten Daten aus dem Liegenschaftskataster erhalten und für unerwünschte Werbeschreiben an die Eigentümer missbraucht. Nach der bisherigen Fassung des Vermessungsgesetzes kann das Vermessungsamt (Liegenschaftsamt) Eigentümerangaben jedem zur Verfügung stellen, der ein „berechtigtes Interesse" an den Daten darlegt.[95] In einigen Fällen erhalten Makler die Eigentümerdaten schon dann, wenn bloß behauptet wurde, dass sie ein berechtigtes Interesse an den Daten haben – ohne dass eine entsprechende Prüfung stattfand. Wir haben uns daher für eine Verschärfung des Vermessungsgesetzes eingesetzt.

Die Senatsverwaltung für Stadtentwicklung und Umwelt hat unsere Vorschläge aufgegriffen und eine Änderung des Vermessungsgesetzes auf den Weg gebracht. Darin werden die Voraussetzungen konkretisiert, unter denen Daten aus dem Liegenschaftskataster herausgegeben werden dürfen. Der Entwurf sieht vor, dass ein berechtigtes Interesse nur dann gegeben ist, wenn die Daten der Anbahnung von Erwerbsverhandlungen dienen und ein konkretes Interesse am Erwerb der betroffenen Liegenschaft glaubhaft gemacht wird. Kein berechtigtes Interesse ist gegeben, wenn die Datenerhebung lediglich dazu dient, allgemein die Verkaufsbereitschaft des Eigentümers zu prüfen, um diesem Maklerleistungen anzubieten, ohne dass der Makler von einem bestimmten Käufer beauftragt wurde, den Erwerb des konkreten Grundstücks zu ermitteln. Dadurch wird eine Erhebung zu bloßen Werbezwecken ausgeschlossen. Gleichzeitig wird der Verkauf von Grundstücken nicht behindert, falls tatsächlich ein solches Interesse besteht. Zudem genügt es nach der künftigen Gesetzeslage nicht mehr, dass der Antragsteller dieses berechtigte Interesse durch bloße Behauptung darlegt. Vielmehr muss er sein berechtigtes Interesse nunmehr „glaubhaft machen". Das

94 JB 2013, 10.2
95 § 17 Abs. 1 Nr. 2 Vermessungsgesetz Berlin

heißt, der Antragsteller muss durch geeignete Unterlagen die Wahrscheinlichkeit dieser Sachlage nachweisen.

Außerdem haben wir 2013 kritisiert, dass sog. „zuverlässige“ Unternehmen von der Darlegung des berechtigten Interesses befreit werden konnten. Grund dafür war, dass eine Prüfung der Zuverlässigkeit in der täglichen Praxis nicht stattfand. Vielmehr wurde auch hier ohne weitere Prüfung grundsätzlich von der Zuverlässigkeit aller Antragsteller ausgegangen. Diese wurde nur dann verneint, wenn andere Tatsachen bekannt wurden, z. B. dass der Antragsteller in der Presse als hochgradig straftatverdächtig in Erscheinung getreten ist. Da eine adäquate Zuverlässigkeitsprüfung in der täglichen Praxis nicht durchgeführt werden kann, soll die Befreiungsmöglichkeit ganz gestrichen werden.

Erleichterungen sind hingegen bei dem weniger schutzwürdigen Zugang zu Flurstücks- und Grundstücksangaben geplant. Dadurch wird im Ergebnis ein angemessener Ausgleich zwischen dem Datenschutz und den Belangen der betroffenen Wirtschaft geschaffen.

Wir hoffen, dass das Gesetzgebungsvorhaben dazu führt, dass Betroffene weniger mit unerwünschter Werbepost belästigt werden.

5.2 Parkausweise – schon auf der Gästeliste?

Auch in diesem Jahr hat uns das Thema Parkraumbewirtschaftung in mehreren Fällen beschäftigt.[96]

Dabei ging es z. B. um den Gästeparkausweis. Einige Bezirke bieten ihren Anwohnern die Möglichkeit an, für ihre Gäste eine temporäre Gästevignette zu erwerben. Diese berechtigt den Besucher für einen bestimmten Zeitraum zum Parken in einer bestimmten Parkraumbewirtschaftungszone. Um diese Vignette zu erhalten, verlangt das Bezirksamt nicht nur die Angabe des Kfz-Kennzeichens, sondern auch den Namen des Gastes. Dadurch kann das Bezirksamt

96 Zuletzt JB 2013, 4.4

einen genauen Einblick darüber erhalten, welchen längerfristigen Besuch der Anwohner erhält.

Dies ist unzulässig. Zwar darf das zuständige Bezirksamt diejenigen Daten erheben, die zur Bearbeitung des Antrags auf eine Gästevignette erforderlich sind.[97] Dazu gehören aber nicht die Namen der einzelnen Gäste. Vielmehr reicht zur Überprüfung der Parkberechtigung die Angabe des Kfz-Kennzeichens aus. Dadurch ist es den Mitarbeiterinnen und Mitarbeitern des Ordnungsamtes möglich zu überprüfen, ob für das entsprechende Fahrzeug ein Gästeparkausweis vorliegt.

Die Verkehrslenkung Berlin, die die Parkraumbewirtschaftung überbezirklich koordiniert, konnte nicht schlüssig darlegen, aus welchem Grund die Erhebung des Namens des Gastes erforderlich ist. Vielmehr wurde uns mitgeteilt, dass zukünftig ganz auf diesen Beantragungsweg verzichtet werde, wenn an der Erhebung des Namens nicht festgehalten werden kann.

Von einem anderen Petenten wurden wir darauf aufmerksam gemacht, dass bei der Antragstellung für den Parkausweis eine Kopie des Personalausweises verlangt wird. Der Personalausweis enthält aber eine Reihe von Daten, die für die Bearbeitung des Antrags nicht relevant sind. Dazu gehören Angaben wie Körpergröße, Augenfarbe und Lichtbild. Beim neuen Personalausweis kommt noch die sechsstellige Zugangsnummer dazu, die grundsätzlich nur dem Ausweisinhaber bekannt sein sollte. Wir haben die Bezirke und die Verkehrslenkung Berlin auf die Problematik aufmerksam gemacht und gebeten, die Antragsteller darauf hinzuweisen, dass die nicht erforderlichen Daten geschwärzt werden können.

In einem weiteren Fall haben uns Beschwerden von Hebammen erreicht. Diese gaben an, dass das Bezirksamt bei der Beantragung eines Sonderparkausweises von Hebammen verlange, Angaben zu Schwangeren bzw. Wöchnerinnen zu machen. So wird nicht nur die genaue Adresse der Betroffenen verlangt, sondern auch welche Art der Behandlung (z. B. Vorsorgeuntersuchung, Wochenbettbesuch) durchgeführt wird. Wozu die Angaben in dieser Genauigkeit benötigt werden, konnte uns die Verkehrslenkung Berlin nicht schlüssig darlegen.

97 § 18 Abs. 1 Satz 2 ASOG, § 6 Abs. 1 Nr. 14 StVG, § 45 Abs. 1b Nr. 2 StVO

Wir haben darauf hingewiesen, dass es sich dabei um sensitive Gesundheitsdaten handelt. Insbesondere in den ersten Monaten der Schwangerschaft kann unter Umständen ein großes Interesse daran bestehen, sie vorerst geheim zu halten. Gesundheitsdaten werden durch das Berliner Datenschutzgesetz (BlnDSG) besonders geschützt und dürfen nur unter strengen Voraussetzungen erhoben werden, die hier aber nicht vorlagen. Außerdem unterliegen Hebammen der Schweigepflicht nach § 203 Abs. 1 Nr. 1 Strafgesetzbuch (StGB).

Wir haben daher gefordert, die Daten zu anonymisieren und nicht mehr adressgenau zu erheben. Dabei haben wir vorgeschlagen, dass statt der genauen Adresse lediglich die Straße oder ein bestimmter Hausnummernbereich von mindestens zehn Hausnummern angegeben wird (z. B. Hauptstraße 15-25). Dadurch wären Rückschlüsse auf die Identität der Schwangeren kaum möglich gewesen. Dies hat die Verkehrslenkung Berlin abgelehnt. Man war lediglich bereit, sich auf einen Hausnummernbereich von drei Hausnummern zu beschränken (z. B. Hauptstraße 5-7). Eine solche Beschränkung stellt allerdings keine Anonymisierung im Sinne des BlnDSG dar. Danach liegt eine solche erst dann vor, wenn die Daten nur mit unverhältnismäßig großem Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten Person zugeordnet werden können.[98] Falls in einem bestimmten Hausnummernbereich von drei Hausnummern ansonsten vorwiegend ältere Menschen wohnen, kann ohne Weiteres auf die schwangere Person geschlossen werden, sodass eine Anonymisierung im Rechtssinne nicht vorliegt. Da die Verkehrslenkung Berlin unseren Vorschlag ablehnte, war eine förmliche Beanstandung nach § 26 BlnDSG geboten.

Bei der Erteilung von Parkausweisen kommt es immer wieder zu Datenschutzverstößen. Die Verkehrslenkung Berlin sollte dies zum Anlass nehmen, sämtliche Beantragungsverfahren auf ihre Vereinbarkeit mit den Datenschutzgesetzen zu überprüfen und gemeinsam mit den Bezirken entsprechend anzupassen. Dabei verlangt der Datenschutz nicht, auf bestimmte Antragsverfahren zu verzichten. Vielmehr sollten sie datenschutzgerecht und bürgerfreundlich ausgestaltet werden. Dies kommt auch den Antragstellern zugute, deren Daten besser geschützt bzw. erst gar nicht in dem bisherigen Umfang erhoben werden.

98 § 4 Abs. 3 Nr. 7 BlnDSG

5.3 Kennzeichenerfassung in Parkhäusern

In immer mehr Parkhäusern werden die Kennzeichen der einfahrenden Fahrzeuge mit denen der ausfahrenden über ein computergestütztes Kamerasystem abgeglichen. Dies sei ein Service für die Betroffenen, die womöglich das Ticket verlieren und unter Verwertung der so zum Kennzeichen gespeicherten Einfahrtzeit minutengenau abrechnen können und nicht sofort die höhere Ticketverlustgebühr bezahlen müssen. Parkhausbetreiber wollen auch Betrug zu ihren Lasten verhindern, wenn sie nach wochenlangem Parken bei der Abholung unter Vorspiegelung eines Ticketverlusts nach ihren allgemeinen Geschäftsbedingungen lediglich die Ticketverlustgebühr verlangen können.

Kennzeichenerfassung lässt die Möglichkeit zu, Bewegungsprofile zu erstellen, aus denen Rückschlüsse auf das Verhalten der Betroffenen gezogen werden können. Alle Parkenden zu erfassen, damit einige Betrugsfälle aufgedeckt werden können, bedeutet unter Einbeziehung der Datennutzungsmöglichkeiten eine erhebliche Einschränkung des Persönlichkeitsrechts, die in der Regel unverhältnismäßig ist.

Dennoch kann es Parkhäuser geben, in denen das Betrugs- bzw. Verlustaufkommen so hoch ist, dass eine Kennzeichenerfassung unter engen Voraussetzungen auch datenschutzrechtlich zulässig ist. Denkbar sind z. B. Parkhäuser in der Nähe von Flughäfen oder Bahnhöfen, in denen Menschen ihr Auto für die Dauer ihres Urlaubs abstellen. Hier sind beide Varianten denkbar: Sowohl der unfreiwillige Verlust des Tickets im Urlaub als auch der Versuch, eine mehrwöchige Parkdauer durch Ticketverlust kostengünstiger zu gestalten.

In diesen Fällen sind die Einfahrenden deutlich sichtbar über die Kennzeichenerfassung und die verantwortliche Stelle durch Beschilderung zu informieren. Der Hinweis muss zu einem Zeitpunkt sichtbar sein, in dem Einfahrende noch eine realistische Möglichkeit haben, sich trotz Kennzeichenerfassung ohne Gefährdung des Verkehrs für oder gegen eine Einfahrt entscheiden zu können. Die Kennzeichendaten sind zu löschen, sobald sie für den Zweck der Abrechnung nicht mehr erforderlich sind, grundsätzlich also kurz nach der Ausfahrt.

Kennzeichenerfassung in Parkhäusern ist unter engen Voraussetzungen zulässig. Dann aber müssen die Beschilderung eine echte Wahl der Nutzung ermöglichen und die Datensicherheit und -löschung gewährleistet sein. Vor dem Hintergrund der Nutzungsmöglichkeiten der Daten für Bewegungsprofile ist eine restriktive Handhabung angebracht.

5.4 Kein P-Schein ohne Gesundheitsbefragung?

Wir haben den Hinweis erhalten, dass das Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) bei der Beantragung von Personenbeförderungsscheinen (sog. P-Schein) von den Antragstellern umfangreiche Gesundheitsdaten erhebt. So wird u. a. gefragt, ob Sehschwächen, Hirnverletzungen, schwere Herz- und Kreislauferkrankungen, Anfallsleiden, Zuckerkrankheit, Geisteskrankheit, Alkohol-, Arzneimittel- oder Drogenmissbrauch, Schwerhörigkeit, Taubheit, Amputation oder Lähmungen bestehen.

Diese Form der Befragung ist datenschutzrechtlich unzulässig. Zwar muss vor der Erteilung eines P-Scheins geprüft werden, ob der Antragsteller gesundheitlich geeignet ist, Fahrgäste zu befördern. Schließlich trägt er eine hohe Verantwortung für die Sicherheit der Fahrgäste und anderer Verkehrsteilnehmenden. Die Fahrerlaubnis-Verordnung sieht allerdings vor, dass die Prüfung der gesundheitlichen Anforderungen durch eine Ärztin oder einen Arzt zu erfolgen hat.[99] Nach Anlage 5 der Fahrerlaubnis-Verordnung verbleiben dabei die detaillierten medizinischen Informationen (Teil 1) bei dem begutachtenden Arzt, während die Behörde lediglich das Ergebnis der ärztlichen Begutachtung (Teil 2) erhält. Diese Aufteilung ist ebenso in anderen Bereichen üblich und auch sinnvoll, da medizinische Daten nach den Datenschutzgesetzen besonders geschützt werden.[100] Daher sollten sie grundsätzlich bei Stellen verbleiben, wo sie der ärztlichen Schweigepflicht unterliegen. Dieses vom Gesetz vorgesehene Verfahren darf nicht dadurch umgangen werden, dass die Behörde die medizinischen

99 § 48 Abs. 4 Nr. 3 bzw. Abs. 5 Nr. 1 i.V. m. § 11 Abs. 9 i.V. m. Anlage 5 Fahrerlaubnis-Verordnung

100 § 13 Abs. 2 BDSG, § 6a BlnDSG

Details beim Antragsteller selbst erfragt und so in den Besitz der Gesundheitsinformationen gelangt.

Das LABO hat die Notwendigkeit der Befragung damit begründet, dass die beauftragten Ärzte oftmals Gefälligkeitsbescheinigungen ausstellen oder den Antragssteller nur oberflächlich untersuchen würden. Allerdings ist in Teil 1 der Anlage 5 zur Fahrerlaubnisverordnung genau festgelegt, welche Untersuchungen durchzuführen sind. Hält ein Arzt sich nicht an diese Vorgaben, kann er sich wegen Ausstellens unrichtiger Gesundheitszeugnisse strafbar machen.[101] Außerdem ist ohnehin fraglich, ob eine Befragung der Antragsteller selbst zuverlässiger ist. Diese sind in der Regel ebenfalls medizinische Laien und können finanziell und beruflich von der Erteilung eines P-Scheins abhängig sein. Im Ergebnis ist daher eine eigene Befragung des Antragstellers durch medizinisch nichtgeschultes Personal des LABO weder sinnvoll noch erforderlich. Sollte die Behörde begründete Zweifel an der gesundheitlichen Eignung des Antragstellers hegen, hat sie die Möglichkeit, weitere Untersuchungen anzuordnen. Allerdings müssen auch diese durch eine Ärztin oder einen Arzt durchgeführt werden.

Medizinische Daten sind besonders schutzbedürftig. Sie sollten grundsätzlich bei Stellen verbleiben, die der ärztlichen Schweigepflicht unterliegen. Dies gilt auch bei der Beantragung von P-Scheinen.

5.5 BVG

5.5.1 Bonitätsprüfung und Preisdiskriminierung bei Jahreskarten

Ein Bürger wies uns darauf hin, dass eine am Schalter bar bezahlte Jahreskarte bei der BVG 740 Euro kostet. Kauft man hingegen ein Abonnement, bezahlt man nur 707 Euro. Hierfür müssen allerdings personenbezogene Daten weitergegeben werden wie Name, Anschrift, Bankverbindung und Geburtsdatum. Außerdem wird von der BVG eine Bonitätsprüfung durchgeführt.

Aus der Praxis

101 § 278 StGB

Es gibt weder im Berliner Datenschutzgesetz (BlnDSG) noch in bereichsspezifischen Gesetzen für die BVG eine Rechtsgrundlage, die eine Bonitätsprüfung durch die BVG erlaubt. Zwar ist es möglich, sich auf eine Einwilligung zu beziehen. Mit dem bislang verwendeten Formular werden die gesetzlichen Anforderungen des BlnDSG jedoch nicht eingehalten. Die Voraussetzungen für eine informierte und freiwillige Einwilligung[102] sind nicht erfüllt. Es wird weder auf die Bedeutung der Datenübermittlung und den Verwendungszweck noch auf die Empfänger der Daten und den Zweck der Übermittlung hingewiesen. Auch fehlen Hinweise auf die Verweigerungsmöglichkeit, datensparsame Alternativen und die Rechtsfolgen. Zudem ist eine besondere Hervorhebung nicht erkennbar. Es findet sich lediglich ein unzureichender Verweis, dass die Verarbeitung und Speicherung von Daten „gemäß den datenrechtlichen Bestimmungen" ausgeführt werden. Auch die momentan vorliegende Einwilligungserklärung ist nur wenig besser.

Es ist aber auch datenschutzpolitisch fragwürdig, dass eine Fahrkarte im personenbedienten Verkauf 33 Euro teurer ist als ein Abonnement unter Preisgabe personenbezogener Daten sowie unter Einbeziehung einer Bonitätsprüfung, die womöglich Einflüsse auf den Score der Betroffenen hat.

Aus datenschutzpolitischer Sicht sollte die BVG eine Preisangleichung der bar bezahlten Jahreskarten im personenbedienten Verkauf und der Jahreskarten im Abonnement-Verfahren anstreben. Darüber hinaus sind die Einwilligungserklärungen zur Prüfung der Bonität derzeit nicht datenschutzkonform.

5.5.2 Neues zum Polizeiarbeitsplatz

2014 haben wir darüber berichtet, dass sich Senat, Berliner Verkehrsbetriebe und die Polizei darauf verständigt hatten, einen Polizeiarbeitsplatz in der BVG-Sicherheitsleitstelle einzurichten.[103] Allerdings ist die erforderliche und vereinbarte datenschutzrechtliche Umsetzung noch immer mangelhaft.

102 § 6 Abs. 5 Satz 1 und 2 BlnDSG
103 JB 2014, 3.5

Eine Polizistin oder ein Polizist in der BVG-Sicherheitsleitstelle hat aus Gründen der besseren Kooperation und schnelleren Einsatzbereitschaft die Möglichkeit, anlassunabhängig auf Live-Videobilder von kriminalitätsbelasteten Schwerpunktbahnhöfen zuzugreifen. Im Gegensatz dazu erhält sie bzw. er anlassabhängig für alle anderen U-Bahnhöfe vom BVG-Personal umgehend eine Freischaltung auf die Videolivesequenz, wenn dort aktuell eine Straftat zur Kenntnis genommen wird. Dieses System ist darin begründet, dass die Polizei nur bei sicherheitsrelevanten Vorfällen Videobeobachtung durchführen darf. Die Unterscheidung zwischen anlassabhängiger und anlassunabhängiger Aufschaltung ist nur sinnvoll, wenn die räumlichen und technischen Umstände eine Kenntnisnahme der für die Polizei nicht freigeschalteten Bilder verhindern. Derzeit sind sowohl die Polizei als auch das BVG-Sicherheitspersonal und ihre jeweilige Technik im selben Raum untergebracht, getrennt durch quergestelltes Mobiliar ähnlich einer „spanischen Wand". Dadurch ist es möglich, dass die Polizei alle Videobilder jederzeit einsehen kann. Dies wird auch nicht dadurch ausgeschlossen, dass Polizistinnen und Polizisten explizit darauf hingewiesen werden, dass sie die nicht freigegebenen Videobilder nicht einsehen dürfen. Wir kritisieren seit Einrichtung des Polizeiarbeitsplatzes, dass die baulichen Gegebenheiten dazu beitragen müssen, die rechtlichen Vorgaben zu erfüllen. Notwendig wäre eine deutliche räumliche Trennung.

Die BVG hat umgehend die baulichen und organisatorischen Voraussetzungen für die Nutzung der Videosequenzen durch die Polizei zu schaffen. Anderenfalls wäre die Nutzung des Polizeiarbeitsplatzes am derzeit vorgesehenen Ort nicht weiter möglich. Dies ist nicht im Interesse der Sicherheit der Fahrgäste der BVG.

5.6 Vorsicht vor der Weitergabe von Zugangsdaten zum Online-Banking!

Es gibt immer mehr Unternehmen, die Dienstleistungen unter Verwendung von Zugangsdaten zum Online-Banking anbieten. Ein Unternehmen bietet z. B. an, mithilfe dieser Daten sog. Mietzahlungsbestätigungen auszustellen. Dazu muss der Kunde dem Unternehmen zunächst seine Zugangsdaten für sein Online-Banking-Konto angeben. Das Unternehmen durchsucht

dann die im Online-Banking-Account vorhandenen Kontobewegungen und identifiziert die Mietzahlungen. Wenn diese ordnungsgemäß erfolgt sind, stellt das Unternehmen eine sog. Mietzahlungsbestätigung aus, die der Betroffene z. B. einem potentiellen Vermieter vorlegen kann, wenn er sich um eine neue Wohnung bewirbt.

Solche Verfahren mögen für den Kunden bequem sein, bergen aber auch ein hohes Sicherheitsrisiko, da es sich bei den Online-Zugangsdaten um besonders missbrauchsanfällige Daten handelt. Auch aus den einzelnen Kontobewegungsdaten können Informationen gewonnen werden, die u. U. viel von den persönlichen Lebensumständen des Betroffenen offenbaren und sensitiv sein können (z. B. Zahlungen von Arzt- und Medikamentenrechnungen, Mitgliedsbeiträge zu Partei und Gewerkschaft). Neben datenschutzrechtlichen Aspekten besteht außerdem die Gefahr, dass Betroffene durch die Weitergabe ihrer Daten gegen die Allgemeinen Geschäftsbedingungen ihrer jeweiligen Bank verstoßen,[104] was ebenfalls Nachteile für den Kunden nach sich ziehen kann. Zu einem anderen Verfahren, in dem es um eine bestimmte Zahlungsmethode ging, wurde bereits gerichtlich festgestellt, dass es Verbrauchern nicht ohne Weiteres zugemutet werden kann, das Online-Banking-Passwort und die TAN an Dritte herauszugeben. Zur Begründung stellte das Gericht fest, das Verfahren berge erhebliche Risiken für die Datensicherheit und eröffne gravierende Missbrauchsmöglichkeiten.[105] Dem Verbraucher mussten daher andere zumutbare Zahlungsmethoden eröffnet werden.

Auch in dem eingangs beschriebenen Beispiel ist zu raten, andere Möglichkeiten zu nutzen. Falls sich der ehemalige Vermieter weigert, eine Mietzahlungsbestätigung auszustellen, kann der Nachweis auch durch andere Mittel, z. B. durch die Vorlage ansonsten geschwärzter Kontoauszüge, erfolgen. Vermieter müssen dies akzeptieren und dürfen einen Nachweis über Mietzahlungen ohnehin erst verlangen, wenn der Abschluss des Mietvertrags unmittelbar bevorsteht.[106]

Online-Banking-Zugangsdaten und die TAN sollten nicht leichtfertig an Dritte herausgegeben werden, da damit erhebliche Risiken für die Datensicherheit verbunden sind und zudem Missbrauchsrisiken eröffnet werden.

104 Diese Frage ist derzeit noch Gegenstand kartellrechtlicher Verfahren.
105 LG Frankfurt a. M., Urteil vom 24. Juni 2015, 2-06 O 458/14
106 JB 2014, 7.1

5.7 Jagd auf Ferienwohnungen – heiligt der Zweck die Mittel?

Aus der Praxis

Das Bezirksamt Mitte hat einen privaten Dienstleister damit beauftragt, Daten von allen Ferienwohnungen zu beschaffen, die im Bezirk Mitte auf beliebten Vermittlungsplattformen im Internet angeboten wurden. Damit wollte das Bezirksamt illegal genutzten Wohnraum aufspüren. Der Dienstleister setzte dazu ein Computer-Programm ein, welches Daten durch ein sog. „Crawling" von den jeweiligen Vermittlungsplattformen abgriff – unabhängig davon, ob die entsprechende Wohnung im Verdacht einer rechtswidrigen Nutzung stand oder nicht. Dabei wurden nicht nur Name und Adresse des Anbieters erhoben, sondern auch eine Beschreibung von dessen Privatwohnung, in welcher z. B. ein Ferienzimmer angeboten wurde.

Diese Datenverarbeitung war rechtswidrig. Die Erhebung personenbezogener Daten zur Ermittlung von Ordnungswidrigkeiten und Straftaten ist nach unserer Rechtsordnung nur dann zulässig, wenn ein sog. Anfangsverdacht vorliegt. Eine anlasslose verdachtsunabhängige Speicherung ist nur im Ausnahmefall unter engen Voraussetzungen zulässig. Dies haben das Bundesverfassungsgericht[107] und der Europäische Gerichtshof[108] in ihren Urteilen zur Vorratsdatenspeicherung deutlich gemacht, wo es um Datenspeicherungen zum Zwecke der Terrorismusabwehr ging.[109] Diese rechtstaatlichen Grundsätze müssen erst recht gelten, wo es – wie hier – „nur" darum geht, zweckentfremdeten Wohnraum aufzuspüren und noch nicht einmal eine Straftat im Raume steht. Zwar ist die Schaffung und Erhaltung bezahlbaren Wohnraums in den Innenstadtbereichen ebenfalls ein hohes Gut. Allerdings rechtfertigt dies nicht eine anlasslose Datenspeicherung. Damit werden alle Anbieter von Ferienwohnungen unter Generalverdacht gestellt, obwohl nicht jede im Internet zu findende Ferienwohnung per se rechtswidrig angeboten ist.

107 BVerfG, Urteil vom 2. März 2010, 1 BvR 256/08
108 EuGH, Urteil vom 8. April 2014, C-293/12 und C-594/12
109 Siehe 4.1

Unbeschadet dessen ist völlig unklar, ob die Maßnahmen überhaupt erfolgversprechend sind, da die Standorte von Ferienwohnungen in der Regel nicht für jedermann abrufbar sind. Wer schon einmal eine Ferienwohnung über ein solches Portal angemietet hat, weiß, dass die genaue Adresse der Wohnung erst dann angezeigt wird, wenn man sich auf dem Portal einloggt oder seine Zahlungsdaten angibt.

Dass auch ein anderer Weg möglich ist, zeigt z. B. der Bezirk Charlottenburg Wilmersdorf, wo Presseberichten zufolge bis Mitte 2014 bereits über 600 Verfahren wegen unerlaubter Ferienwohnungen eingeleitet wurden, ohne dass in vergleichbarer Weise unzulässig Daten erhoben wurden.

Wir haben dem Bezirksamt Mitte angeboten, es bei einer datenschutzkonformen Ausgestaltung der Internetrecherche zu beraten. Es hat dieses Angebot allerdings nicht angenommen und die Datenerhebung trotz unseres Votums wie geplant durchgeführt. Stattdessen wurde ein privates Rechtsgutachten in Auftrag gegeben, welches – wie zu erwarten – zu dem vom Bezirksamt Mitte gewünschten, allerdings unzutreffenden Ergebnis gekommen ist, dass die Datenerhebung unbedenklich sei. Unsere Behörde hat in einem solchen Fall bisher nicht die rechtliche Möglichkeit, eine rechtswidrige Datenverarbeitung zu untersagen, sodass wir lediglich eine Beanstandung[110] aussprechen konnten. Dieses Vollzugsdefizit wird sich mit Inkrafttreten der EU-Datenschutz-Grundverordnung ändern, da dort den Datenschutzaufsichtsbehörden die Möglichkeit eingeräumt wird, eine rechtswidrige Datenverarbeitung zu untersagen.[111]

Die anlasslose Erfassung und Speicherung personenbezogener Daten ist zur Verfolgung bloßer Ordnungswidrigkeiten unzulässig. Sie verstößt gegen das Grundrecht auf informationelle Selbstbestimmung und die Unschuldsvermutung. Das gilt auch bei der Fahndung nach illegalen Ferienwohnungen.

110 § 26 BlnDSG
111 Siehe 2.1.1

5.8 Probleme für Hotelgäste

5.8.1 Ausweiskopien zur Befreiung von der City Tax

Aus der Praxis

Uns erreichen immer wieder Beschwerden, dass insbesondere beim Check-In im Hotel Personalausweiskopien der Gäste angefertigt werden. Wir haben bereits mehrfach darüber berichtet, dass das Kopieren des Personalausweises nicht rechtmäßig ist.[112] Was aber ist mit der Kopie eines Dienstausweises?

Personalausweise werden an Rezeptionen in Hotels trotz breiter Aufklärung noch immer kopiert. Dabei ist die Hinterlegung aller darin enthaltenen Daten weder melderechtlich noch für die Durchführung des Beherbergungsvertrages notwendig. Dem Personalausweis sind viele Daten zu entnehmen, die hierfür überflüssig sind und demnach ohnehin auf einer Kopie zu schwärzen wären, z. B. Foto, Augenfarbe und Körpergröße. Für den neuen Personalausweis mit eID-Funktion gibt es sogar ein Kopierverbot.[113]

Ein Bürger beschwerte sich, weil in einem Hotel anlässlich seiner Übernachtung während einer Dienstreise sein Dienstausweis kopiert wurde. Ein Dienstausweis enthält je nach Ausgestaltung personenbezogene Daten wie Geburtsdatum und Foto.

Das Hotel trug vor, die Kopie sei als Nachweis bei der Abwicklung der sog. City Tax notwendig. Von der Besteuerung sind Übernachtungen aus beruflichen Gründen ausgeschlossen, wenn der Übernachtungsgast diesen Grund gegenüber dem Beherbergungsbetrieb, dem Hotel, glaubhaft macht.[114] Als Rechtsgrundlage zur Datenerhebung in Form einer Dienstausweiskopie ist diese Klausel zu unbestimmt. Sie dient aber der Ausfüllung des Merkmals der Erforderlichkeit der Datenerhebung und -verarbeitung zur Durchführung eines Vertragsverhältnisses.[115] Das Hotel kann für diesen Nachweis gegenüber dem Finanzamt z. B. eine Kopie des Dienstausweises beifügen. Allerdings dürfen aus

112 Siehe auch JB 2014, 15 (S. 181); JB 2013, 8.7
113 § 14 PAuswG; Begründung zu § 14 PAuswG in BR-Drs. 550/08 vom 8. August 2008; VG Hannover, Urteil vom 28. November 2013, 10 A 5342/11
114 § 1 Abs. 3 Satz 1 und 2 Übernachtungsteuergesetz (ÜnStG)
115 § 28 Abs. 1 Satz 1 Nr. 1 BDSG

dieser Kopie nicht mehr personenbezogene Daten hervorgehen, als für diesen Zweck notwendig sind.

Die Anfertigung einer Dienstausweiskopie ist möglich, damit ein Hotel gegenüber dem Finanzamt nachweisen kann, dass die Übernachtungsteuer wegen einer beruflich veranlassten Übernachtung nicht erhoben wurde. Für den Nachweis sind nicht erforderliche Daten wie Fotos zu schwärzen.

5.8.2 „Schwarze Listen“

In dem Hotel einer großen Kette wurden potenzielle Hotelgäste am Empfang abgewiesen, weil sie nach Auskunft des Empfangspersonals in einer sog. „Schwarzen Liste“ geführt würden. Auf Nachfrage wurden zu dieser Liste keine weiteren Auskünfte erteilt. Erst uns gegenüber machte man nähere Angaben. Tatsächlich würde eine solche Liste hotelintern geführt. Darin seien die Betroffenen ausschließlich mit dem Vermerk „Raucher“ bzw. „Schwarzschläfer“ aufgeführt. Eine Auskunft den Betroffenen gegenüber gebe es nicht, da die Liste nur innerhalb des Hotels verwendet würde und nicht öffentlich sei.

Im Rahmen der Vertragsfreiheit kann ein Hotel entscheiden, mit welchen Gästen es einen Beherbergungsvertrag schließen möchte. Als eine mögliche Basis für diese Entscheidung und um einen geordneten und sicheren Hotelbetrieb zu gewährleisten, ist es nachvollziehbar, dass ein Hotel eine Liste in Bezug auf Personen führt, die den Hausfrieden bereits gestört haben. Wenn beispielsweise trotz Rauchverbots in den Zimmern geraucht und dadurch ein hotelweiter Rauchalarm ausgelöst wird, kann dies dazu führen, dass das gesamte Hotel geräumt werden muss. Es kann auch sein, dass Gäste weitere, nicht angemeldete Gäste in ihren Zimmern schlafen lassen, um Kosten zu sparen. Beides ist eine vertragswidrige Nutzung. Sollte ein solches Verhalten bestimmten Personen nachgewiesen werden, ist es gerechtfertigt, diese unter konkreter Benennung von Name, Zeitpunkt und Kontext in einer Liste zu speichern. Von dieser Speicherung sind die Betroffenen zu unterrichten. Eine Unterscheidung zwischen intern und extern geführten Listen kennt das BDSG nicht, sofern personenbezogene Daten erfasst werden. Die in der Hotelliste geführten Daten sind daher auch zu beauskunften. Den Betroffenen stehen nämlich weitere Rechte z. B.

zur Berichtigung, Löschung und Sperrung[116] zu, die sie nur geltend machen können, wenn sie die Eintragung kennen.

Das Hotel hat die Hausverbotsliste nun bei der Zentrale der Hotelkette unter Verwaltung des betrieblichen Datenschutzbeauftragten angelegt. Um Personen in diese Liste aufzunehmen, muss ein substantiiert vorgetragener Grund aufgeführt sein. Die Betroffenen werden über die Speicherung informiert und können dann ihre weiteren Rechte geltend machen.

Hotelverbotslisten sind zulässig. Die datenschutzrechtlichen Vorgaben müssen aber beachtet werden.

5.9 GeoBusiness Code of Conduct – Verhaltensregel zur Geodatennutzung durch Wirtschaftsunternehmen

Im Juli haben wir zum zweiten Mal nach 2012[117] einem Branchenverband beschieden, dass sein Verhaltenskodex mit dem geltenden Datenschutzrecht vereinbar ist. Die entsprechende Anerkennung hatte der Verein Selbstregulierung in der Informationswirtschaft (SRIW e. V.) beantragt, damit die wirtschaftliche Nutzung von Geodaten öffentlicher Stellen durch Unternehmen nach einer anerkannten Selbstverpflichtungserklärung für den Umgang mit den Geodaten erfolgen kann. Das ist deshalb erforderlich, weil es häufig hochauflösende und genaue Geodaten gibt, die einen Personenbezug zulassen. Als Beispiel seien Eigentümerinformationen in Grundstücksdaten genannt, die von der Rohstoffwirtschaft genutzt werden können, um ihre Betriebsplanung weiter zu verbessern; auch Angaben zu denkmalgeschützten Gebäuden, die für die Versicherungswirtschaft relevant sind, gehören dazu. Unternehmen haben die Möglichkeit, der Selbstverpflichtungserklärung beizutreten.[118] Sie müssen nachweisen, dass Geschäftsprozesse den datenschutzrechtlichen Vorgaben genügen. Dazu werden u. a. bestimmte technische und organisatorische Regelungen des Unternehmens in Bezug auf den Datenschutz abgefragt. Den

116 § 35 BDSG
117 JB 2012, 15.1
118 www.geodatenschutz.org

Aufsichtsbehörden wurde der elektronische Zugang zu den Akkreditierungen der Unternehmen ermöglicht. Bislang sind deutschlandweit fünf Unternehmen dem Verhaltenskodex beigetreten.[119]

Die Nutzung von Geodaten öffentlicher Stellen wird durch den jetzt anerkannten GeoBusiness Code of Conduct erleichtert. Nach der EU-Datenschutz-Grundverordnung[120] wird die praktische Bedeutung solcher Verhaltenskodizes noch zunehmen.

119 Stand: 10. Dezember 2015
120 Siehe 2.1.1

6 Jugend

6.1 Ergänzendes Hilfesystem für Betroffene sexueller Gewalt

Aus der Praxis

Der Runde Tisch „Sexueller Kindesmissbrauch in Abhängigkeits- und Machtverhältnissen in privaten und öffentlichen Einrichtungen und im familiären Bereich“ hat in seinem Abschlussbericht empfohlen, ein ergänzendes Hilfesystem (EHS) für diejenigen einzurichten, die in ihrer Kindheit bzw. Jugend sexuellen Missbrauch erlitten haben und noch heute an dessen Folgewirkungen leiden. Dazu sollte über den für den Missbrauch im familiären Bereich eingerichteten Fonds hinaus eine Erweiterung auf den institutionellen Bereich erfolgen. Diejenigen Opfer, die aus den Regelsystemen des Gesundheits- und Sozialwesens keine Leistungen mehr erhalten, können durch das EHS unterstützt werden.

Im institutionellen Bereich haben die einzelnen Bundesländer die Arbeitgeberverantwortung für Missbrauchsfälle, für die Beschäftigte des jeweiligen Landes einstehen müssen, zu übernehmen. Die beim Bund eingerichtete Geschäftsstelle „Fonds sexueller Missbrauch“ nimmt die das EHS betreffenden Anträge entgegen und leitet sie zur Prüfung der Arbeitgeberverantwortung an das zuständige Land weiter.

Bei der Umsetzung des EHS in den Bundesländern trat die Frage auf, inwieweit sich im Rahmen der Prüfung der Arbeitgeberverantwortung durch das jeweilige Bundesland die Notwendigkeit ergeben kann, Informationen über die Täter zu kennen. Insbesondere in Fallkonstellationen, in denen mögliche Täter noch aktiv im Dienst sein könnten, kann es notwendig werden, dienstrechtliche Maßnahmen zu ergreifen. Da eine Erhebung und Weiterleitung von Täternamen durch die beim Bund eingerichtete Stelle nicht erfolgen, oblag es den einzelnen Bundesländern, ein Verfahren zur Prüfung ihrer Arbeitgeberverantwortung zu entwickeln. Hierbei war zu klären, ob die Kenntnis von Daten über den Täter als Voraussetzung für eine Hilfegewährung für erforderlich gehalten wird, um diese dann ggf. direkt bei den Opfern zu erheben.

Die in Berlin für das EHS zuständige Senatsverwaltung für Bildung, Jugend und Wissenschaft hat uns frühzeitig um Beratung im Hinblick auf ein datenschutzgerechtes Verfahren gebeten. Hierbei haben wir die Problematik der Erhebung von Täternamen und die sich daraus ergebenden möglichen Folgen und Konsequenzen für die Opfer intensiv erörtert. In den einzelnen Bundesländern entstand eine uneinheitliche Praxis, da einige Bundesländer die Erhebung der Täternamen verlangen, andere offenbar darauf verzichten. In Berlin hat sich die Senatsverwaltung entschieden, lediglich in denjenigen Fallkonstellationen, in denen in Betracht kommt, dass sich die Täter noch aktiv im Dienst befinden, eine Abfrage des Täternamens mit dem ausdrücklichen Einverständnis der Betroffenen und unter Erläuterung der möglichen Folgen vorzunehmen. Zwischenzeitlich wurde eine Koordinierungsstelle bei der Senatsverwaltung eingerichtet. Zusätzlich hat im Oktober die Beratungsstelle zum Ergänzenden Hilfesystem in Kooperation mit zwei erfahrenen Trägern in der Arbeit mit Betroffenen sexualisierter Gewalt ihre Arbeit aufgenommen. Sie informiert über Antragsvoraussetzungen und bietet Unterstützung bei der Antragstellung.

Wir gehen davon aus, dass mit dem von der Senatsverwaltung für Bildung, Jugend und Wissenschaft gewählten Verfahren den Datenschutzbelangen der oftmals traumatisierten Opfer sexueller Gewalt Rechnung getragen werden kann und ihnen Hilfe durch das ergänzende Hilfesystem zuteilwird.

6.2 Gemeinsame Ausführungsvorschriften für Maßnahmen zum Kinderschutz

Die Senatsverwaltung für Bildung, Jugend und Wissenschaft hat uns den gemeinsam mit der Senatsverwaltung für Gesundheit und Soziales erarbeiteten Entwurf der „Gemeinsamen Ausführungsvorschriften über die Durchführung von Maßnahmen zum Kinderschutz in den Jugend-, Gesundheits- und Sozialämtern des Landes Berlin“[121] zur Prüfung vorgelegt. Die Vorschriften regeln die Zusammenarbeit dieser Ämter bei Kindeswohlgefährdung.

121 AV Kinderschutz JugGesSoz

Eine Neufassung der Ausführungsvorschriften von 2008[122] ist u. a. durch die mit dem Bundeskinderschutzgesetz 2012 geschaffenen Neuregelungen im Bereich des Kinderschutzes notwendig geworden. Allerdings sind wir erst in einem späten Stadium des in einem mehrjährigen Prozess unter Federführung der Senatsverwaltung für Gesundheit und Soziales gemeinsam mit der Senatsverwaltung für Bildung, Jugend und Wissenschaft erarbeiteten Entwurfs der Ausführungsvorschriften beteiligt worden.

Wir haben insbesondere die nicht ausreichende Differenzierung zwischen den im Hinblick auf den Umgang mit Fällen von Kindeswohlgefährdung unterschiedlichen gesetzlichen Aufgabenzuweisungen der Jugend- und der Gesundheitsämter kritisiert. Während der Gesetzgeber den Schutzauftrag bei Kindeswohlgefährdung[123] und damit die Verpflichtung, diese mit den Instrumenten des Kinder- und Jugendhilferechts abzuwenden, den Jugendämtern zuweist, haben die Gesundheitsämter in erster Linie die Aufgaben der Prävention, Gesundheitsförderung, Gesundheitshilfe und die Sicherstellung des Schutzes der Gesundheit für Kinder und Jugendliche wahrzunehmen. Die uns vorgelegten Ausführungsvorschriften nahmen diese Differenzierung der gesetzlichen Aufgaben sowie Verpflichtungen und der daraus folgenden unterschiedlichen datenschutzrechtlichen Befugnisse zur Datenverarbeitung nicht ausreichend vor. Gerade für die einzelfallbezogene Zusammenarbeit zwischen den Jugend- und Gesundheitsämtern ist es jedoch wichtig, die datenschutzrechtlichen Möglichkeiten, aber auch Grenzen der Kooperation aufzuzeigen, um den handelnden Fachkräften in diesem sensiblen Bereich Rechtssicherheit im Umgang mit den datenschutzrechtlichen Vorschriften zu geben.

In konstruktiver Zusammenarbeit mit der Senatsverwaltung für Bildung, Jugend und Wissenschaft ist es uns gelungen, einen gemeinsamen Entwurf der Ausführungsvorschriften abzustimmen. Die notwendige Abstimmung mit der Senatsverwaltung für Gesundheit und Soziales steht noch aus.

122 Gemeinsame Ausführungsvorschriften über die Durchführung von Maßnahmen zum Kinderschutz in den Jugend- und Gesundheitsämtern der Bezirksämter des Landes Berlin (AV Kinderschutz JugGes) vom 8. April 2008

123 § 8a Sozialgesetzbuch – Achtes Buch (SGB VIII)

Die Ausführungsvorschriften sind geeignet, den in den Jugend- und Gesundheitsämtern tätigen Fachkräften die notwendige Rechtssicherheit im Umgang mit Fällen von Kindeswohlgefährdung zu geben und so einen effektiven Kinderschutz unter Beachtung der datenschutzrechtlichen Rahmenbedingungen zu ermöglichen. Im Interesse der Praxis sollten die Ausführungsvorschriften zeitnah in Kraft gesetzt werden.

6.3 Ein neues Fachverfahren für die Jugendhilfe

Die Senatsverwaltung für Bildung, Jugend und Wissenschaft wird sukzessive bis 2018 in den bezirklichen Jugendämtern ein neues Fachverfahren einführen. Das u.a. im Bereich der Gutscheinfinanzierung der Kindertageseinrichtungen in Berlin seit vielen Jahren bewährte Verfahren ISBJ[124] wird als Basis für das neue IT-Fachverfahren ISBJ-Jugendhilfe (ISBJ-JuHi) verwendet werden. Die bisher heterogene Software-Landschaft in den bezirklichen Jugendämtern soll durch ein einheitliches Verfahren abgelöst werden, um eine erhebliche Arbeitsentlastung z. B. durch die Bereitstellung zentraler Dokumentvorlagen oder die Erstellung zentraler Statistiken in den Jugendämtern zu erreichen.

Die Einführung des Verfahrens, das auf der Grundlage der Software SoPart KOMMUNAL[125] realisiert wird, erfolgt in mehreren Stufen. Die erste Stufe betrifft den Arbeitsbereich Wirtschaftliche Jugendhilfe (WJH). Die zweite Stufe umfasst die Arbeitsbereiche Allgemeiner Sozialer Dienst (ASD) und die dritte Stufe umfasst die Arbeitsbereiche Amtsvormundschaften/Unterhaltsvorschuss/Beistandschaft (AV/UV).

Da die Verarbeitung und Nutzung der Sozialdaten den gleichen datenschutzrechtlichen Vorgaben unterliegen, die auch bei der herkömmlichen Aktenführung gelten, war es notwendig, die rechtlichen Anforderungen schon in den Planungen zu berücksichtigen. Die Senatsverwaltung für Bildung, Jugend und Wissenschaft hat uns bereits in den Prozess der Ausschreibung der Software

124 Integrierte Software Berliner Jugendhilfe
125 Die Software wird bereits in Teilen der Berliner Justiz eingesetzt.

einbezogen. Da die bezirklichen Jugendämter als eigenständige datenverarbeitende Stellen anzusehen sind, war es für uns entscheidend, dass die Software die notwendige Mandantenfähigkeit aufweist und damit die Möglichkeit zur Begrenzung der Zugriffsrechte auf die bezirkseigenen Jugendhilfedaten umsetzen konnte. Die Senatsverwaltung hat die rechtlichen Anforderungen berücksichtigt, sodass die notwendige Trennung der Datenbestände gewährleistet ist.

Angesichts der Komplexität des IT-Fachverfahrens und der besonderen Sensitivität der verarbeiteten Sozialdaten der Jugendhilfe ist es notwendig, die Implementierung auch unter Datensicherheitsaspekten intensiv zu begleiten. Die Beteiligten haben auch hier die Datenschutzvorgaben weitgehend bereits umgesetzt. 2015 konnten die Planungen zur Einführung von ISBJ Jugendhilfe für den Bereich der Wirtschaftlichen Jugendhilfe abgeschlossen werden. Ziel ist es, 2016 nach einer Pilotierungsphase in den Bezirksämtern Mitte, Neukölln und Treptow-Köpenick die bisher in diesem Bereich eingesetzte Software abzulösen.

Wir befinden uns mit der Senatsverwaltung für Bildung, Jugend und Wissenschaft in einem konstruktiven Abstimmungsprozess und erwarten, dass die datenschutzrechtlichen Anforderungen auch bei den weiteren Schritten der Einführung des neuen IT-Fachverfahrens berücksichtigt werden.

6.4 Videoaufnahmen in Kitas

Aus der Praxis

Im vergangenen Jahr berichteten wir darüber, dass im Rahmen eines vom Bundesministerium für Familie, Senioren, Frauen und Jugend geförderten und vom Deutschen Jugendinstitut bundesweit durchgeführten Projektes zur Sprachförderung im Kitaalltag Videoaufnahmen von Kindern und pädagogischen Fachkräften angefertigt worden sind. Die vom Deutschen Jugendinstitut für die Anfertigung und Nutzung der Videoaufnahmen entwickelten Einverständniserklärungen genügten nicht den datenschutzrechtlichen Anforderungen.[126]

126 JB 2014, 4.1

Das Bundesministerium, das das Projekt mit erheblichen Finanzmitteln gefördert hat, hat mit uns unter Beteiligung der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie der Senatsverwaltung für Bildung, Jugend und Wissenschaft die Problematik im Hinblick auf die Videoaufnahmen der Kinder und der pädagogische Fachkräfte erörtert. Das Ministerium hat signalisiert, die bestehenden Bedenken aufgreifen zu wollen und zukünftig umfassender die Datenschutzbelange in entsprechenden Projekten zu regeln. Bei künftigen Projektförderungen, insbesondere solchen, in denen pädagogische Materialien mittels Medien erarbeitet werden, solle zukünftig stets ein Datenschutzkonzept verlangt werden. Auch solle eine enge Abstimmung mit der behördlichen Datenschutzbeauftragten erfolgen.

Für das zugrunde liegende Projekt zur Sprachförderung, in dem ein multimediales Handbuch erarbeitet worden ist, konnte die zuständige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit einige Verbesserungen wie eine teilweise Verpixelung der Gesichter unter Verzicht auf die Nennung von Namen der Kinder und pädagogischen Fachkräfte erreichen.

Die Senatsverwaltung für Bildung, Jugend und Wissenschaft hat an uns den Wunsch herangetragen, dass wir Handlungsleitlinien entwickeln. Wir haben entsprechende Hinweise zum datenschutzgerechten Umgang mit Foto-, Video- und Tonaufnahmen in Kindertageseinrichtungen entworfen. Diese Hinweise befinden sich derzeit in der Abstimmung mit der Senatsverwaltung für Bildung, Jugend und Wissenschaft.

Wir gehen davon aus, dass Handlungsleitlinien helfen, mehr Rechtssicherheit im Umgang mit den neuen Medien im pädagogischen Alltag der Kindertageseinrichtungen zu erreichen und so den Datenschutzbelangen wirksam Rechnung zu tragen.

6.5 Nachbesserungen bei den Kita-Eigenbetrieben

Aus der Praxis

Bei dem Verfahren Kita Portal handelt es sich um ein Fachverfahren, welches von allen dem Kita-Eigenbetrieb Nord-Ost zugehörigen Kitas genutzt werden soll. Das Kita Portal ist eine Webanwendung zur Unterstützung der Verwaltungsarbeit in den Kindertagesstätten und der Verwaltung des Kita-Eigenbetriebes. Es werden personenbezogene Daten der Kinder, ihrer Familien und der Beschäftigten verarbeitet.

Die uns vorgelegten Unterlagen mussten mehrfach überarbeitet werden, da die erörterten Anforderungen zunächst nicht ausreichend umgesetzt wurden. Ergänzungs- und Änderungsbedarf wurde insbesondere in dem vorgelegten Rollen- und Berechtigungskonzept, dem Protokollierungskonzept sowie der Dateibeschreibung festgestellt.

Rollen- und Berechtigungskonzept
Als wesentlicher Bestandteil der Sicherheit wurden die Zugriffsrechte überprüft. So wurde der nicht begründete und nicht nachvollziehbare Zugriff auf die Daten des Bildungsgutscheins durch das Sekretariat der Geschäftsleitung inzwischen unterbunden. Bei weiteren Rollen, wie z. B. dem Controlling, wurde dahingehend nachgebessert, dass nun besser nachvollziehbar ist, welche Zugriffe bezüglich der umfangreichen Aufgaben notwendig sind. Einige Berechtigungen bedürfen jedoch noch einer aufmerksamen Betrachtung.

Protokollierungskonzept
Da im Rechte- und Rollenkonzept weitreichende Zugriffsrechte definiert wurden, kommen der Protokollierung und der Auswertung von Zugriffen eine erhebliche Bedeutung zu. Dies betraf vor allem den Aufbau der Protokolldatensätze (was wird protokolliert) und die Auswertung der Protokolle. Den Hinweisen wurde weitgehend gefolgt. So werden sämtliche Verarbeitungen (lesender, schreibender, löschender Zugriff) nutzerbezogen protokolliert und regelmäßig ausgewertet. Anhaltspunkte für eine datenschutzgerechte Protokollierung zur Gewährleistung der Revisionsfähigkeit[127] gibt die Orientierungshilfe „Protokollierung“ des Arbeitskreises Technik.[128]

127 § 5 Abs. 2 Nr. 5 BlnDSG
128 Abrufbar unter http://www.datenschutz-berlin.de/attachments/637/oh-proto.pdf

Bei der Löschung der Protokolldaten sind noch Unklarheiten vorhanden, die einer weiteren Abklärung bedürfen. Grundsätzlich gilt, dass eine kurze Aufbewahrungsdauer zu begrüßen ist, jedoch sollte sichergestellt sein, dass die Daten nicht vor Auswertung gelöscht werden. Die Auswertung sollte generell im Vier-Augen-Prinzip erfolgen.

Dateibeschreibung

Für jede automatisierte Datenverarbeitung muss die datenverarbeitende Stelle eine Dateibeschreibung nach bestimmten Vorgaben fertigen.[129] Diese kann von jeder Person unentgeltlich beim behördlichen Datenschutzbeauftragten eingesehen werden. Sinn dieser Vorschrift ist, dass sich Betroffene selbst ein Bild über die Verarbeitung ihrer personenbezogenen Daten und der ergriffenen Maßnahmen zum Schutz dieser Daten machen können.

Wir haben empfohlen, die Dateibeschreibung so zu formulieren, dass dieses Recht auch sinnvoll wahrgenommen werden kann. Dazu ist es wichtig, die Formulierungen so zu wählen, dass die Sicherheit des technischen Verfahrens nicht beeinträchtigt wird und Bürgerinnen und Bürger sie verstehen. Verweise auf Sicherheitskonzepte oder ähnliche Unterlagen sollten vermieden werden. Vielmehr sollten die ergriffenen technisch-organisatorischen Maßnahmen allgemeinverständlich in einer Übersicht dargestellt werden.

Bei der Einführung neuer Fachverfahren sollte unsere Behörde möglichst frühzeitig einbezogen werden. Auf diese Weise lassen sich langwierige Abstimmungsprozesse häufig vermeiden.

129 Siehe § 19 Abs. 2 BlnDSG

7 Soziales

7.1 Entwurf eines Prostituiertenschutzgesetzes

Aus der Praxis

Wir haben gegenüber der Senatsverwaltung für Arbeit, Integration und Frauen zum Referentenentwurf eines Prostituiertenschutzgesetzes (ProstSchG) des Bundesministeriums für Familie, Senioren, Frauen und Jugend Stellung genommen. Ausweislich der Gesetzesbegründung soll das ProstSchG dazu beitragen, die in der Prostitution Tätigen besser zu schützen, ihr Selbstbestimmungsrecht zu stärken und Kriminalität in der Prostitution zu bekämpfen.[130] Zu diesem Zweck sieht der Entwurf u.a. eine Anmeldepflicht für die Aufnahme der Tätigkeit als Prostituierte oder Prostituierter, die Ausstellung einer Anmeldebescheinigung nach Durchführung einer obligatorischen gesundheitlichen Beratung sowie Kontrollen von Räumen und Personen vor. Bei Verstößen gegen die Anmelde- und Beratungspflicht sollen Anordnungen gegenüber den Prostituierten erlassen werden können.

Zwar regelt der Referentenentwurf in allgemeiner Form die Verarbeitung personenbezogener Daten, lässt aber offen, für welche konkreten Stellen diese Regelungen gelten sollen. Da die Länder das geplante Gesetz auszuführen haben, regeln die Länder auch die Einrichtung oder Benennung der zuständigen Behörden und das Verwaltungsverfahren. Solange dies nicht geschehen ist, lässt sich nicht abschließend beurteilen, inwieweit die Verarbeitung personenbezogener Daten durch diese Behörden erforderlich ist.

Ob die vorgesehene Anmeldepflicht ein geeignetes Mittel zum besseren Schutz der Prostituierten ist, wird in der öffentlichen Diskussion teilweise bezweifelt. Der Entwurf sieht immerhin vor, dass die Betroffenen wählen können, ob auf ihrer Anmeldebescheinigung, die sie bei Kontrollen vorzeigen müssen, ihr Klarname oder ein Pseudonym eingetragen wird. Wir haben empfohlen, die Ausstellung einer pseudonymisierten Anmeldebescheinigung als Regelfall vorzusehen. Diese sollte neben dem Lichtbild lediglich den für die Prostitutionstätigkeit gewählten Alias-Namen, die angemeldeten Tätigkeitsorte, den

130 Siehe S. 32 des Referentenentwurfs

Gültigkeitszeitraum und die ausstellende Behörde enthalten. Weitere Angaben sind weder für die Überprüfung, ob die oder der Prostituierte eine tatsächlich für sie bzw. ihn ausgestellte Bescheinigung mit sich führt, noch für die Einleitung weiterer ordnungsrechtlicher Maßnahmen erforderlich.

Die zur Verhütung dringender Gefahren für die öffentliche Sicherheit und Ordnung vorgesehene Befugnis, Grundstücke, Geschäftsräume und Räumlichkeiten, auch wenn sie zugleich Wohnzwecken dienen, jederzeit betreten zu können, begegnet verfassungsrechtlichen Bedenken. Es ist nämlich fraglich, ob die verfassungsunmittelbare Schranke des Art. 13 Abs. 2 GG beachtet wird. Danach dürfen Durchsuchungen nur durch den Richter, bei Gefahr im Verzug auch durch die in den Gesetzen vorgesehenen anderen Organe angeordnet und nur in der dort vorgeschriebenen Form durchgeführt werden.

Aufgrund der genannten Kritikpunkte und verfassungsrechtlichen Bedenken sollte der Referentenentwurf eines Prostituiertenschutzgesetzes überarbeitet werden.

7.2 Übersendung vollständiger Schwerbehindertenakten zur externen Begutachtung

Das Landesamt für Gesundheit und Soziales (LAGeSo) hat vollständige Schwerbehindertenakten zwecks Feststellung des Grades der Behinderung an externe Gutachterinnen und Gutachter versandt. Es hat dafür keine Einwilligungen der Betroffenen eingeholt, sondern diese zu Beginn des Verwaltungsverfahrens lediglich allgemein auf ein Widerspruchsrecht hingewiesen. Die Auswahl der begutachtenden Person und die Übermittlung an diese erfolgten somit ohne Kenntnis und ohne Einwilligung der Betroffenen.

Das Vorgehen des LAGeSo war unzulässig. Die Übermittlung der vollständigen Schwerbehindertenakte an externe Gutachterinnen und Gutachter ohne vorherige Unterrichtung der Betroffenen war nicht erforderlich, da eine zumutbare Alternative bestand. Denn bereits bei der Bewilligung bzw. Festsetzung von Sozialleistungen lassen sich die Zeiträume für spätere Begutachtungen festlegen.

Solche Untersuchungen sind demnach planbar, sodass die Betroffenen zeitnah über die Einschaltung einer Gutachterin oder eines Gutachters und die damit verbundene Übermittlung ihrer Sozialdaten informiert werden können.

Die bisherige Vorgehensweise des LAGeSo ließ das Widerspruchsrecht der Betroffenen gegen die Übermittlung von Sozialdaten an die konkrete Gutachterin oder den konkreten Gutachter ins Leere laufen. Da die Betroffenen das Widerspruchsrecht aber auch nach Beginn des Verwaltungsverfahrens jederzeit ausüben können müssen, ist es aus Gründen der Verfahrenstransparenz geboten, dass sie rechtzeitig die Information erhalten, an welche Gutachterin oder welchen Gutachter die Sozialdaten übermittelt werden sollen. Bisher waren die Betroffenen gezwungen, vorsorglich der Übermittlung ihrer Daten an jegliche externe begutachtende Person zu widersprechen, selbst wenn sie nur die Übermittlung an eine bestimmte Person ausschließen möchten. Damit würden die Betroffenen faktisch die Begutachtung als solche ablehnen und hätten die möglichen Folgen bis hin zur Ablehnung des Antrages wegen Verletzung der Mitwirkungspflichten zu tragen. Dies ist eine unangemessene Benachteiligung der Betroffenen.

Aus Gründen der Handhabbarkeit des Verfahrens haben wir vorgeschlagen, die Unterrichtung über eine geplante, konkrete Übermittlung mit einem Hinweis auf das Bestehen einer Widerspruchsmöglichkeit zu verbinden.

Das LAGeSo hat unsere Empfehlungen aufgegriffen und das Verfahren überarbeitet.

Die Betroffenen müssen über jede geplante Begutachtung zur Feststellung des Grades der Behinderung durch externe Gutachterinnen und Gutachter informiert und darauf hingewiesen werden, dass sie der Datenübermittlung an die begutachtende Person widersprechen können.

7.3 Probleme in Seniorenheimen

7.3.1 Ärztliche Gutachten als Aufnahmebedingung?

Eine Bürgerin hat sich darüber beschwert, dass die Liegenschaftsverwaltung eines Bezirksamtes für die Anmietung einer Wohnung in einem Seniorenwohnhaus die Vorlage eines ärztlichen Gutachtens verlangt.

Hierzu hat uns die Liegenschaftsverwaltung mitgeteilt, anhand der ärztlichen Gutachten solle geprüft werden, ob die Mieterinnen und Mieter selbstständig und ohne fremde Hilfe in den Wohnungen leben können. Personal für Betreuung und Pflege sei in den Seniorenwohnhäusern nicht vorgesehen. Ein Arztgespräch vor dem Umzug in ein Seniorenwohnhaus biete die Gelegenheit, mit einer „neutralen", jedenfalls nicht zu den Angehörigen zählenden Person unter Berücksichtigung des Gesundheitszustandes nachzudenken, ob noch einmal in eine andere Wohnung oder stattdessen gleich in ein Heim mit entsprechend ausgebildetem Pflege- und Betreuungspersonal gezogen werden solle.

Da mit der Anmietung einer Wohnung in einem Seniorenwohnhaus keine Pflegedienstleistungen einhergehen, handelt es sich um normale Wohnungsmietverträge. Die Entscheidung darüber, Dienstleistungen eines Pflegedienstes o. Ä. in Anspruch nehmen zu wollen, treffen somit die Bewohnerinnen und Bewohner bzw. deren Angehörige (wie bei anderen Mietverhältnissen auch) unabhängig von dem mit der Liegenschaftsverwaltung bestehenden Mietverhältnis. Deshalb war nicht erkennbar, wofür die Liegenschaftsverwaltung in ihrer Funktion als Vermieterin Gesundheitsdaten der Bewohnerinnen und Bewohner benötigt. Wir haben darauf hingewiesen, dass die Anforderung ärztlicher Bescheinigungen unter diesen Umständen unzulässig ist, und angeregt, zukünftig ein Informationsblatt an die Wohnungsinteressenten herauszugeben. Wir haben empfohlen, in diesem Informationsblatt zunächst die Erwägungen zur Frage des Umzugs in eine Wohnung oder ein Pflegeheim darzulegen und den Bewerberinnen und Bewerbern ein diesbezügliches Gespräch mit einem Arzt oder einer „neutralen" Person nahezulegen.

Die Liegenschaftsverwaltung hat uns mitgeteilt, dass man aufgrund unserer Hinweise nunmehr gänzlich auf die Anforderung ärztlicher Bescheinigungen

verzichte. Unserer Anregung folgend werde man ein Informationsblatt für Wohnungsinteressenten erstellen, sobald dies zeitlich möglich sei. Bis dahin werde man die Bewerberinnen und Bewerber im Rahmen eines Gespräches bitten, die Vor- und Nachteile eines Umzugs in die Seniorenwohnhäuser zu bedenken.

Die Liegenschaftsverwaltung als Vermieterin von Seniorenwohnungen kann den Bewerberinnen und Bewerbern ein Gespräch mit einem Arzt zum Für und Wider des Umzugs in eine Seniorenwohnung nahelegen, darf aber selbst keine Gesundheitsdaten anfordern. Die Vermietung einer Seniorenwohnung darf nicht von der Vorlage eines ärztlichen Gutachtens abhängig gemacht werden.

7.3.2 Biografiefragebogen

Aus der Praxis

Die Bewohnerinnen und Bewohner eines Pflegeheims haben sich darüber beschwert, dass das Pflegeheim detaillierte biografische Angaben von ihnen erfragen wollte. Dafür wurde ihnen ein umfangreicher Fragebogen mit der Bitte vorgelegt, diesen auszufüllen. Er enthielt detaillierte Fragen, die z. T. intime Angaben verlangten.

Wir haben uns an das Pflegeheim gewandt und betont, dass wir den Nutzen, den ein solcher Fragebogen in der Biografiearbeit haben kann, nicht in Frage stellen wollen. Der Nutzen ist vor allem darin zu sehen, dass die Einbeziehung der gesammelten Informationen eine persönlichkeitsfördernde und individuelle Pflege und Betreuung ermöglicht. Gleichwohl gab es zu bedenken, dass hiermit eine umfangreiche Erhebung und Verarbeitung personenbezogener, teilweise äußerst sensitiver Daten verbunden ist. Sammelt das Pflegeheim solche biografischen Angaben, greift es in das Recht der Pflegeheimbewohnerinnen und -bewohner auf informationelle Selbstbestimmung ein.

Biografiearbeit kann nur auf freiwilliger Basis erfolgen. Eine Erhebung und Verarbeitung von Biografiedaten setzt deshalb voraus, dass die Betroffenen darin einwilligen. Dieser Einwilligung muss eine umfassende schriftliche und verständliche Aufklärung, insbesondere über Sinn und Zweck der Biografiearbeit, vorausgehen. Hierbei muss deutlich werden, dass durch die Nichtangabe

von Informationen keine Nachteile entstehen. Es ist zudem darauf zu achten, dass nur solche Daten erfragt werden, die für die Durchführung des vom Pflegeheim praktizierten Konzepts zur Biografiearbeit auch tatsächlich benötigt werden.

Das Pflegeheim hat den Biografiefragenbogen sowie ein dazugehöriges Informationsblatt anhand unserer Vorgaben überarbeitet. In dem Informationsblatt wird jetzt gut sichtbar auf die Freiwilligkeit der Angaben hingewiesen, zudem wird die Datenverarbeitung verständlich erläutert. Auch die Einwilligungserklärung ist verständlich formuliert und optisch hervorgehoben. Aus dem Fragebogen wurden zahlreiche Fragen entfernt, u.a. zum Umgang mit Erkrankungen, mit dem Tod und mit Konfliktsituationen.

Biografiearbeit in Pflegeheimen ist nur auf freiwilliger Basis möglich und setzt eine informierte Einwilligung der Betroffenen voraus.

7.4 Sozialamt fragt Dritte nach Bargeldnachlass

Ein Sozialamt ist nach dem Tod einer von einem Pflegedienst betreuten Person schriftlich an diesen Pflegedienst herangetreten. Das Sozialamt hat den Pflegedienst um Auskünfte zum verbliebenen Bargeldnachlass der verstorbenen Person, konkret zur Höhe des Nachlasses und an wen der Nachlass ggf. ausgezahlt worden ist, gebeten.

Das Anschreiben des Sozialamtes entsprach nicht den gesetzlichen Vorgaben. Die Erhebung der Angaben zum Bargeldnachlass mithilfe dieses Anschreibens war daher unzulässig.

Anders als das Sozialamt zunächst meinte, handelt es sich bei den erfragten Angaben um Sozialdaten. Das sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), die von einem Sozialleistungsträger im Hinblick auf seine Aufgaben nach dem Sozialgesetzbuch erhoben, verarbeitet oder genutzt werden.[131]

131 § 67 Abs. 1 Satz 1 SGB X

Entscheidend für die Einordnung als Sozialdatum sind die Personenbezogenheit und der funktionale Zusammenhang mit der Aufgabenerfüllung. Beides ist bei den Informationen zum Bargeldnachlass einer verstorbenen Person der Fall. Zum einen bezieht sich die Nachfrage zum Bargeldnachlass auf eine konkrete Person. Zum anderen dienen die erbetenen Auskünfte, wie das Sozialamt selbst mitteilte, der Erfüllung einer dem Sozialamt obliegenden Aufgabe, nämlich der Prüfung des Nachlasses im Rahmen von Kostenersatz durch die Erben bzw. bei der Übernahme der Bestattungskosten.

Bittet das Sozialamt einen Pflegedienst um Auskünfte zum Nachlass einer verstorbenen Person, erhebt es Sozialdaten bei einer nicht-öffentlichen Stelle und nicht direkt bei der betroffenen Person bzw. deren Erben. In solchen Fällen muss das Sozialamt auf die Rechtsvorschrift, die zur Auskunft verpflichtet, oder aber auf die Freiwilligkeit der erfragten Angaben hinweisen.[132] Durch diese Hinweispflicht wird vermieden, dass eine nicht-öffentliche Stelle Sozialdaten übermittelt, ohne dazu verpflichtet zu sein. Dies wird jedoch, wie auch die an uns herangetragene Anfrage des Pflegedienstes zeigt, typischerweise der Fall sein, wenn eine Behörde hoheitlich um Mitteilung bestimmter Angaben bittet. Die Hinweispflicht dient somit der Herstellung von Verfahrenstransparenz.

Das Sozialamt benannte in seinem Anschreiben weder eine zur Auskunft verpflichtende Rechtsvorschrift noch wies es auf die Freiwilligkeit der Angaben hin. Wir haben gegenüber dem Sozialamt einen Mangel festgestellt.[133] Daraufhin hat das Sozialamt den dem Anschreiben zugrundeliegenden Vordruck nach den gesetzlichen Vorgaben überarbeitet. Der Vordruck weist nunmehr auf die Freiwilligkeit der Angaben hin.

Werden Sozialdaten statt beim Betroffenen bei einer nicht-öffentlichen Stelle erhoben, muss diese, sofern es keine Auskunftspflicht gibt, ausdrücklich auf die Freiwilligkeit der Angaben hingewiesen werden.

132 § 67 a Abs. 4 SGB X
133 § 26 Abs. 2 BlnDSG

8 Gesundheitswesen

8.1 Verordnung zum öffentlichen Gesundheitsdienst – noch immer Fehlanzeige

Nachdem wir bereits Anfang 2013 zu einem von der Senatsverwaltung für Gesundheit und Soziales vorgelegten Entwurf einer Verordnung zur Regelung der Datenverarbeitung in Einrichtungen des öffentlichen Gesundheitsdienstes (DatVO) Stellung genommen haben, ist die angestrebte Rechtsverordnung noch immer nicht erlassen worden.

Durch den Erlass der DatVO sollen die im Gesetz des öffentlichen Gesundheitsdienstes (GDG) enthaltenen Ermächtigungsgrundlagen umgesetzt werden. Das GDG sieht zum einen eine Ermächtigungsgrundlage zur Regelung der Verarbeitung personenbezogener Daten, insbesondere über ihre Verarbeitung in Dateien und auf sonstigen Datenträgern, ihre Übermittlung, ihre Löschung sowie die Datensicherung vor. Zum anderen ermächtigt das Gesetz zur Regelung der Verarbeitung von Daten über die Angehörigen der staatlich geregelten Berufe des Gesundheitswesens und zur Regelung der Statistiken für die integrierte Gesundheits- und Sozialberichtserstattung. Mit der Rechtsverordnung sollen die für die Tätigkeit des öffentlichen Gesundheitsdienstes zwingend erforderlichen Datenverarbeitungen auf eine rechtliche Grundlage gestellt werden.

Der Erlass der Rechtsverordnung ist in der Vergangenheit nicht mit der gebotenen Intensität vorangebracht worden, sodass in den Gesundheitsämtern erforderliche Datenverarbeitungen teilweise ohne Rechtsgrundlage erfolgen. Unabhängig davon begrüßen wir unsere frühzeitige Einbindung in die im Sommer wieder aufgenommene Arbeit an der Verordnung.

Bei der DatVO handelt es sich um eine wesentliche Rechtsgrundlage für die erforderliche Datenverarbeitung im öffentlichen Gesundheitsbereich. Der Erlass dieser Rechtsverordnung ist überfällig.

8.2 Einführung des klinischen Krebsregisters

Anknüpfend an unsere Beratung in den Vorjahren begleiteten wir zusammen mit der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg intensiv die Vorbereitung der gesetzlichen Regelungen zur klinischen Krebsregistrierung in den Ländern Berlin und Brandenburg.134 Im Sommer begann die Erarbeitung des Staatsvertrages zur Errichtung des gemeinsamen klinischen Krebsregisters.

Es soll eine Datengrundlage zur Verbesserung der Qualität der onkologischen Versorgung bereitstellen. Die behandelnden Ärztinnen und Ärzte erhalten zum einen Informationen zur Qualität ihrer Behandlung und zum anderen werden ihnen Angaben über alle diagnostischen und therapeutischen Schritte der Mitbehandelnden zur Verfügung gestellt. Die Sensitivität des Datenbestandes des Krebsregisters ergibt sich daraus, dass alle Krebserkrankten in Berlin und Brandenburg erfasst und weitreichende Informationen über ihren Gesundheitszustand zusammengeführt werden.

Die auf unsere Anregung gestärkte Widerspruchsregelung ermöglicht den Patienten, zumindest darüber entscheiden zu können, ob und in welchem Umfang ihre medizinischen Daten Eingang in das Krebsregister finden. Einerseits können sie der Speicherung dieser Daten generell widersprechen. Andererseits können sie, wenn sie dies wünschen, erreichen, dass das Tätigwerden einer Ärztin oder eines Arztes nicht in die Registerdaten eingeht und so auch nicht den anderen Leistungserbringern bekannt wird. Unabhängig vom Willen der Krebserkrankten wird jedoch in jedem Fall die Tatsache der Erkrankung vom Register erfasst. Nicht übernommen wurde die von uns vorgeschlagene Regelung, dass die erkrankte Person durch ihren Widerspruch gegenüber den behandelnden Leistungserbringern erreichen kann, dass diese gar nicht erst Daten an das Register übermitteln.

Eine Gliederung des Registers in eigenverantwortliche Bereiche dient dazu, für jede dem Register zugewiesene Aufgabe die Datengrundlage bereitzustellen, die für die jeweilige Tätigkeit benötigt wird. Am wichtigsten ist dabei die

134 Siehe JB 2014, 5.2

Unterscheidung zwischen identifizierenden Angaben wie dem Namen und der Adresse einerseits und den medizinischen Daten andererseits. Diese Differenzierung wird mit dem vorliegenden Entwurf erreicht:

Wer eine Meldung aufnimmt und auf Vollständigkeit und Plausibilität prüft oder verschiedene Meldungen in einem Verlaufsdatensatz zusammenfasst, der benötigt nur den Zugriff auf die Daten der jeweiligen einzelnen Person, darf jedoch auch ihren Namen erfahren, wenn eine Rückfrage bei dem meldenden Arzt erforderlich ist. Dies gilt entsprechend für die Abrechnung mit den Krankenkassen und Versicherungen und Rückmeldung zu der Qualität der Behandlung eines einzelnen Patienten. Die Personen, die in diesem verantwortungsvollen Bereich tätig sind, werden in einem Versorgungsbereich zusammengefasst, der personell und organisatorisch von den anderen Bereichen getrennt wird.

Werden Daten z. B. zur Überprüfung der Einhaltung medizinischer Behandlungsleitlinien ausgewertet, kann dies ohne Kenntnis der Namen der Patienten geschehen. Diese und andere qualifizierte medizinische Analysen werden einem Auswertungsbereich zugeordnet. Hier stehen patientenidentifizierende Angaben nicht zur Verfügung.

Die Datenspeicherung ist eine nicht auf Dritte außerhalb des Registers übertragbare Aufgabe. Sie erfolgt zentral in einer Koordinierungsstelle, die daneben die verwaltungstechnischen Aufgaben des Registers wahrnimmt. Die Beschäftigten der Koordinierungsstelle dürfen dabei nicht auf die Daten der anderen Bereiche zugreifen. Verschlüsselung und weitergehende Datenbanktechniken sichern diese Zugriffsbeschränkung ab.

Auch Zugriffe Dritter müssen durch technische Sicherungsmaßnahmen verhindert werden. Der gebündelte Datenbestand besitzt einen erheblichen monetären Wert. Die sich hieran entzündenden Begehrlichkeiten sind bei der Wahl der Sicherungsmaßnahmen zu berücksichtigen. Zwar liegen uns Planungen zur einzusetzenden Informationstechnik vor, jedoch wurden trotz der geplanten nahen Inbetriebnahme die Sicherheitsbetrachtungen noch nicht soweit vorgenommen, dass eine vernünftige Planung möglich ist.

Wir begrüßen die intensive Einbeziehung unseres Hauses bei der Vorbereitung der rechtlichen Grundlagen für die zukünftige klinische Krebsregistrierung. Wichtige Grundsätze des Datenschutzes konnten so in einem frühen Stadium Eingang finden. Trotz des hohen Zeitdrucks und des engen finanziellen Rahmens muss bei der nunmehr anstehenden Errichtung des Registers ein adäquater Schutz des Datenbestandes erreicht werden.

8.3 Outsourcing der Archivierung von Patientenakten

Bei einem Krankenhausverbund prüften wir die Vergabe von Leistungen zur Verarbeitung von Patientendaten an Dritte, insbesondere die Archivierung der Patientenakten.

Das Berliner Landeskrankenhausgesetz stellt an die Vergabe von Aufträgen zur Verarbeitung von Patientendaten – worunter auch die Archivierung von Patientenakten fällt – klare Anforderungen. Danach ist es zulässig, eine andere Stelle mit der Verarbeitung von Patientendaten zu beauftragen. Ist diese jedoch kein Krankenhaus, muss sichergestellt werden, dass die verarbeitende Stelle keine Möglichkeit hat, die Namen der Patienten und andere identifizierende Daten zur Kenntnis zu nehmen. Wir prüfen sukzessive die Krankenhäuser auf die Einhaltung dieser Bestimmungen.

Im Rahmen der Prüfung des Krankenhausverbundes mussten wir Defizite bei der Umsetzung der rechtlichen Rahmenbedingungen im Hinblick auf die Archivierung feststellen. Der Krankenhausverbund übergab seine Patientenakten an einen externen Dienstleister, der sie in unverschlossenen Behältnissen aufbewahrte. Wurde eine Akte vom Krankenhaus benötigt, suchte sie der Dienstleister anhand der patientenidentifizierenden Daten heraus und versandte sie an das Krankenhaus. Dabei war es ihm möglich, Einsicht in die Patientenakte zu nehmen. Dies stellt eine Verletzung der ärztlichen Schweigepflicht und einen Verstoß gegen die datenschutzrechtlichen Bestimmungen dar.

Der Krankenhausverbund hat daraufhin ein Konzept entwickelt, um dem festgestellten Mangel zu begegnen. Die Behältnisse sollen versiegelt und nummeriert werden. Bei Bedarf sollen die Behälter anhand ihrer Nummer ausgewählt

und im versiegelten Zustand mit allen enthaltenen Akten dem Krankenhaus überstellt werden. Wir haben auf notwendige Ergänzungen hingewiesen, mit denen sichergestellt wird, dass das Krankenhaus einen Siegelbruch feststellen und mit einer Vertragsstrafe sanktionieren kann.

Der Krankenhausverbund hat angekündigt, die gesetzlichen Anforderungen im Zuge eines bevorstehenden Anbieterwechsels und der damit verbundenen Umlagerung der Akten umzusetzen.

Krankenhäuser müssen bei der Auslagerung von aufbewahrungspflichtigen Altakten dafür sorgen, dass der Dienstleister die Inhalte der Akten nicht zur Kenntnis nehmen kann. Dafür stehen praktikable Lösungen bereit.

8.4 Charité Universitätsmedizin Berlin

8.4.1 Mangelhafte Verfahrensführung: Sicherheitskonzepte und Kontrolle fehlen

Wir haben die Einhaltung der gesetzlichen Vorgaben zur Einführung von neuen IT-Verfahren und Führung eines Verzeichnisses dieser Verfahren [135] bei der Charité geprüft. Dabei mussten wir gravierende Defizite feststellen, die beanstandet wurden.

Die Charité ist das größte Universitätsklinikum Deutschlands. An vier Standorten mit mehr als 3.000 Krankenbetten arbeiten mehr als 13.000 Personen, darunter mehr als 3.700 Ärztinnen und Ärzte. Die Charité arbeitet hochgradig innovativ und mit modernsten diagnostischen und therapeutischen Methoden. Viele hiervon werden durch Informationstechnik unterstützt, die einer ständigen Fortentwicklung unterworfen ist.

Bei der Einführung neuer Verfahren der Informationstechnik, mit denen Patientendaten verarbeitet werden, ist besondere Sorgfalt vonnöten. Wiewohl die Gesundung der Patienten das primäre Ziel darstellt und auch

135 § 5 Abs. 3, § 19 BlnDSG

Effizienzgesichtspunkte Berücksichtigung finden müssen, ist bei alldem auch der Schutz der Angaben über den Gesundheitszustand der Erkrankten vor unbefugter Offenlegung und die Wahrung der Rechte der Patienten zu gewährleisten.

Dazu hat der Gesetzgeber bestimmt, dass vor Einführung eines neuen Verfahrens eine Reihe von Schritten zu gehen sind: Erstens sind die durch das Verfahren entstehenden Risiken zu bewerten und Maßnahmen zu ihrer Begrenzung zu finden.[136] Zweitens sind diese Maßnahmen in einem systematischen Sicherheitskonzept zu bündeln. Drittens hat die oder der behördliche Datenschutzbeauftragte das Verfahren auf verbleibende Restrisiken zu prüfen.[137] Auf der Basis des Votums der oder des Datenschutzbeauftragten trifft dann die Krankenhausleitung die Entscheidung über die Umsetzung des Verfahrens. Die geplanten Maßnahmen werden vor Aufnahme des Verfahrens umgesetzt. Zum Schluss werden das Verfahren, seine Zwecke, die verarbeiteten Daten, die Schutzmaßnahmen und die durchlaufenen Prüfschritte in einem in wesentlichen Teilen öffentlich einsehbaren Verzeichnis dokumentiert.

Damit ist auch Transparenz geschaffen: Jeder einzelne Bürger kann ohne weitere Voraussetzungen nachvollziehen, wie das Krankenhaus mit den Daten umgeht. Und sowohl interne wie öffentliche Datenschutzaufsicht können auf das Verzeichnis zurückgreifen, um regelmäßig zu überprüfen, ob der Schutz der Daten noch immer gewährleistet ist oder ggf. zusätzliche Maßnahmen ergriffen werden müssen.

Im Vorfeld einer Überprüfung technischer Datenschutzmaßnahmen bei der Charité haben wir uns das Verfahrensverzeichnis vorlegen lassen. Dabei zeigten sich gravierende Lücken.

Die von uns vorab ausgewählten Verfahren mit besonderen Risiken waren nicht verzeichnet. Es blieb daher unklar, seit wann welche Daten wie verarbeitet werden und ob überhaupt Maßnahmen zu ihrem Schutz ergriffen wurden. Bei anderen im Verzeichnis aufgeführten Verfahren fehlten grundlegende Angaben. Dokumente, auf die verwiesen wurde, lagen nicht vor. Andere Einträge waren

136 § 5 Abs. 3 BlnDSG
137 § 19a Abs. 1 Satz 3 Nr. 1 BlnDSG

hoffnungslos veraltet, sodass erhebliche Zweifel bestehen, dass die gesetzlich vorgeschriebenen regelmäßigen Kontrollen durchgeführt wurden. Nahezu nirgends konnte die Vorabprüfung durch die oder den Datenschutzbeauftragten nachvollzogen werden. Ebenso nahezu durchgängig war nicht erkennbar, ob je eine Risikoanalyse vorgenommen oder ein Sicherheitskonzept zusammengestellt wurde.

Somit mussten wir nicht nur feststellen, dass das Verfahrensverzeichnis als solches den gesetzlichen Anforderungen nicht genügt. Die Lücken weisen auf ein wesentlich größeres Problem: Sie deuten darauf hin, dass die Charité teilweise neue Verfahren in ungeregelter Weise einführt. Die vom Gesetzgeber vorgegebene und angesichts der Sensitivität der Daten und Komplexität der Informationstechnik notwendige systematische Vorgehensweise bei der Planung von Sicherheitsmaßnahmen wird nicht eingehalten.

Damit steht die Sicherheit der Daten der Patienten und auch der Beschäftigten der Charité in erheblichem Zweifel. Aus früheren Prüfungen ist uns bekannt, dass die Charité durchaus technische Sicherheitsvorkehrungen trifft. Ohne ein systematisches Vorgehen verbleiben jedoch mit hoher Wahrscheinlichkeit unbemerkt erhebliche Löcher im Schutzwall, den die Charité um ihre Daten errichtet hat. Angreifer sind in der Lage, diese Löcher zu finden und könnten unbeobachtet Geräte kompromittieren und Daten abziehen oder manipulieren. So sind in der jüngsten Vergangenheit erhebliche Sicherheitsdefizite in Medizingeräten bekannt geworden, die an Krankenhausnetze angeschlossen wurden. Wenn ein Unbefugter sich Zugang zum internen Chariténetz verschaffen kann, wie weit ist es dann noch bis zur ggf. lebensbedrohlichen Manipulation?

Schlussendlich mussten wir feststellen, dass die Charité bisher nicht in der Lage ist, selbst die vorhandenen öffentlichen Teile des Verfahrensverzeichnisses Bürgern zur Verfügung zu stellen, obwohl hierauf ein gesetzlich verbrieftes Recht besteht. Fehlende interne Transparenz und fehlende Transparenz nach außen kommen zusammen.

Die vorgefundenen Mängel wurden beanstandet. Schon vorab sagte uns die Charité zu, die bestehenden Defizite aufzuarbeiten. In Bezug auf die Dokumentation kann und muss das unverzüglich geschehen. Die gesetzlich vorgegebenen Prozesse bei Einführung oder substanzieller Änderung von Verfahren

müssen etabliert und ihre Befolgung durchgesetzt werden. Die Herstellung einer durchgehenden und systematischen Informationssicherheit im laufenden Betrieb ist schließlich eine sehr große Aufgabe, welcher die Charité substanzielle personelle und sachliche Ressourcen widmen muss. Wir werden die Charité bei ihren Anstrengungen begleiten und die Öffentlichkeit über den Fortschritt informieren.

Krankenhäuser sind wegen der von ihnen verarbeiteten sensitiven Daten zu besonderer Sorgfalt bei der Einführung neuer IT-Verfahren und ihrer internen Kontrolle verpflichtet. Das Verzeichnis aller betriebenen Verfahren dient sowohl der Datenschutzkontrolle als auch der Transparenz für die Öffentlichkeit. Ein laxes Vorgehen führt zu vermeidbaren und in ihrer Reichweite nicht abschätzbaren Risiken für die Patienten.

8.4.2 Erhebung von Patientendaten zur Aufklärung von Abrechnungsbetrug

Die Staatsanwaltschaft Berlin ist mit dem Verdacht an die Charité herangetreten, dass bei der Charité ermächtigte Chefärzte gegen das Gebot der persönlichen Leistungserbringung verstoßen haben könnten. Die Staatsanwaltschaft hat die Charité aufgefordert, interne Untersuchungen zu diesen Vorwürfen durchzuführen und der Staatsanwaltschaft die Ergebnisse zur Verfügung zu stellen.

Die Charité hat diesen Verdacht zum Anlass genommen, die Leistungserbringung und Leistungsdokumentation aller Ärzte der Charité zu überprüfen, die über eine solche Ermächtigung verfügten, und der Staatsanwaltschaft zugesagt, die Ergebnisse der internen Untersuchung mitzuteilen.

Die Charité forderte die Ärzte zur Übersendung einer Aufstellung aller von den ermächtigten Ärzten mit der Kassenärztlichen Vereinigung (KV) abgerechneten Fälle (inkl. Leistungs- und Abrechnungsinformation) auf. Dabei wurden der Hintergrund, dass die Staatsanwaltschaft an die Charité herangetreten ist, sowie die getroffene Vereinbarung, dieser einen Untersuchungsbericht zur Verfügung zu stellen, nicht transparent gemacht.

Für die Datenerhebung der Abrechnungsunterlagen bestand keine Rechtsgrundlage; auch konnte sie nicht auf eine Einwilligung der betroffenen Ärzte gestützt werden. Da es sich bei den von der Charité erhobenen Daten, die in dem Bericht zusammengefasst wurden, um unzulässig erhobene Daten handelt, war auch eine Übermittlung an die Staatsanwaltschaft datenschutzrechtlich unzulässig.

Bei unserer Bewertung war zu berücksichtigen, dass zum Zeitpunkt der Übermittlung des Berichtes an die Staatsanwaltschaft bereits wirksame Durchsuchungsbeschlüsse des Amtsgerichtes Tiergarten vorlagen. Im Ergebnis hätte die Staatsanwaltschaft alle dem Bericht zugrundeliegenden Daten der Charité im Rahmen der Durchsuchung und Beschlagnahme erhalten.

Aufgrund der unzulässigen Datenerhebung und Übermittlung an die Staatsanwaltschaft haben wir einen datenschutzrechtlichen Mangel festgestellt.[138] Von einer Beanstandung haben wir insbesondere aufgrund der Zusage der Charité, uns in das weitere Verfahren einzubeziehen, abgesehen. Überdies haben wir berücksichtigt, dass der Vorstand der Charité eine Durchsuchung der Räumlichkeiten und Beschlagnahme der Unterlagen nur vor dem Hintergrund der Kooperation mit der Staatsanwaltschaft vermeiden konnte. Es ist davon auszugehen, dass die Staatsanwaltschaft von den vorliegenden Durchsuchungsbeschlüssen Gebrauch gemacht hätte, wenn die Charité den Untersuchungsbericht nicht an die Staatsanwaltschaft gesandt hätte. Die Ermittlungsverfahren der Staatsanwaltschaft gegen die beschuldigten Ärzte wurden in der Zwischenzeit eingestellt.

Eine krankenhausinterne Aufklärung des Verdachts von Leistungsmissbrauch kann nur im Rahmen des rechtlich Zulässigen erfolgen. Darüber hinausgehende Ermittlungen können nur durch die dafür vorgesehenen Strafverfolgungsbehörden selbst erfolgen. Einer Aufforderung der Staatsanwaltschaft zu weitergehenden Ermittlungen muss entgegengetreten werden.

138 § 26 BlnDSG

8.5 Kommunikation zwischen Ärzten und Patienten

Aus der Praxis

Wir erhielten mehrere Anfragen von ärztlich und therapeutisch tätigen Personen zu zulässigen Formen der elektronischen Kommunikation mit Patienten.

Ärztlich oder therapeutisch tätige Personen unterliegen der Schweigepflicht.[139] Was sie über ihre Patientinnen und Patienten erfahren, dürfen sie nur bei gesetzlicher Erlaubnis oder mit Einwilligung der Betroffenen offenbaren. Wenn sie mit ihren Patienten elektronisch kommunizieren, gehört der Schutz der Inhalte der Kommunikation dazu. Mehr noch: Bereits der Umstand, dass überhaupt ein Behandlungsverhältnis besteht, geht Dritte nichts an.

Der beste Weg, sich mit einer behandelnden Person auszutauschen, ist immer noch der Besuch in der Praxis. Auch ist ein Telefonanruf zur Vereinbarung eines Termins unbedenklich; steht doch die telefonische Kommunikation unter dem Schutz der Telefonanbieter. Auch im Zeitalter IP-basierter Anschlüsse sind sie zu dem gleichen Schutz des gesprochenen Worts verpflichtet wie bei den elektromechanischen Vermittlungssystemen der alten Zeit.

Doch der Bedarf steigt, auch zwischen den Praxisbesuchen eine Anfrage stellen zu können oder Angaben über den Verlauf der Behandlung zu übermitteln; oder auch nur den nächsten Termin nicht über das Telefon, sondern außerhalb der Öffnungszeiten über ein Internetportal zu buchen.

Wer den eigenen Patientinnen und Patienten diese Kommunikationsformen eröffnen will, muss die Voraussetzungen dafür schaffen, dass die Vertraulichkeit gewahrt bleibt. In der Regel wird dabei ein Dienstleister einbezogen. Dies muss für die Betroffenen transparent sein. Da der Dienstleister in der Regel zumindest Kenntnis von dem Bestehen des Behandlungsverhältnisses erhält, ist eine ausdrückliche Schweigepflichtentbindung durch die Betroffenen notwendig.

Anderes gilt nur, wenn der Dienstleister rechtlich eigenständig handelt und mit den Betroffenen ein unabhängiges Vertragsverhältnis (z. B. zur Übermittlung

139 § 203 StGB

eines Terminwunsches) eingeht. Dann muss dieser informieren, dass bei ihm die ärztliche Schweigepflicht nicht gilt, und eine Einwilligung der Betroffenen einholen.

Zwischen den Geräten der Patientinnen und Patienten, sei es PC oder Smartphone, und den Servern der Leistungserbringer oder ihrer Dienstleister muss die Kommunikation sicher von Ende zu Ende verschlüsselt werden. Etabliert ist dies bei der Interaktion mit einem Webangebot, das ohne verschlüsselte Verbindung und qualifiziertes Zertifikat zur Identifikation des Anbieters nicht betrieben werden darf. Werden nicht nur allgemeine, sondern für einzelne Patientinnen und Patienten individualisierte Informationen bereitgestellt, muss dem Patienten auch ein Zugang über ein Pseudonym eröffnet werden.

Nichts anders gilt für die Übertragung von einem mobilen Gerät aus, das die Betroffenen bei sich tragen, sei es, dass sie eine App auf ihrem Smartphone nutzen, um den Fortschritt der Therapie zu dokumentieren, sei es, dass ein am Körper getragenes Messgerät über die Mobilfunkverbindung Daten kontinuierlich überträgt. In dieser Konstellation dürfen die empfangenden Server nicht „irgendwo in der Cloud", sondern ausschließlich bei dem vereinbarten Dienstleister landen, der sie dann an die jeweilig behandelnde Person überträgt. Verschlüsselung und gegenseitige Authentisierung bei allen Verbindungen sind Pflicht.

Es liegt nahe, persönliche Kommunikation zwischen behandelnder und behandelter Person über E-Mail abzuwickeln. Um dies sicher zu gestalten, müssen beide Seiten die Ende-zu-Ende-Verschlüsselung beherrschen, Schlüssel austauschen und ihre Authentizität überprüfen. Noch sind diese Voraussetzungen selten gegeben. Darüber hinaus ist die Kommunikationsbeziehung stets im Klartext an der E-Mail abzulesen. Dies führt dazu, dass es sehr anspruchsvoll ist, E-Mail rechtskonform für die Patientenkommunikation einzusetzen, und in der Regel davon abgeraten werden muss. Ein Ersatz lässt sich oft über die Bereitstellung eines Webangebots mit hinterlegten Nachrichten oder einer Chat-Funktion schaffen. Aber auch hier muss an eine sichere Form der Authentifizierung beider Seiten gedacht werden.

Bei einigen Anbietern modernerer Kommunikationsmittel, wie Instant Messaging und Audio-Video-Konferenzen, wurde von vornherein an eine

Ende-zu-Ende-Verschlüsselung gedacht. Ihrer Nutzung steht dann nichts im Wege, wenn die Verfahren auf Zuverlässigkeit geprüft sind, die Anbieter in Deutschland oder einem anderen EU-Mitgliedstaat bzw. einem Drittland mit angemessenem Datenschutzniveau ansässig sind (und die Datenverarbeitung auch tatsächlich ausschließlich dort erfolgt) und die Patienten in die Offenbarung des Behandlungsverhältnisses an diese Anbieter eingewilligt haben.

Die neuen Wege der Kommunikation zwischen behandelnden Personen und ihren Patientinnen und Patienten sind nutzbar, wenn die nötigen Voraussetzungen geschaffen werden: Transparenz, Einholung von Einwilligungen in unvermeidliche Offenbarungen, sichere Verfahren.

9 Beschäftigtendatenschutz

9.1 Bonitätsauskünfte im Bewerbungsverfahren

In mehreren Fällen haben Unternehmen vor oder während eines Bewerbungsgespräches eine Bonitätsabfrage getätigt, um die Zuverlässigkeit der Bewerberinnen und Bewerber zu überprüfen. In einem Fall war die Bewerberin für das Telefonmarketing eines Unternehmens vorgesehen. Nach Auffassung des Unternehmens sei eine gute Bonität eine Voraussetzung, um nicht in die Gefahr der Bestechlichkeit zu kommen.

Die Vermögensverhältnisse gehören grundsätzlich zur Privatsphäre und müssen daher für die Geschäftsleitung ohne Interesse sein. Nur in Ausnahmefällen haben Unternehmen ein berechtigtes Interesse an Informationen über die finanzielle Situation ihrer Beschäftigten, das eine Übermittlung von Bonitätsdaten durch eine Auskunftei rechtfertigt.

Ein Fragerecht der Unternehmen kommt nur dann in Betracht, wenn die Beschäftigten eine Position ausfüllen sollen, in der Seriosität und Vertrauenswürdigkeit in finanziellen Fragen bedeutsam sind (z. B. Finanzberatung). Gleiches gilt aber auch für Beschäftigte, bei denen finanzielle Zuverlässigkeit gefordert ist (z. B. Kassiererinnen oder Kassierer).

Eine etwaige Bestechlichkeit kann nicht als Argument herangezogen werden, um eine umfassende Bonitätsauskunft einzuholen. Bewerber sollten nicht aufgrund privater finanzieller Probleme stigmatisiert und als kriminalitätsanfällig angesehen werden. Die Bonitätsabfrage, bei der das Unternehmen gegenüber der Auskunftei einen falschen Anfragegrund angegeben hatte, war rechtswidrig.

Standardisierte Bonitätsauskünfte enthalten auch Informationen, die Aufschluss über die privaten Lebensumstände und über Geld- und Warenkreditverträge der Betroffenen geben. Die Einholung einer solchen Auskunft ist in der Regel unzulässig, da diese über das für die Einstellungsentscheidung erforderliche Informationsinteresse hinausgeht und in das Persönlichkeitsrecht der Bewerberinnen und Bewerber eingreift.

9.2 Öffentliche Kommentierung von Personalangelegenheiten

Im Zuge der Bewerbung einer Rechtsreferendarin um einen Ausbildungsplatz im Rechtsamt und eines dadurch entstandenen Streits hat das Bezirksamt Neukölln in einer Pressemitteilung die Faktenlage erklärt sowie die Vorkommnisse aus seiner Sicht bewertet. Insbesondere wurden dabei Einzelheiten zum Bewerbungsverfahren der Rechtsreferendarin dargelegt und disziplinarische Maßnahmen durch die Kammergerichtspräsidentin gefordert. Das Bezirksamt machte geltend, dass die Rechtsreferendarin den Bewerbungsvorgang selbst in den Medien öffentlich gemacht hat.

Personenbezogene Daten von Bewerbern dürfen für Zwecke des Beschäftigungsverhältnisses nur erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich ist.[140] Im vorliegenden Fall war es für die Begründung eines möglichen Ausbildungsverhältnisses allerdings nicht notwendig, Personalangelegenheiten gegenüber der Öffentlichkeit mitzuteilen. Insbesondere unterliegen Personaldaten einer besonderen Vertraulichkeit. Zu ihnen haben in der Regel nur Beschäftigte Zugang, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind.

Ferner konnte die Veröffentlichung nicht dadurch gerechtfertigt werden, dass sie zur Wahrung berechtigter Interessen eines Dritten erforderlich war.[141] Zwar stellte die Richtigstellung (etwaiger) unwahrer Tatsachenbehauptungen ein legitimes Interesse des Bezirksamtes Neukölln dar, um die Mitarbeiterinnen und Mitarbeiter des Bezirksamtes (als Dritte) vor einer (etwaigen) Verunglimpfung und Verbreitung von Lügen zu schützen, indem das Bezirksamt Neukölln auf die richtige Faktenlage hinwies. Insoweit musste das schutzwürdige Interesse der Betroffenen zurücktreten, da es Anliegen des Bezirksamtes war, die Öffentlichkeit über das tatsächliche Geschehen aufzuklären. Allerdings konnte sich dieses Interesse letztlich nur auf die Tatsachen beziehen, die richtiggestellt werden sollten. Für Fakten, die darüber hinaus an die Öffentlichkeit gegeben

140 § 2 Abs. 2 BlnDSG i.V. m. § 32 Abs. 1 Satz 1 BDSG
141 § 2 Abs. 2 BlnDSG i.V. m. § 28 Abs. 2 Nr. 2 a) BDSG

wurden, konnte dies nicht gelten. So kann das Recht auf Richtigstellung letztlich nicht dazu führen, dass die gesamte Historie des Bewerbungsvorgangs dargelegt wird, ohne dass sich die Rechtsreferendarin konkret in den Medien darauf bezogen hat.

Die Veröffentlichung ließ sich auch nicht auf den presserechtlichen Informationsanspruch stützen. Auskünfte gegenüber der Presse können verweigert werden, wenn ein schutzwürdiges privates Interesse verletzt wird.[142]

Das Bezirksamt Neukölln hat uns bestätigt, dass es unsere Hinweise zum Umgang mit Personaldaten bei zukünftigen ähnlichen Sachverhalten berücksichtigen wird.

Das Interesse von Behörden, etwaige unwahre Tatsachenbehauptungen in der Öffentlichkeit richtigzustellen, ist grundsätzlich als legitim anzusehen. Allerdings dürfen Personaldaten nicht über das erforderliche Maß hinaus veröffentlicht werden, da diese einer strengen Vertraulichkeit unterliegen.

9.3 Big Boss is watching you – Videoüberwachung im Beschäftigungsverhältnis

Immer mehr Beschäftigte aus verschiedenen Tätigkeitsbereichen wenden sich an uns, um auf die Videoüberwachung in ihrem Arbeitsumfeld aufmerksam zu machen. Dabei kommen sowohl offene als auch versteckte Kameras zum Einsatz. Einige Beschäftigte berichteten von Verhaltens- und Leistungskontrollen bzw. von der Nutzung des Videomaterials ohne ihr Einverständnis für interne Schulungen oder Fortbildungen. Die Unternehmen trugen zumeist vor, dass diese Kameras der Abschreckung und der Verhinderung von Diebstählen dienen. Es wurde auch angegeben, dass durch die Kameras eine Kommunikation mit den Beschäftigten bei Abwesenheit der Geschäftsleitung oder die Analyse des Kundenstroms intendiert sei.

142 § 4 Abs. 2 Nr. 4 Berliner Pressegesetz

Durch den Einsatz von Videokameras sind schutzwürdige Interessen der Beschäftigten berührt. Bei den Beschäftigten kann ein ständiger Überwachungsdruck entstehen, da durch die Kameras eine permanente und lückenlose Kontrolle möglich ist. Das Unternehmen ist nur zu Überwachungsmaßnahmen befugt, wenn diese für den durch das Unternehmen angegebenen Verwendungszweck erforderlich sind.[143] Sofern die Kameras aufgrund einer potenziellen Diebstahlgefahr installiert wurden, rechtfertigen allgemeine, nicht näher beschriebene Vorfälle eine Videoüberwachung nicht. Die teilweise von den Unternehmen angeführten Argumente der Kundenstromanalyse oder die Kommunikation der Leitung mit den Beschäftigten können die Videoüberwachung nicht legitimieren, da diese Ziele durch mildere Mittel erreicht werden können.[144]

Der Eingriff in das Persönlichkeitsrecht der Beschäftigten ist dann besonders gravierend, wenn die Überwachung kontinuierlich erfolgt und sie ihr nicht ausweichen können. Es müssen daher stets Maßnahmen getroffen werden, die die schutzwürdigen Interessen der Beschäftigten berücksichtigen, wie z. B. die Reduzierung des Erfassungsbereichs oder die Verpixelung der Gesichter. Ferner sollte im Arbeitsvertrag selbst oder in einer entsprechenden Geschäftsrichtlinie klargestellt werden, dass etwaige Videoaufzeichnungen nicht für Verhaltens- und Leistungskontrollen der Beschäftigten herangezogen werden. Eine Nutzung dieser Aufnahmen für interne Schulungen oder Fortbildungen ist grundsätzlich nicht zulässig.

Durch die Videoüberwachung sind schutzwürdige Interessen der Beschäftigten berührt. Diese darf nicht zu einer unzumutbaren Drucksituation führen. Eine Interessenabwägung muss daher für einen Ausgleich der widerstreitenden Interessen der Geschäftsleitung und der Beschäftigten sorgen.

143 Siehe § 6b Abs. 1 BDSG bei öffentlich zugänglichen Räumen, § 32 Abs. 1 Satz 1 BDSG bei nicht-öffentlich zugänglichen Räumen

144 So können Kundenströme auch durch eigene Beobachtungen der Beschäftigten analysiert werden. Eine Kommunikation mit den Beschäftigten bei Abwesenheit der Geschäftsleitung, auch wenn es hierzu Bildmaterials bedarf, kann z. B. durch den Einsatz von Smartphones realisiert werden.

9.4 GPS-Tracking im Beschäftigungsverhältnis

Mehrere Beschäftigte von Handwerksunternehmen erfragten bei uns die rechtliche Zulässigkeit von GPS-Ortungssystemen in ihren Dienstfahrzeugen. Die Beschäftigten gaben teilweise an, dass sie aufgrund der permanenten Überwachung auch psychischen Druck erleiden. Die Unternehmen machten vor allem geltend, dass die GPS-Ortung zur flexibleren Terminierung bei anfallenden Störeinsätzen im Tagesgeschäft diene.

Die Erhebung und Verarbeitung der Ortungsdaten ist zulässig, wenn dies zur Durchführung des Beschäftigungsverhältnisses erforderlich ist.[145] Dabei ist eine permanente Ortung der Beschäftigten nicht notwendig. Im Allgemeinen ist eine Datenverarbeitung aus betrieblichen Gründen nur zur Sicherheit oder zur Koordinierung des Einsatzes der Beschäftigten zulässig. Es ist immer zu prüfen, ob eine Aufenthaltsbestimmung der Handwerker in einem Havariefall durch ein milderes Mittel erreicht werden kann.[146] Eine Ortung kommt dann nicht in Betracht, wenn dem Unternehmen aufgrund der Tagesplanung der Beschäftigten klar ist, wo sich diese im Zeitpunkt des Störeinsatzes gerade befinden.

Im Ergebnis sollte gewährleistet sein, dass das Ortungssystem nur in absoluten Ausnahmefällen (z. B. bei Störeinsätzen) genutzt und anderenfalls deaktiviert wird. Ferner muss eine Verhaltens- und Leistungskontrolle der Beschäftigten ausgeschlossen sein. Sofern das GPS-System auch für Zwecke des Diebstahlschutzes genutzt werden soll, ist es ausreichend, wenn die Ortung durch das System technisch etwa erst nach einem Kfz-Diebstahl eingesetzt wird. Darüber hinaus ist die Verarbeitung der Daten zum Zwecke der Dokumentation der Einsatzzeiten gegenüber dem Kunden nicht erforderlich, da in vielen Fällen ohnehin eine Pauschale berechnet wird bzw. dieser Zweck auch hier durch den Einsatz milderer Mittel erreicht werden kann, etwa durch das bereits zum jetzigen Zeitpunkt vorgeschriebene Führen von Fahrten- und Stundenbüchern.

Bei unseren Prüfungen konnten wir ferner feststellen, dass in den Unternehmen kein betrieblicher Datenschutzbeauftragter bestellt wurde. Unabhängig

145 § 32 Abs. 1 Satz 1 BDSG
146 Z. B. durch Kontaktaufnahme über das Diensthandy

von der Anzahl der mit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten beschäftigten Personen besteht eine Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten, wenn eine Vorabkontrolle erforderlich ist. Diese ist bei einem geplanten Einsatz eines Ortungssystems vorzunehmen, da die Verarbeitung der Positionsdaten dazu bestimmt werden kann, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens.[147]

Im Ergebnis hat ein Unternehmen auf unsere Forderung hin das GPS-System aus dem Fahrzeug eines Mitarbeiters, für dessen Einsatz im Unternehmen das GPS-Gerät nachweislich nicht erforderlich war, ausgebaut. Ferner wurde der Dienstleister angewiesen, die Positionsdaten nur für den aktuellen und nicht für den nachträglichen Abruf zu speichern, sodass das Risiko einer potenziellen Verhaltens- und Leistungskontrolle verringert wurde.

Der Einsatz eines Ortungssystems bei Beschäftigten ist streng am Erforderlichkeitsgrundsatz zu messen und sollte nur in Ausnahmen zulässig sein. Eine Speicherung der Positionsdaten ist über den Zweck der Einsatzkoordinierung hinaus nicht notwendig. Diese sind daher nach Erfüllung des Zweckes zu löschen.

9.5 Daten von Bediensteten im Internet

Aus der Praxis

Wir beschäftigten uns in verschiedenen Zusammenhängen mit der Frage, ob personenbezogene Daten von Behördenbeschäftigten, d.h. dienstliche Kontaktdaten und behördliche Schreiben, E-Mails und Entscheidungen, durch Private in das Internet eingestellt werden dürfen. So erreichte uns z. B. die Beschwerde einer bayerischen Verwaltungsmitarbeiterin, deren Antwort-E-Mail auf eine Bürgeranfrage samt ihrer dienstlichen Kontaktdaten auf einer Berliner Webseite veröffentlicht wurden. Auch Beschäftigte unserer Behörde waren davon betroffen, dass ihre Schreiben eingescannt und ins Internet eingestellt wurden. Darüber hinaus erhielten wir eine Reihe von Anfragen, die die Veröffentlichung von Behördenkommunikation betrafen.

147 § 4d Abs. 5 Satz 2 Nr. 2 BDSG

Die Zulässigkeit solcher Veröffentlichungen muss im Einzelfall geprüft werden. Sofern die Informationen durch einen rechtmäßigen Informationszugang nach dem Berliner Informationsfreiheitsgesetz (IFG) erlangt wurden,[148] sind die Daten der Betroffenen nicht schutzwürdig. Da die nach dem IFG erlangten Informationen keinen Verwendungsbeschränkungen unterliegen, spricht nichts gegen eine Veröffentlichung im Internet. Handelt es sich um Informationen, die nicht auf der Grundlage des IFG erlangt wurden, stellt sich gleichwohl die Frage, ob die Informationen bei einem IFG-Antrag freizugeben wären. Wenn ja, dürfen die Angaben veröffentlicht werden.

In jedem Fall müssen Betroffene nach der Rechtsprechung des Bundesverfassungsgerichts[149] keine falschen Zitierungen hinnehmen, d. h. wenn ihnen Äußerungen in den Mund gelegt werden, die von ihnen nicht getätigt wurden und die ihren Geltungsanspruch beeinträchtigen. Zudem sind die Betroffenen dann schutzwürdig, wenn die Informationen in einen Kontext gestellt werden, durch den die Grenze zur Schmähkritik, Formalbeleidigung oder Diffamierung überschritten ist und die Gefahr der Stigmatisierung besteht.

Im Fall der bayerischen Verwaltungsmitarbeiterin bestand die Besonderheit, dass die Zulässigkeit der Veröffentlichung nicht an den Wertungen eines Informationsfreiheitsgesetzes hätte gemessen werden können, da ein solches in Bayern bisher nicht existiert. Im Ergebnis spielte dies jedoch keine Rolle, da die Betreiber der Webseite die Angaben zu der Mitarbeiterin auf unsere Anfrage durch nicht sprechende Kürzel ersetzten und sich das Anliegen der Betroffenen damit erledigte.

Auch Behördenbeschäftigte bleiben bei der Wahrnehmung öffentlich-rechtlicher Aufgaben und somit in ihrer Eigenschaft als Amtswalter Trägerinnen und Träger von Grundrechten. Das bedeutet, dass ihre personenbezogenen Daten gegenüber den Veröffentlichungsbedürfnissen Dritter schutzwürdig sein können. Gleichwohl müssen in Berlin auch die Wertungen des IFG berücksichtigt werden. Das IFG ermöglicht grundsätzlich einen voraussetzungslosen Anspruch zu behördlichen Informationen.

148 § 6 Abs. 2 Satz 2 IFG
149 BVerfGE 54, S. 148

9.6 Wenn der Arbeitgeber den Facharzt kennt – Umgang mit Arbeitsunfähigkeitsbescheinigungen

Aus der Praxis

Der Personalrat eines Kita-Eigenbetriebes wandte sich an uns, da die Kita-Leitung einer Einrichtung die Beschäftigten angewiesen hat, die Arbeitsunfähigkeitsbescheinigung ausschließlich bei der örtlichen Kita-Leitung und nicht auch alternativ beim Personalservice abzugeben.

Aus der Angabe des Fachgebietes der Ärztin bzw. des Arztes kann die Führungskraft ohne Weiteres Rückschlüsse auf die Art der Erkrankung ziehen, die die Betroffenen in ihren schutzwürdigen Belangen nicht unerheblich beeinträchtigen können. So kann z. B. die Fachbezeichnung „Onkologie" auf eine bestehende Krebserkrankung, der Zusatz „Drogenambulanz" auf etwaige Alkohol- oder Drogenprobleme oder der „Fachbereich Psychiatrie" auf psychische Erkrankungen hindeuten.

Gemäß Entgeltfortzahlungsgesetz (EntgFG)[150] haben die Beschäftigten eine ärztliche Bescheinigung über das Bestehen der Arbeitsunfähigkeit, sofern sie länger als drei Kalendertage andauert, spätestens an dem darauffolgenden Arbeitstag beim Arbeitgeber vorzulegen. Dabei ist der Begriff des Arbeitgebers allerdings nicht gleichzusetzen mit dem Begriff des direkten Vorgesetzten. Zwar hat die Kita-Leitung ein nachvollziehbares Interesse an der Kenntnis der Arbeitsunfähigkeitsbescheinigung bei der Dienstplanung, die Einreichung der Arbeitsunfähigkeitsbescheinigung beim Personalservice stellt aber im Rahmen der Prüfung der Verhältnismäßigkeit ein milderes Mittel dar, das die Interessen der Betroffenen weniger beeinträchtigt.

Wir haben daher die Geschäftsleitung des Eigenbetriebes aufgefordert, es den Betroffenen weiterhin freizustellen, ob sie Arbeitsunfähigkeitsbescheinigungen bei der Personalstelle oder bei der örtlichen Kita-Leitung abgeben.

Die verpflichtende Abgabe der Arbeitsunfähigkeitsbescheinigung bei der direkten Führungskraft ist nicht erforderlich. Den gesetzlichen Vorgaben kann entsprochen werden, wenn den Betroffenen freisteht, selbst über den Adressaten ihrer Arbeitsunfähigkeitsbescheinigung (Führungskraft oder Personalservice) zu entscheiden.

150 § 5 Abs. 1 Satz 2 i.V. m. § 5 Abs. 1 Satz 1 EntgFG

10 Forschung

10.1 Datensicherheit bei PISA-Studien – durchgefallen?

Seit 2000 werden die PISA-Studien (Programme for International Student Assessment) von der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) durchgeführt. Dies sind internationale Schulleistungsstudien mit dem Ziel, alltags- und berufsrelevante Kenntnisse und Fähigkeiten Fünfzehnjähriger zu messen.

Bisher erfolgte die stichprobenhafte Auswahl der Teilnehmerinnen und Teilnehmer an der PISA-Studie mittels eines Client-Server-Programms. Alle infrage kommenden Lehrkräfte sowie Schülerinnen und Schüler wurden lokal in einem Client-Programm der teilnehmenden Schule erfasst. Die Studienleitung erhielt lediglich pseudonymisierte Listen zur Stichprobenziehung, indem die Einträge statt identifizierender Daten wie Namen und Geburtsdatum nur eine laufende Nummer enthielten. Die Pseudonyme der ausgewählten Teilnehmerinnen und Teilnehmer wurden dann an die jeweilige Schule zurückgemeldet. Sie erstellte eine ausführlichere Schülerteilnahmeliste, etwa mit Angaben zum Zuwanderungshintergrund und Zensuren. Der Inhalt ging wiederum nur pseudonymisiert an die Studienleitung. Das war ein datensparsames Verfahren.

Dieses Client-Server-Programm ist nun durch eine Webanwendung ersetzt worden. Die Listen werden nicht mehr lokal, sondern auf den Servern der Studienleitung gespeichert. Dies begründete man damit, dass die Installation der Client-Software manche Schulen überfordert und den Einbau anderer, kostenpflichtiger Software notwendig gemacht habe. Die bisherigen Funktionen der Client-Anwendung wurden in JavaScript implementiert.

Mit der neuen Webanwendung werden Schüler- und Lehrerdaten verarbeitet. Konkret handelt es sich bei Schülerinnen und Schülern neben Vor- und Nachnamen um Informationen zum Zuwanderungshintergrund, zur zuhause gesprochenen Sprache, Lesefähigkeit und zu Halbjahreszensuren in Deutsch, Mathematik, Biologie, Chemie, ggf. Naturwissenschaften, Englisch. Für diese Daten besteht ein hoher Schutzbedarf. Denn die Informationen sind

relevant für das persönliche Ansehen und berufliche Fortkommen der betroffenen Schülerinnen und Schüler.

Die Verschlüsselung der Daten ausschließlich auf der Basis eines Passworts haben wir als problematisch angesehen. Vorzugswürdig ist der Einsatz einer Zwei-Faktor-Authentifizierung. Daneben könnte als Alternative auch eine lokale Speicherung der Daten vorgesehen werden. Zudem halten wir eine Signatur der JavaScript-Codes für erforderlich.

Positiv ist dagegen, dass die Ver- und Entschlüsselung der nicht pseudonymisierten Daten ausschließlich auf den Clients und zudem eine angemessene Transportverschlüsselung und Authentifizierung des Servers erfolgen. Zudem werden die Nutzer, d. h. die Schulen, im Rahmen der Anleitung zur Webanwendung über die erforderliche Datensicherheit durch Nutzung aktueller Software, sicherer Netzwerke und Virenschutz informiert. Dies muss in verständlicher Weise und an geeigneter Stelle im Rahmen der Anleitung erfolgen.

Die teilnehmenden Schülerinnen und Schüler füllen im Rahmen der Studie u. a. Fragebögen aus. Bisher handelte es sich um Papierformulare. Nun erfolgte durch die internationale Studienleitung eine vollständige Umstellung auf computergestützte Erhebungen. Dies hat zu einer erheblichen Einschränkung der Konfigurierbarkeit der Erhebungsinstrumente geführt, was aus datenschutzrechtlicher Sicht problematisch ist. Denn die Rechtslage in den Teilnehmerländern der PISA-Studie ist nicht einheitlich. Aus diesem Grund kann es erforderlich werden, die Erhebungsinstrumente an die jeweilige Rechtslage anzupassen. Die eingesetzte Technik muss solche Anpassungen gewährleisten.

In Berlin werden die Datenverarbeitungsschritte zwar weitestgehend auf das Schulgesetz Berlin (SchulG) gestützt. Nicht alle Angaben können jedoch im Rahmen der PISA-Studie auf der Grundlage von § 9 SchulG verpflichtend erhoben werden. Es muss daher möglich sein, die Freiwilligkeit bestimmter Angaben kenntlich zu machen bzw. Fragen vollständig zu streichen, wenn das Einverständnis der Eltern für das Beantworten einer Frage nicht erteilt worden ist.

Angaben zu Schülerinnen und Schülern, die Auswirkungen auf ihr persönliches Ansehen und berufliches Fortkommen haben können, unterliegen einem hohen Schutzbedarf. Es müssen entsprechende technische und organisatorische Datensicherheitsmaßnahmen getroffen werden. Zudem müssen bei internationalen Studien die Erhebungsinstrumente Anpassungen an die jeweilige Rechtslage zulassen.

10.2 Nationale Kohorte – große Forschung, kleiner Datenschutz?

Die „Nationale Kohorte" (NAKO) ist eine Langzeit-Bevölkerungsstudie über die Dauer von 20 bis 30 Jahren. Ziel der Gesundheitsstudie soll es sein, die Ursachen für die Entstehung von Krankheiten wie Krebs, Demenz, Diabetes und Infektionskrankheiten zu erforschen. Insgesamt sollen 200.000 zufällig ausgewählte Teilnehmerinnen und Teilnehmer im Alter von 20 – 69 Jahren medizinisch untersucht und nach ihren Lebensgewohnheiten befragt werden.[151] Seit 2014 werden in insgesamt 18 Studienzentren deutschlandweit Basisuntersuchungen durchgeführt. Wir haben ein Studienzentrum in Berlin kontrolliert.

Die Studie wird vom Verein Nationale Kohorte e.V. durchgeführt. Das von uns geprüfte Berliner Studienzentrum wird für den Verein im Auftrag tätig.

Obwohl sensitive Gesundheitsdaten und weitere aussagekräftige Daten zu den Probanden in einem ungewöhnlich großen Umfang erhoben werden, liegt noch immer kein vollständiges Datenschutzkonzept vor, das den Studienzentren als klare Vorgabe für ihre Tätigkeit dient. Zudem mussten wir feststellen, dass zu bestimmten wichtigen Fragen keine Weisungen des Auftraggebers vorliegen. Durch die unzureichende Vorbereitung der verschiedenen Prozesse ergibt sich eine Reihe von Problemen:

Im Studienzentrum werden Daten gespeichert, die dort für die eigentlichen Aufgaben nicht mehr benötigt werden. So überprüft das Studienzentrum

151 Zum Hintergrund siehe zuletzt JB 2013, 11.1

umständlich, ob die von ihm erhobenen und übertragenen Daten vollständig und unversehrt bei einer zentralen Stelle eingegangen sind. Dazu betreibt das Studienzentrum eine doppelte Datenhaltung. Würde dem Nationale Kohorte e. V. eine automatisierte Lösung zur Verfügung stehen, könnte dies vermieden werden.

Ein Grundpfeiler des Datenschutzkonzepts der NAKO ist die Trennung der Verantwortlichkeit für Daten zwischen verschiedenen Stellen und Bereichen. Insbesondere wird zwischen medizinischen Daten aus den Untersuchungen und den Angaben zur Person der Probanden wie Adresse und Telefonnummer unterschieden. Die Berechtigungen zum Zugriff darauf sollen strikt getrennt vergeben werden. Eine entsprechende Trennung ist auch für das Studienzentrum vorgesehen, wird aber bei der Übertragung der Probandendaten nicht vollständig umgesetzt.

Es gibt keine durchgängige Vorgehensweise zur Löschung von Daten. Auch hier führt dies zu Datenbeständen, für deren Aufbewahrung kein originäres Bedürfnis besteht. Schließlich führt die mangelhafte Planung zu vermeidbaren Sicherheitsrisiken. Dies gilt besonders für den Schutz der Datenübertragungen. Auch stellt der Auftraggeber für eine zentrale Webanwendung keine ausreichenden Möglichkeiten zur Verfügung, die Berechtigungen aller Beschäftigten des Studienzentrums auf das notwendige Maß einzuschränken.

Das Studienzentrum selbst hat ein Jahr nach Aufnahme der ersten Untersuchungen die Arbeit an dem eigenen Sicherheitskonzept nicht abgeschlossen. Während dieses Jahres wurden zwar einige Verbesserungsmaßnahmen umgesetzt. Doch stützt sich das Studienzentrum nach wie vor auf eine Infrastruktur, die nicht für die sensitiven Daten ausgelegt ist, wie sie im Rahmen der Studie erhoben werden. Eine durchgehende Risikoanalyse fehlt gänzlich.

Großprojekte bedürfen einer entsprechend sorgfältigen Vorbereitung. Datenschutz- und Sicherheitskonzepte müssen ausgearbeitet sein, bevor die Datenverarbeitung aufgenommen wird. Wir werden die Fortschreibung der Konzepte und die Weiterentwicklung des Forschungsvorhabens weiterhin aufmerksam verfolgen.

10.3 Warnschussarrest – Forschung im Bereich der Jugendkriminalität

Das Kriminologische Forschungsinstitut Niedersachsen hat in Kooperation mit der Universität Kassel im Auftrag des Bundesministeriums der Justiz und für Verbraucherschutz die neue jugendstrafrechtliche Sanktionsmöglichkeit des Jugendarrestes untersucht. Erforscht wurde, ob der sog. Warnschussarrest im Zeitraum 2013/2014 angewendet wurde, warum die Vorschrift nicht angewendet wurde und welche Einstellung Praktiker dem Warnschussarrest entgegenbringen. Dafür wurden auch in Berlin betroffene Jugendliche und Praktiker wie Jugendrichterinnen und -richter, Jugendstaatsanwältinnen und -anwälte, Bewährungshelferinnen und -helfer, Vollzugsleiterinnen und -leiter sowie Jugendgerichtshelferinnen und -helfer befragt. Zudem wurden u. a. einzelfallbezogene Analysen etwa der Akten bei den Gerichten durchgeführt. An die Verarbeitung der sensitiven Daten müssen besondere Anforderungen gestellt werden.

Eine Besonderheit stellten bei dem Forschungsprojekt zum Warnschussarrest die niedrigen Fallzahlen dar. Nach unseren Informationen wurde 2013 in Berlin nur ein Warnschussarrest verhängt. 2014 gab es zehn männliche Arrestanten und eine weibliche Arrestantin. Dies schließt praktisch eine Anonymisierung aus. Niedrige Fallzahlen ermöglichen es auch, mit nur geringem Zusatzwissen die jeweiligen Betroffenen zu identifizieren. Die Anonymisierung der für ein bestimmtes Forschungsvorhaben erhobenen personenbezogenen bzw. personenbeziehbaren Daten, sobald es der Forschungszweck zulässt, gehört allerdings zu den grundlegenden Anforderungen an die zulässige Datenverarbeitung im Forschungsbereich.

Es besteht ein hohes Stigmatisierungsrisiko, wenn sich die erhobenen Angaben einer oder einem bestimmten Betroffenen zuordnen lassen. Für die Aktenanalysen trifft dies jedenfalls zu. Aber auch Angaben der Praktiker können Spezifika enthalten, die eine Identifikation der oder des Jugendlichen zulassen. Die Angaben aus dem Strafverfahren sind geeignet, die Jugendlichen in ihrem persönlichen Ansehen und Fortkommen erheblich zu beeinträchtigen. Bei Forschungsprojekten im Bereich der Jugendkriminalität sind die schutzwürdigen Interessen der betroffenen Jugendlichen im besonderen Maße

zu berücksichtigen. Hierauf ist auch bei der Auslegung von Forschungsklauseln, etwa in der Strafprozessordnung, zu achten.

Bei einer tiefgreifenden Datenverarbeitung wie der Aktenanalyse muss daher zur Wahrung der schutzwürdigen Interessen der Betroffenen jedenfalls eine ausreichende Transparenz gewährleistet werden. Die Betroffenen – sowie bei fehlender Einsichtsfähigkeit die Erziehungsberechtigten – müssen mit ausreichend zeitlichem Vorlauf darüber informiert werden, dass eine Analyse des konkreten Einzelfalls für Zwecke des Forschungsprojekts stattfindet. Es muss ein Widerspruchsrecht eingeräumt und ein Verfahren zur Umsetzung von Widersprüchen eingerichtet werden. Hierfür kann ein sog. Adressmittlungsverfahren eingesetzt werden, bei dem die Justizbehörden die entsprechenden Informationen und Unterlagen an die Betroffenen vermitteln. In Anbetracht der niedrigen Fallzahlen hätte hierin auch kein unverhältnismäßiger Aufwand bestanden.

Zudem haben wir bei der Beratung zu diesem Forschungsprojekt darauf hingewiesen, dass das Anliegen des Forschungsvorhabens weitestgehend durch eine nicht personenbeziehbare Befragung der Praktiker hätte erfüllt werden können. Fragen zur generellen Einstellung und zur Beurteilung der Qualität des Warnschussarrests sowie die Erhebung von Vorschlägen der Praktiker zur Verbesserung der Praxis sind datenschutzrechtlich unproblematisch, sofern keine potenziell identifizierenden Daten wie demografische Angaben oder spezifische Angaben zur Tätigkeit erhoben werden.

Angaben aus Strafverfahren sind geeignet, die Betroffenen erheblich in ihrem persönlichen Ansehen und Fortkommen zu beeinträchtigen. Bei Forschungsprojekten im Bereich der Jugendkriminalität sind die schutzwürdigen Interessen der betroffenen Jugendlichen im besonderen Maße zu berücksichtigen.

10.4 Falschparker auf dem Radar

Im Frühjahr berichtete die Presse über das Siemens-Forschungsprojekt City2.e 2.0. Getestet werden im Rahmen des Projekts in Straßenlaternen eingebaute Sensoren, die freie Parkplätze erkennen. Über eine App sollen suchende Autofahrer zu Parklücken navigiert werden.

Neben der Siemens AG sind insbesondere die Senatsverwaltung für Stadtentwicklung und Umwelt und die Verkehrsmanagementzentrale Berlin Betreibergesellschaft mbH an dem Projekt beteiligt. Die neue Technologie wird in der Bundesallee unter realen Bedingungen getestet. Für das Erkennen freier Parkplätze werden Radarsensoren eingesetzt. Diese registrieren nur, ob eine Fläche frei oder besetzt ist. Weitergehende Informationen etwa über Fahrzeuge oder Halter werden nicht erfasst. Insofern stellt der Einsatz der Radarsensoren aus Datenschutzsicht kein Problem dar.

Die in Straßenlaternen integrierten Radarmodule enthalten allerdings auch einen RFID-Scanner. Diese sind zwar nicht vom aktuellen Testbetrieb umfasst, zukünftig könnten mithilfe der Scannerkomponente jedoch weitergehende Informationen (z. B. zur Abrechnung von Parktickets, Erfassung von Verkehrsvergehen) aus dem Straßenraum erhoben werden. Ermöglichen würde dies etwa die Vergabe von scannbaren und personalisierten Parkberechtigungen, die z. B. als RFID-Chip an der Windschutzscheibe angebracht werden.

Diese Ausweitung der Funktionalität würde massive datenschutzrechtliche Probleme aufwerfen. Werden Anwohnerparkausweise und sonstige Parkberechtigungen nur noch etwa über Vignetten bzw. RFID-Transponder vergeben, denen eine eindeutige Seriennummer zugeordnet ist, können bei einer Verbreitung der Technologie umfangreiche Bewegungsprofile erstellt werden. Selbst mit einer Einwilligung der Autofahrer ist das Vorgehen problematisch. Denn die Autofahrer wollen ggf. lediglich von der bequemen Abrechnungsmöglichkeit profitieren. Jedenfalls muss eine Alternative zu dem personenbeziehbaren Parkberechtigungsnachweis bestehen bleiben.

Erfreulich war zwar, dass die Projektpartner schon frühzeitig auf uns zugekommen sind. So konnten wir schon vor Beginn des Testbetriebs beratend Hinweise geben. Bedauerlicherweise lagen uns allerdings zunächst nur

unvollständige Informationen vor. Erst zu einem späteren Zeitpunkt ergab sich, dass im Rahmen des Testverfahrens im Bereich der Bundesallee zur Kontrolle der Radarsensorik auch Bildaufnahmen des öffentlichen Straßenraums gemacht werden. Wir halten für diesen Zweck eine niedrige Auflösung der Bilder für ausreichend. Keinesfalls ist die Erkennbarkeit personenbezogener Merkmale der Verkehrsteilnehmer wie Kfz-Kennzeichen oder Gesichter erforderlich. Für die Betroffenen muss mit geeigneten Mitteln Transparenz hinsichtlich des Testbetriebs und der Videobeobachtung hergestellt werden.

Der Einsatz von Radarsensoren zur Registrierung freier Parkplätze ist als datenschutzfreundliche Technologie zu begrüßen. Die positiven Effekte für Autofahrer dürfen allerdings nicht mit weiteren Datenerfassungen verknüpft werden, die zu einer weitreichenden Überwachung führen können. Zudem dürfen auch in der Forschungsphase nur im erforderlichen Umfang personenbezogene Daten erhoben und verarbeitet werden.

11 Wirtschaft

11.1 Videoidentifizierung bei Banken

Banken sind verpflichtet, Neukundinnen und -kunden nach den Vorgaben des Geldwäschegesetzes (GwG) zu identifizieren.[152] Bei den Filialbanken ist dies in der Regel kein Problem, denn die Betroffenen kommen zur Kontoeröffnung in die Filiale. Demgegenüber waren Online- und Internet-Banken bisher darauf angewiesen, dass die potenziellen Kundinnen und Kunden das Post-Ident-Verfahren durchlaufen. Dies entspricht nicht den Bedürfnissen des „medienbruchfreien Internet-Zeitalters". Deshalb hat die Bundesanstalt für Finanzdienstleistungen (BaFin) per Rundschreiben[153] die Videoidentifizierung grundsätzlich für rechtmäßig erklärt. Diese würde zu keinen verstärkten Sorgfaltspflichten führen,[154] da die Betroffenen bei der Videoidentifizierung als persönlich anwesend gelten könnten. Das Rundschreiben enthält die salvatorische Klausel, dass die Ausführungen der BaFin unbeschadet von parallel zu beachtenden datenschutzrechtlichen Anforderungen gelten. Inzwischen haben sich verschiedene Unternehmen am Markt etabliert, die als Auftragnehmer für Banken Videoidentifizierungen durchführen.

Trotz des Rundschreibens der BaFin ist zweifelhaft, ob eine Videoidentifizierung geldwäscherechtlich möglich ist. Voraussetzung dafür ist, dass man die per Video zugeschaltete Person als persönlich anwesend betrachtet. Nach dem Vertragsrecht[155] reicht zwar die Videozuschaltung als Anwesenheit aus, das Geldwäschegesetz fordert aber grundsätzlich gerade eine persönliche Anwesenheit. Ist die zu überprüfende Person nicht anwesend und will sie die Videoidentifizierung nutzen, soll sie ein Ausweisdokument in die Kamera halten. Noch offen ist zudem die Frage, ob die angewandten Verfahren wirklich fälschungssicher

152 § 4 GwG
153 Rundschreiben 01/2014 (GW) vom 5. März 2014, S. 7 f.
154 § 6 Abs. 2 Nr. 2 GwG
155 § 147 Bürgerliches Gesetzbuch (BGB)

sind. Auch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hält dieses Verfahren deshalb nicht für gesetzeskonform.[156]

Soweit Banken trotz dieser Bedenken Videoidentifizierung zulassen, sollten sie folgenden datenschutzrechtlichen Mindeststandard beachten:

- Die Kommunikation zwischen den Betroffenen und dem Identifizierungsunternehmen sollte verschlüsselt erfolgen.
- Eine Kommunikation per Skype kommt selbst dann nicht in Betracht, wenn die Betroffenen ausdrücklich zugestimmt haben.
- Die Banken sollten mit ihren Dienstleistern vereinbaren, dass die für die Bank erhobenen und gespeicherten Daten nicht für weitere Banken genutzt werden dürfen (Verbot der Poolbildung).
- Der Dienstleister wird einen Screenshot des Ausweispapieres erstellen. Dabei dürfen nur zur Identifizierung nach dem GwG benötigte Daten gespeichert werden. Andere Daten sind zu löschen.[157] Noch besser ist allerdings ein Verfahren, bei dem die nicht benötigten Daten gar nicht erst aufgenommen werden, was technisch möglich ist.
- Die BaFin geht in dem Rundschreiben davon aus, dass bei dem Gespräch eine Audio- und Videoaufzeichnung stattfindet. Eine Erforderlichkeit der Audioaufzeichnung ist nicht erkennbar. Auch eine Videoaufzeichnung ist nur zulässig, wenn eine entsprechende Einwilligung der Betroffenen vorliegt.

Videoidentifizierungen sind datenschutzrechtlich nicht unproblematisch.

11.2 Politisch exponierte Personen bei der Geldwäscheüberprüfung

Aus der Praxis

Ein Abgeordneter wurde von der deutschen Vertriebsgesellschaft eines Londoner Zahlungsdienstleisters als Kunde abgelehnt, da er eine politisch exponierte Person (PEP) sei. Diese Information habe man durch die Abfrage

156 BfDI, 25. Tätigkeitsbericht (2013-2014), S. 139 f.
157 § 8 Abs. 1 Satz 2 GwG

einer Datenbank erhalten. Geschäftsabschlüsse mit PEPs seien zu aufwendig. Der Abgeordnete fragte uns, ob der Zahlungsdienstleister rechtmäßig gehandelt habe.

Das Geldwäschegesetz verpflichtet Finanzdienstleister bei Geschäftsbeziehungen mit PEPs[158] zu verstärkter Sorgfalt (u. a. Bestimmung der Herkunft der Vermögenswerte, verstärkte kontinuierliche Überwachung), da bei diesem Personenkreis ein erhöhtes Geldwäscherisiko bestehe. Der Finanzdienstleister muss Verfahren implementieren, die sicherstellen, dass bei PEPs die verstärkten Sorgfaltspflichten umgesetzt werden können. Dies setzt voraus, dass der Finanzdienstleister die PEPs ggf. aktiv ermittelt. Grundsätzlich kann deshalb die Vorgehensweise des Zahlungsdienstleisters nicht beanstandet werden. Nach den geldwäscherechtlichen Vorgaben sind die Erhebung und Verarbeitung von „PEP-Daten" zur Begründung eines rechtsgeschäftlichen Vertragsverhältnisses mit den Betroffenen bei Zahlungsdienstleistern erforderlich.[159] Zu berücksichtigen ist auch, dass es sich bei der Information, dass jemand eine PEP ist, um ein allgemein zugängliches Datum handelt.

Nach dem deutschen Geldwäschegesetz sind Abgeordnete in einem deutschen Landtag in der Regel keine PEPs.[160] Allerdings unterfiel der Zahlungsdienstleister als Unternehmen mit Sitz in London nicht dem deutschen, sondern dem englischen Geldwäschegesetz; hier ist nur von „Members of parliaments" (Mitgliedern von Parlamenten) die Rede. Aus diesem Grund ist es nachvollziehbar, dass der Zahlungsdienstleister den Begriff der PEP weiter fasste als nach deutschem Geldwäschegesetz. Die Privatautonomie gestattete es dem Zahlungsdienstleister, einen Vertragsschluss mit dem Abgeordneten abzulehnen.

Finanzdienstleister müssen sicherstellen, dass bei politisch exponierten Personen verstärkte Sorgfaltspflichten angewandt werden.

158 § 6 Abs. 2 Nr. 1 GwG spricht von Personen, „die ein wichtiges öffentliches Amt" ausüben oder ausgeübt haben.

159 § 28 Abs. 1 Satz 1 Nr. 1 Bundesdatenschutzgesetz (BDSG)

160 § 6 Abs. 2 Nr. 1 Satz 2 GwG

11.3 Datenhunger der Bundesbank und der Europäischen Zentralbank

Aus der Praxis

Hinter dem harmlosen Begriff „AnaCredit“ (Analytical Credit Dataset) verbirgt sich die Planung der Europäischen Zentralbank, ein europaweit einheitliches Kreditregister aufzubauen. Es soll den Notenbanken helfen, Bonitätsrisiken bei einzelnen Banken zu erkennen, um eine zweite Lehman-Krise zu verhindern. Die Daten sollen bei geldpolitischen und aufsichtsbehördlichen Fragestellungen herangezogen werden. Nach dem derzeitigen Planungsstand[161] sollen Kredite ab 25.000 Euro eingemeldet werden. Pro Kredit sollen etwa 100 Datenattribute zu sechs Themen (Kreditgeber/Kreditnehmer, Information zu Krediten, Bewertung dieser Kredite, Risikopositionen, Verlustpositionen, Bilanzangaben) an die Bundesbank bzw. die Europäische Zentralbank übermittelt werden.

Da durch „AnaCredit“ nur die Bonität der Banken überprüft werden soll, benötigt die Europäische Zentralbank im zentralen Kreditregister keine personenbezogenen Daten von Kreditnehmerinnen und -nehmern. Diese auf den ersten Blick beruhigende Mitteilung darf aber nicht darüber hinwegtäuschen, dass mit personenbezogenen Daten gearbeitet werden muss, um zu erkennen, ob die Betroffenen mehrere Kredite bei unterschiedlichen Banken erhalten haben, und um evtl. Nachmeldungen zuordnen zu können.

Noch befindet sich das zentrale Kreditregister in der Planungsphase. Bevor „AnaCredit“ implementiert wird, wäre es empfehlenswert, noch einmal zu evaluieren, ob dieses „bürokratische Monster“ wirklich in der Lage ist, Krisen wie die Lehman-Insolvenz, die durch die fehlerhafte Bewertung von verbrieften Krediten entstanden ist, zu verhindern. Bei einer positiven Evaluierung sollte bei der Umsetzung von „AnaCredit“ u. a. Folgendes beachtet werden:

- Da ein europaweit einheitliches Kreditregister entstehen soll, gibt es keine Gründe, für die Bundesbank zusätzliche Forderungen (mehr Daten, früherer Implementierungsbeginn) zu erheben.

161 Derzeit gibt es nur einen Gesetzentwurf für Kredite juristischer Personen.

- Banken sollten möglichst nicht verpflichtet werden, Daten für „AnaCredit“ zu erheben, die sie nicht für den Vertragszweck oder für sonstige bankrechtliche Zwecke benötigen. Bei überschießenden Daten haben die Banken eine strikte Zweckbindung zu beachten. Die Daten sollten möglichst schnell gelöscht werden.
- Banken sollten Betroffene auf die Einmeldung in das zentrale Kreditregister hinweisen.
- Es sollte geprüft werden, ob trotz der Probleme mit Zweitkrediten und Nachmeldungen eine nicht personenbezogene Meldung der Banken an die Zentralbanken möglich ist. Die Banken können über die SCHUFA erkennen, ob ein Zweitkredit vorliegt. Nachmeldungen könnten über ein Pseudonym erfolgen.
- Hilfsweise sollten die personenbezogenen Daten an ein Trust-Center gemeldet werden, das unabhängig von der Bundesbank oder der Europäischen Zentralbank arbeiten sollte.

Das geplante Kreditmelderegister sollte vor seiner Einführung auf seine Erforderlichkeit hin evaluiert werden. In jedem Fall müssen die Datenschutzinteressen der Kreditnehmerinnen und -nehmer ausreichend berücksichtigt werden.

11.4 Probleme bei Versicherungsmaklern

Wer für den Abschluss eines Versicherungsvertrages die Hilfe einer Versicherungsmaklerin oder eines Versicherungsmaklers in Anspruch nimmt, kann Schwierigkeiten haben, den Verbleib der zur Vermittlung anvertrauten personenbezogenen, teils sensitiven Daten zu überblicken. Wir haben ein Maklerunternehmen überprüft, bei dem wir gravierende Transparenzprobleme feststellten. Diese sind aber exemplarisch für die gesamte Branche.

In einer „Erstinformation für meine Kunden“ ließ sich das Unternehmen in 17 Zeilen Einwilligungen für zahlreiche Datenflüsse geben. Diese betrafen u.a. eine übergeordnete Maklerservicegesellschaft, Rückversicherer, Versicherer,

Maklerpools, Auskunfteien und das Recht, Werbung per E-Mail, Fax, Telefon und SMS zu senden. Die Einwilligungserklärung war schon unwirksam, weil sie im Text nicht deutlich hervorgehoben war.[162] Auch nach mehrmaligem Lesen ist für den durchschnittlichen Betroffenen nicht nachvollziehbar, wer unter welchen Bedingungen welche personenbezogenen Daten von ihm erhält.

Auch die branchenübliche Aufgabenverteilung führt nicht dazu, für die Kundinnen und Kunden mehr Transparenz zu ermöglichen. Häufig wissen diese bei Vertragsschluss nicht einmal, ob sie mit einer Hauptmaklerin bzw. einem Hauptmakler, einer Untermaklerin bzw. einem Untermakler oder mit freien Beschäftigten eines Maklerunternehmens gesprochen haben. Gänzlich unübersichtlich wird es, wenn freie Beschäftigte eines Maklerunternehmens gleichzeitig auch eigenständig ein Versicherungsunternehmen führen. Hier wissen die Betroffenen am Ende nicht mehr, mit welcher verantwortlichen Stelle sie überhaupt Kontakt hatten.

Versicherungsmaklerpools bieten Maklern Softwarelösungen an, mit denen sie ihre gesamten Datenbestände im Pool verarbeiten können. Die Pools handeln mit den Versicherungen Mengenrabatte aus und unterstützen die angeschlossenen Unternehmen bei den Vertragsabschlüssen. Die Verträge, die die Maklerpools anbieten, sind unterschiedlich. Teils werden Leistungen angeboten, die über eine bloße Auftragsdatenverarbeitung hinausgehen. Hier ist in der Regel eine Einwilligung der Betroffenen erforderlich.

Die Versicherungsvermittlungsbranche hat inzwischen das datenschutzrechtliche Defizit erkannt und strebt eine für die gesamte Branche geltende Verhaltensrichtlinie an.[163] Die Versicherungen selbst haben gezeigt, dass durch Verhaltensregeln das Datenschutzniveau einer ganzen Branche verbessert werden kann.[164]

Die Transparenz bei der Datenverarbeitung von Versicherungsmaklerunternehmen ist zu verbessern.

162 § 4a Abs. 1 Satz 4 BDSG
163 § 38a BDSG
164 Zum Verhaltenskodex des Gesamtverbands der Deutschen Versicherungswirtschaft (GDV) siehe JB 2012, 15.1

11.5 Online-Lotto

Die Deutsche Klassenlotterie Berlin teilte uns auf Nachfrage mit, dass sie Online-Lottospieler („6 aus 49“) bei der Anmeldung und bei jedem Spiel mit der vom Land Hessen geführten Sperrdatei abgleicht, die personenbezogene Daten von Spielsüchtigen enthält. Hierzu sei sie nach den Konzessionsbedingungen und Vorgaben der Senatsverwaltung für Inneres und Sport als oberster Glücksspielaufsichtsbehörde verpflichtet. Diese ist der Auffassung, dass das Glücksspiel „6 aus 49“, welches offline nicht als gefährliches Spiel angesehen wird, ein gefährliches Spiel darstelle, wenn es per Internet betrieben werde.

Nur Veranstalter von Lotterien mit besonderem Gefährdungspotenzial, Spielbanken und Veranstalter von Sportwetten sind verpflichtet, an dem bundesweiten Spielersperrsystem teilzunehmen.[165] Auch wenn der Glücksspielstaatsvertrag (GlüStV) keine Legaldefinition für Lotterien mit besonderem Gefährdungspotenzial enthält, ist unstreitig, dass „6 aus 49“ kein besonderes Suchtgefährdungspotenzial hat, da diese Lotterie nur zweimal pro Woche veranstaltet wird. Gesperrte Spielerinnen und Spieler dürfen nur an Lotterien, die häufiger als zweimal pro Woche veranstaltet werden, nicht teilnehmen.[166] Die Senatsverwaltung für Inneres und Sport begründet ihre Rechtsauffassung mit § 4 Abs. 5 Nr. 1 GlüStV. Danach sind Veranstalter sämtlicher Glücksspiele im Internet verpflichtet, den Ausschluss Minderjähriger oder gesperrter Spieler durch Identifizierung und Authentifizierung zu gewährleisten. Da auch Sportwetten und gefährliche Lotterien im Internet angeboten werden, wird durch diese Norm sichergestellt, dass keine gesperrten Spielerinnen und Spieler an gefährlichen Spielen teilnehmen können. Dem Wortlaut kann aber nicht entnommen werden, dass Glücksspiel im Internet generell als gefährlich bewertet wird. Die Norm stellt nur klar, dass Sperrungen auch online erfasst werden müssen.

Es ist auch mehr als zweifelhaft, ob eine Lotterie im Internet ein höheres Suchtpotenzial bietet als das Lottospielen im Geschäft. Die Nichtgestattung des Online-Lottos würde auch schon deshalb keinen Sinn machen, weil Gesperrte weiter „6 aus 49“ in einem der zahlreichen Lotto-Annahmestellen spielen

165 § 8 Abs. 2 und 4 Glücksspielstaatsvertrag (GlüStV)
166 § 22 Abs. 2 Satz 1 GlüStV

können. Die Sperrdatei enthält sensitive Daten, denn Spielsucht ist ein Gesundheitsdatum. Schon aus diesem Grunde ist eine restriktive Auslegung von § 4 Abs. 5 Nr. 1 GlüStV geboten.

Daten von Online-Lottospielerinnen und -spielern dürfen nicht mit der Sperrdatei zur Bekämpfung der Glücksspielsucht abgeglichen werden.

11.6 Weitergabe von Daten aus dem Gewerberegister an Arbeitgeber

Aus der Praxis

Das Ordnungsamt des Bezirks Friedrichshain-Kreuzberg informierte die Arbeitgeberin eines Angestellten darüber, dass diesem die Ausübung eines Gewerbes wegen Unzuverlässigkeit untersagt sei.[167] Das Ordnungsamt sah Verdachtsmomente, dass der Betroffene als Vertretungsberechtigter des Unternehmens tätig sei, obwohl auch dies ihm in der Verbotsverfügung untersagt worden war. Später räumte die Behörde ein, dass eine genauere Prüfung ergeben könnte, dass der Petent tatsächlich nicht die Funktion bzw. Stellung eines Vertretungsberechtigten eingenommen habe. Die schnelle Information der Arbeitgeberin sei erforderlich gewesen, um von dieser ein andernfalls drohendes gewerberechtliches Zuverlässigkeitsverfahren abzuwenden.

Der Umgang mit personenbezogenen Daten im gewerberechtlichen Verfahren ist in der Gewerbeordnung bereichsspezifisch geregelt.[168] Danach dürfen Informationen aus gewerberechtlichen Verfahren nur an öffentliche Stellen weitergegeben werden, die an dem gewerberechtlichen Verfahren beteiligt waren, und nur soweit, wie dies zur Erfüllung ihrer Aufgaben erforderlich ist. Andere öffentliche Stellen sind zu informieren, wenn dies für die Verwirklichung der Rechtsfolgen der Gewerbeuntersagung erforderlich ist.[169] Eine Datenübermittlung an nicht-öffentliche Stellen ist danach nicht möglich. Zwar verweist die Gewerbeordnung für die Übermittlung der Daten für andere Zwecke auf

167 § 35 Gewerbeordnung (GewO)
168 § 11 GewO
169 § 11 Abs. 5 GewO

die Datenschutzgesetze der Länder, sie schließt aber eine Übermittlung an nicht-öffentliche Stellen aus.[170]

Das Ordnungsamt war fälschlicherweise davon ausgegangen, dass die Datenübermittlung nach § 6 Abs. 1 Satz 2 Berliner Datenschutzgesetz (BlnDSG) rechtmäßig erfolgt sei. Hierbei übersah es nicht nur, dass der Sachverhalt abschließend in der Gewerbeordnung geregelt ist, sondern auch, dass diese Norm als Ausnahmeregel eng auszulegen ist und nur Datenverarbeitungen erlaubt, die schutzwürdige Belange der Betroffenen nicht beeinträchtigen.

Informationen über eine Gewerbeuntersagung dürfen nicht an private Dritte weitergegeben werden.

11.7 Trojanische Pferde in Form von getarnten Behördenschreiben

Zahlreiche Freiberufler erhielten ein personalisiertes Werbeschreiben eines Unternehmens, das gewerbliche Internetportale zur öffentlichen Darstellung und Empfehlung von Unternehmen betreibt. Das Werbeschreiben war so ausgestaltet, dass nicht auf den ersten Blick erkennbar war, dass mit einer Bestätigung der Daten und Rücksendung des Bogens ein kostenpflichtiger Eintrag für zwei Jahre auf der Internetseite des Unternehmens erfolgte. Vielmehr erweckten die Werbeschreiben den Eindruck, dass die Bestätigung der Daten für eine behördliche Registrierung notwendig waren. Die Werbeschreiben enthielten bereits die Namen der Betroffenen sowie die jeweiligen Anschriften. Diese Daten hatte das Unternehmen teilweise den Internetseiten der Industrie- und Handelskammern (IHKs) und den dort gelisteten Branchenverzeichnissen entnommen.

Grundsätzlich können bei beruflichen Werbeanschreiben, die im Hinblick auf die berufliche Tätigkeit des Betroffenen und unter seiner beruflichen Anschrift

170 Tettinger/Wank/Ennuschat, Gewerbeordnung, 8. Aufl. 2011, § 11 GewO, Rn. 30

erfolgen, Daten aus allgemein zugänglichen Quellen genutzt werden.[171] Es dürfen allerdings keine schutzwürdigen Interessen der Betroffenen entgegenstehen.[172] Dies war aber vorliegend der Fall. Der Bundesgerichtshof hat bereits in ähnlichen Fällen entschieden, dass solche Werbeschreiben, die aufgrund der drucktechnischen Gestaltung den Eindruck eines vermeintlichen Behördenschreibens erwecken, überraschenden Charakter haben.[173] Ein derartiges Werbeschreiben kann nicht rechtmäßig zugesandt werden, da dies nicht im Interesse der Betroffenen liegt. Unsere Recherchen haben ergeben, dass Schutzverbände gegen das Unternehmen zivilrechtliche Klagen wegen der Geschäftspraxis erhoben haben. Außerdem wurde diese Praxis bereits dem Vorgänger des Unternehmens gerichtlich untersagt. Wir haben inzwischen mehrere Bußgeldverfahren wegen der datenschutzrechtlichen Verstöße eingeleitet.

Werbeschreiben, die in betrügerischer Absicht zur Generierung von Verträgen genutzt werden, sind unzulässig.

11.8 Anonymitätsversprechen auf dem Prüfstand

11.8.1 Online

Aus der Praxis

Wer kennt das nicht: Schaut man sich ein Produkt im Onlineshop an, erscheint es wenig später auch in der Bannerwerbung des Nachrichtenportals. Zufall? Wohl kaum. Dahinter steckt eine Werbestrategie, die häufig mit den Begriffen „Targeting“ bzw. „Retargeting“ belegt wird[174] und die im Wesentlichen darauf basiert, dass Personen in ihrem Internetnutzungsverhalten verfolgt und analysiert werden.[175]

171 § 28 Abs. 3 Satz 2 Nr. 2 BDSG; siehe Anwendungshinweise der Datenschutzaufsichtsbehörden zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für werbliche Zwecke (Stand: September 2014), Ziff. 3.7

172 § 28 Abs. 3 Satz 6 BDSG

173 BGH, Urteil vom 26. Juli 2012, VII ZR 262/11

174 Zu Deutsch etwa „ins Visier nehmen“

175 „Web Tracking“, siehe JB 2012, 16.4

Es geht darum, Nutzerinnen und Nutzer webseitenübergreifend wiederzuerkennen und mithilfe dieser Informationen z. B. Werbeplätze auf Webseiten in Echtzeit meistbietend zu verkaufen (sog. Real Time Advertising bzw. Real Time Bidding). Die Verfahren basieren hauptsächlich auf dem Einsatz von Cookies. Diese werden durch die Webseitenbetreiber, aber auch durch Dritte gesetzt, die dazu z. B. nicht sichtbare Webinhalte bereithalten, welche beim Laden einer Webseite über die sog. iframes-Technik eingebunden werden. Den Nutzerinnen und Nutzern werden durch die Cookies Kennungen (kurz „IDs“) zugeordnet, die die beteiligten Akteure untereinander austauschen bzw. mit den eigenen IDs „matchen“. So ist es möglich, die Nutzerinnen und Nutzer bei dem Besuch einer fremden Webseite wiederzuerkennen, ggf. detaillierte Profile zu diesen anzukaufen und diese über fremde Seiten mit Werbeanzeigen zu erreichen. Ausschlaggebend für die Entscheidung, Werbung aufzuspielen, ist damit nicht mehr die potenzielle Zielgruppe einer Webseite, sondern die Kenntnisse über die konkrete Person, die die Webseite in diesem Moment besucht.

Und die Verfolgung der digitalen Spuren geht noch weiter: Das Konzept eines Unternehmens, das wir geprüft haben, zielt darauf ab, die Nutzerinnen und Nutzer nicht nur an einem Gerät wiederzuerkennen, sondern sie geräteübergreifend, vom Home-PC über das Tablet bis zum Smartphone, zu verfolgen. Während ein Home-PC zum Teil von verschiedenen Personen genutzt wird, z. B. durch alle Angehörigen einer Familie, sind Smartphones Gegenstände, die in der Regel einer einzigen Person zuzuordnen sind. Vor diesem Hintergrund wird immer deutlicher, dass die beim Web Tracking aufgezeichneten Informationen nicht nur auf die Geräte, sondern auf die an den Geräten sitzenden einzelnen Nutzerinnen und Nutzer zurückführbar sind.

Personen, nicht Geräte werden ins Visier genommen und gezielt mit Werbung angesprochen. Darauf basieren die Geschäftsmodelle. Trotzdem argumentieren die beteiligten Akteure, dass nur mit zufällig vergebenen IDs und anonymisierten „Profilen“ gearbeitet werde und keine Informationen zur Identifikation von Personen vorlägen. Der Hintergrund ist ein rechtlicher: Ohne Einwilligung der Betroffenen dürfen personenbezogene Nutzungsdaten nicht durch Dritte verwendet werden. Auch das Setzen von Cookies bedarf jedenfalls nach europäischem Recht grundsätzlich einer Einwilligung.[176] Wenn die Daten hin-

176 Art. 5 Abs. 3 der Europäischen E-Privacy-Richtlinie (Richtlinie 2002/58/EG); zur bisher nicht erfolgten Umsetzung dieser Vorgaben in das deutsche Recht, siehe JB 2014, 13.2

gegen anonymisiert sind, dürfen sie zum Zwecke der Marktforschung anderer Diensteanbieter übermittelt werden.[177]

Anonymisieren bedeutet, dass Daten nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Die Bestimmbarkeit einer Person hängt aber nicht davon ab, ob diese namentlich identifiziert werden kann. Im Kontext der Internetwerbung hat es keine Bedeutung, wo eine Person wohnt und wie sie heißt. Personen sollen nicht per Post erreicht, sondern dort und in Echtzeit beworben werden, wo sie sich regelmäßig aufhalten: In der virtuellen Welt. Wesentliche Teile der Lebensgestaltung von Personen sind über die Nutzung von internetfähigen Geräten ablesbar. Die Verarbeitung der Daten hat dann individuelle Folgen für die einzelnen Nutzerinnen und Nutzer: Wenn Personen unterscheidbar und adressierbar sind, können diese wiedererkannt, verfolgt, profiliert, (über die Geräte) kontaktiert und ggf. in ihren Entscheidungen manipuliert werden.

Die Voraussetzungen der Verarbeitung personenbezogener Daten im Internet werden zukünftig u. a. von der neuen EU-Datenschutz-Grundverordnung[178] bestimmt, die sich auch zu den Identifizierungsmöglichkeiten bei der Inanspruchnahme von Onlinediensten äußert.[179] Inwieweit die speziellen Vorgaben der E-Privacy-Richtlinie zum Einsatz von Cookies nach dem Inkrafttreten der Datenschutz-Grundverordnung Bestand haben oder erneuert werden, ist zum jetzigen Zeitpunkt ungewiss. Jedenfalls bleibt zu hoffen, dass sich die Interventionsmöglichkeiten für die Betroffenen künftig auch in der Praxis deutlich verbessern.

Auf Möglichkeiten der Betroffenen, sich gegen das Web Tracking zu wenden, haben wir bereits hingewiesen.[180] Der Einsatz von Werbeblock-Erweiterungen für den Browser kann jedenfalls die Einblendung von Werbung reduzieren und damit z. B. verhindern, dass über das Laden von Bannerwerbung personenbezogene Daten von Dritten erhoben werden. Fraglich ist allerdings, wie zuver-

177 § 15 Abs. 5 Satz 3 TMG
178 Siehe 2.1.1
179 Siehe Erwägungsgrund (24) der EU-Datenschutz-Grundverordnung
180 JB 2012, 16.4

lässig diese Dienste sind bzw. in der Zukunft sein werden: So sind die Betreiber eines viel genutzten Werbeblockers in die Kritik geraten, nachdem sie sich entschlossen, bestimmte Werbung gegen Entgelt doch durchzulassen. Zudem sind manche Webseitenbetreiber mit hohen Besucherzahlen – so z. B. eine große deutsche Boulevardzeitung – dazu übergegangen, ihre Inhalte nur noch abrufbar zu machen, wenn keine Werbeblocker aktiviert sind.

Daten können auch dann personenbezogen sein, wenn zwar keine herkömmlichen Identifikatoren (z. B. der Name), wohl aber eindeutige Informationen verfügbar sind, die es ermöglichen, Personen zu unterscheiden, diese individuell zu adressieren und unterschiedlich zu behandeln.

11.8.2 Offline

Auch in der realen Welt hinterlassen wir digitale Spuren, so z. B. beim Bezahlen mit EC- und Kreditkarten, aber auch beim Einsatz von Kundenkarten.

Anonyme Kundenkarten

Die Deutschen tragen Umfragen zufolge durchschnittlich 4,5 Karten in ihren Geldbörsen. Mehr als jeder zweite Haushalt besitzt eine PAYBACK Karte.[181] Mit Kundenkarten sollen Verbraucherinnen und Verbraucher an das Unternehmen oder die hinter der Kundenkarte stehenden Konzerne gebunden werden und ihre Käufe auf die entsprechenden Geschäfte konzentrieren. Häufig werden für die Rabattgewährung vielfältige personenbezogene Daten zu Interessen, Konsum- und Kaufgewohnheiten sowie soziale und familiäre Verhältnisse über das Anmeldeformular in Erfahrung gebracht. Kundendaten werden so zusammengetragen und mit immer ausgefeilteren Methoden ausgewertet, um immer genauere Kundenprofile zu erhalten.

Inzwischen experimentieren die Unternehmen mit sog. „anonymen Kundenkarten". Anders als bei den üblichen Kundenkarten werden hier gerade

181 https://www.tns-emnid.com/presse/pdf/presseinformationen/tns_emnid_studie_bonusprogramme.pdf und https://www.tns-emnid.com/presse/pdf/presseinformationen/2015_02_02_tns-emnid_bonusprogramme.pdf

keine Informationen wie Namen oder Adressen erfasst. Die Rabattierung erfolgt allein über die Kartennummer, die erworbenen Warenkörbe und den gezahlten Preis.

Solche Konzepte gehen in die richtige Richtung. Allerdings sind die Daten, die beim Einsatz einer solchen Karte von dem Unternehmen erhoben werden, nicht anonym. Es handelt sich um pseudonyme Daten, für die die Regelungen des Bundesdatenschutzgesetzes (BDSG) gelten. Zwar sind die Nutzerinnen und Nutzer einer solchen Karte für die verantwortliche Stelle wesentlich schwerer zu identifizieren, weil das Pseudonym in der Regel nur von dem Betroffenen selbst aufgedeckt werden kann. Je häufiger eine solche pseudonyme Karte jedoch eingesetzt wird, desto mehr Kombinationen von gekauften Produkten werden erfasst, die Rückschlüsse auf individuelle Produktvorlieben zulassen. Es ist nicht auszuschließen, dass Personen über diese Produktprofile wiedererkannt und identifiziert werden können.

Anonymisierung beim Real World Tracking

Mit der Erhebung von Standortinformationen können unsere Bewegungen in der realen Welt digital erfasst werden. So gibt es z. B. neue Methoden, die Wege von Kundinnen und Kunden in einem Laden oder Shoppingcenter zu verfolgen. Dazu werden unterschiedliche Techniken eingesetzt, die darauf basieren, dass immer mehr Personen Smartphones bei sich tragen. Wir berichteten bereits über ein solches „Real World Tracking“,[182] bei dem die von den Smartphones der Kundinnen und Kunden automatisch ausgesendeten Suchanfragen nach einem offenen WLAN[183] von Empfängergeräten in Läden oder Shoppingcentern ausgewertet werden. Mit diesen Informationen, die Aufschluss über die Aufenthaltsorte der Kundinnen und Kunden geben, können die Bewegungsverläufe von Personen individuell nachgezeichnet werden.

Die Identifikation von Geräten und Personen erfolgt bei diesen WLAN-basierten Verfahren über die sog. MAC-Adressen. Dabei handelt es sich um eindeutige Kennungen der Geräte, die durch die Smartphones bei der Suche nach einem offenen WLAN ausgesendet und von den Empfängergeräten im Laden erhoben werden. Die erhobenen Daten können nur dann anonym sein,

182 JB 2014, 13.3

183 Sofern die WLAN-Schnittstelle aktiviert ist

wenn diese Kennungen unkenntlich gemacht bzw. gelöscht werden. Eine wirksame Anonymisierung setzt überdies voraus, dass die aufgezeichneten Wege der Kundinnen und Kunden nicht so individuell sind, dass sie einzelnen Personen zugeordnet werden können und diese unterscheidbar und adressierbar machen.

Wie die Verfahren rechtlich und technisch einzuordnen sind, wird derzeit mit anderen Aufsichtsbehörden in Deutschland erörtert. Auch die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation hat sich mit diesen Fragen auseinandergesetzt.[184]

Bei der Frage, ob Daten anonymisiert sind, muss nicht nur der aktuelle Zeitpunkt berücksichtigt, sondern auch die zukünftige Entwicklung im Blick behalten werden. Soweit Anonymisierungsverfahren eingesetzt werden, müssen diese routinemäßig daraufhin überprüft werden, ob sich die Gefahr der Reidentifizierung angesichts neuer technischer Möglichkeiten realisiert hat.

11.9 Fehlendes Impressum

Wenn Dritte im Internet beleidigt oder herabgesetzt werden, ist es häufig schwierig, die Verantwortlichen zu ermitteln. Insbesondere fehlt es auf den entsprechenden Webseiten in der Regel an dem gesetzlich erforderlichen Impressum.[185] So lag auch der Fall einer Petentin: Ohne ihr Zutun war eine Webseite eigens dafür eingerichtet worden, ausschließlich Inhalte über die Betroffene zu verbreiten. Auch der Name der Webseite setzte sich aus dem Namen der Petentin zusammen. Das Impressum hingegen enthielt nur eine nicht sprechende E-Mail-Adresse und keine weiteren Kontaktangaben, die Hinweise auf die für die Veröffentlichung Verantwortlichen hätten liefern können.

Die Veröffentlichungen betrafen die berufliche Betätigung der Petentin als Sachverständige. Sie vermittelten den Eindruck, dass über „verifizierte Informationen", Dokumente und die „Einschätzung von Fachleuten" belegt werden

184 Siehe 15.6
185 § 5 TMG

könne, dass die Petentin weder persönlich noch fachlich zur Ausübung ihres Berufs geeignet sei. Die Webseite war über die einschlägigen Suchmaschinen indexiert und konnte bei einer namentlichen Suche der ersten Seite der Trefferliste entnommen werden. Die Petentin berichtete, dass die Veröffentlichungen zu massiven beruflichen Beeinträchtigungen geführt hätten, da sie als Sachverständige auf einen einwandfreien Ruf angewiesen sei.

Die Webseite wurde von einem Dienstleister gehostet, der seinen Kundinnen und Kunden die Erstellung von Homepages nach einem Baukastenprinzip anbietet. Auf unsere Nachfrage stellte der Dienstleister fest, dass die Betreiber der Webseite gegen seine Nutzungsbedingungen verstießen. Die Kundinnen und Kunden, die ihre Homepages erstellen und hosten lassen, waren nach den Nutzungsbedingungen des Dienstleisters verpflichtet, ihrer Impressumspflicht ordnungsgemäß nachzukommen. Da dies vorliegend nicht erfüllt war, sperrte der Dienstleister die Webseite und löschte sie später, sodass die Inhalte nicht mehr abrufbar waren. Die Einhaltung der Impressumspflicht ist im Übrigen auch Voraussetzung dafür, dass die datenschutzrechtliche Kontrolle der Webseiten-Betreiber durch Betroffene und die Aufsichtsbehörde ermöglicht wird. Zuständig für die Verhängung von Bußgeldern bei Verletzung der Impressumspflicht sind derzeit die Bezirke bzw. die Medienanstalt Berlin-Brandenburg.[186]

Auch wenn ein Hostprovider für fremde Inhalte grundsätzlich nicht haftet, kann er dennoch als sog. „Störer" von den Betroffenen in die Pflicht genommen werden. Weisen die Betroffenen die Hostprovider auf eine Verletzung ihrer Persönlichkeitsrechte hin, können diese nach der Rechtsprechung verpflichtet sein, zukünftige Verletzungen zu verhindern.

186 Siehe 13.3

11.10 Videoüberwachung, Drohnen und Dashcams

11.10.1 Videoüberwachung im ÖPNV – aber bitte mit Augenmaß!

Nach den schrecklichen Anschlägen in Paris wurde auch hierzulande wieder der Ruf nach mehr Videoüberwachung im öffentlichen Nah- und Regionalverkehr laut. Mehr Videoüberwachung kann zwar in Einzelfällen zur nachträglichen Aufklärung beitragen, verhindern kann sie solche Anschläge oder die Begehung von Straftaten jedoch nicht. Der Ausbau von Videoüberwachung ist daher kein Allheilmittel zur Gewährung eines effektiven Schutzes der Bevölkerung.

Daher ist es umso wichtiger, Videoüberwachung in ein intelligentes Sicherheitskonzept einzubetten und sie dort gezielt einzusetzen, wo sie sinnvoll zum Tragen kommen kann. Eine flächendeckende unterschiedslose Überwachung ist kaum hilfreich und greift gleichzeitig stark in die Persönlichkeitsrechte der Betroffenen ein. Sie kann ein diffuses bedrohliches Gefühl der Überwachung hervorrufen, das einer demokratischen Gesellschaft abträglich ist.

Allerdings ist genau das in den vergangenen Jahren offenbar ein verstärkter Trend. Wir wurden darauf aufmerksam gemacht, dass bundesweit mehrere Verkehrsverbünde bei Neuausschreibungen im öffentlichen Personennah- und Regionalverkehr von den Verkehrsunternehmen pauschal eine Rund-um-die-Uhr-Überwachung in Zügen auf sämtlichen Verkehrslinien verlangten. Diese sollte unabhängig davon stattfinden, ob es sich um eine Linie in einem gefährdeten Innenstadtbereich oder eine Verbindung in Randbezirken handelt, in denen kaum Straftaten zu erwarten sind. Wir haben daher gemeinsam mit den anderen Datenschutzaufsichtsbehörden der Länder und des Bundes eine Orientierungshilfe erarbeitet, die die gesetzlichen Anforderungen an eine Videoüberwachung in Zügen des Personennah- und Regionalverkehrs konkretisiert.[187]

Insbesondere haben wir deutlich gemacht, dass vor dem Einsatz der Videotechnik eine Gefährdungsanalyse und eine Abwägung mit den Persönlichkeits-

187 Orientierungshilfe „Videoüberwachung in öffentlichen Verkehrsmitteln“ des Düsseldorfer Kreises (Stand: 16. September 2015), Dokumentenband 2015, S. 54

rechten der Fahrgäste durchgeführt werden müssen. Anders als bei der Videoüberwachung von Bahnhöfen sind Reisende in Zügen länger unter Beobachtung, sodass ein tieferer Grundrechtseingriff angenommen werden kann. Wir haben diese Orientierungshilfe der S-Bahn Berlin GmbH zugeleitet, da im aktuellen Ausschreibungsverfahren zum Teilnetz Ring ebenfalls eine Ausrüstung der neuen Züge mit Videotechnik gefordert wird. Wir werden die S-Bahn beratend begleiten, wenn die Technik eingesetzt werden soll. Für die BVG ist die Orientierungshilfe zwar nicht unmittelbar anwendbar, da diese als Anstalt des öffentlichen Rechts Sondervorschriften des Berliner Datenschutzgesetzes unterliegt. Die Grundsätze der Orientierungshilfe haben allerdings auch dort ihre Gültigkeit.

Einer Videoüberwachung in Zügen des Personennah- und Regionalverkehrs muss eine Gefährdungsanalyse vorausgehen, die eine Abwägung mit den Persönlichkeitsrechten der Betroffenen beinhaltet. Sie sollte in ein sinnvolles Sicherheitskonzept eingebettet werden. Ansonsten droht eine solche Maßnahme in bloßem Aktionismus zu verpuffen, der nicht sinnvoll zur Sicherheit beiträgt und gleichzeitig die Persönlichkeitsrechte der Betroffenen unangemessen beeinträchtigt.

11.10.2 Einsatz von Drohnen zu privaten und kommerziellen Zwecken

Aus der Praxis

Ein deutscher Liedermacher vermutete einst, dass über den Wolken die Freiheit wohl grenzenlos sei. Mithilfe von Drohnen ist diese Vermutung auch ohne eine teure Flugreise mittlerweile nachprüfbar. Der Ausdruck „Drohne" wird umgangssprachlich sowohl für militärisch, privat oder kommerziell genutzte unbemannte, ferngesteuerte Luftfahrzeuge verwendet. Flugdrohnen werden in vielfältiger technischer Ausstattung inzwischen in jedem Elektronikmarkt angeboten und immer häufiger von Privaten für die Freizeitbeschäftigung gekauft und im nachbarschaftlichen Umfeld eingesetzt.

Eine kritische datenschutzrechtliche Betrachtung ist nötig, wenn diese Flugdrohnen zusätzlich mit Digital-, Videokameras oder Mikrofonen bestückt werden und damit eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten einhergeht. Der potenziell beobachtete Bereich wird nur von

den technischen Gegebenheiten der eingesetzten Kamera begrenzt. Mauern, Zäune oder sonstige Abtrennungen, die Dritten das Betreten des so geschützten Bereichs oder den Einblick in diesen erschweren oder unmöglich machen sollen, stellen im Rahmen des Drohneneinsatzes kein Hindernis mehr dar. Da können durchaus Begehrlichkeiten aufkommen: Ein unbeobachteter Blick in den Garten des Nachbarn, auf die Sonnenterrasse oder in sonstige nicht einfach zugängliche Orte.

Für Betroffene ist es hingegen nicht ohne Weiteres möglich, den für den Drohneneinsatz Verantwortlichen zu erkennen. Aus diesen Gründen kann ein solcher mobiler Kameraeinsatz im Vergleich zum Einsatz einer stationären Videoüberwachungsmaßnahme mit einem ungleich größeren Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen verbunden sein. In einigen Fällen war es den Betroffenen allerdings möglich, den Besitzer der Drohne zu identifizieren, sodass uns entsprechende Eingaben erreicht haben. So haben wir die Mitteilung eines Kleingärtners erhalten, dass auf dem Nachbargrundstück in seiner Kleingartenkolonie eine solche Drohne im Einsatz gewesen sei, mit der Bildaufnahmen von benachbarten Parzellengrundstücken und öffentlichen Flächen gemacht worden seien. Bei unserer Überprüfung stellte sich allerdings heraus, dass keine Fotos oder Videoaufnahmen der Nachbargrundstücke entstanden sind.

Das Bundesdatenschutzgesetz ist anwendbar, soweit die Videoaufnahmen nicht ausschließlich zu persönlichen oder familiären Zwecken erfolgt.[188] Dies ist insbesondere dann zweifelhaft, wenn Nachbargrundstücke oder der öffentlich zugängliche Raum beobachtet oder die Aufnahmen für jedermann zugänglich ins Internet gestellt werden. Da Videoaufnahmen von öffentlich zugänglichen Räumen nur im Rahmen eines berechtigten Interesses erfolgen dürfen und der Umstand der Beobachtung erkennbar gemacht werden muss,[189] ist diese in der Regel unzulässig. Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben in einem Beschluss vom September Rahmenbedingungen für den Einsatz von Drohnen formuliert.[190]

188 § 27 Abs. 1 Satz 2 BDSG
189 § 6b BDSG
190 Beschluss des Düsseldorfer Kreises vom 15./16. September 2015: Nutzung von Kameradrohnen durch Private, Dokumentenband 2015, S. 53

Auch die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (sog. Berlin Group) hat bereits 2013 unter unserem Vorsitz Empfehlungen für die Begrenzung des Einsatzes von Drohnen erarbeitet.[191]

Grundsätzlich sollte niemand ohne seine Einwilligung gefilmt und die Privatsphäre anderer geachtet werden. Private Nutzer dürfen Drohnen mit Foto- oder Videoausrüstung nur in solchen Bereichen einsetzen, in denen eine Verletzung von Rechten Dritter ausgeschlossen werden kann.

11.10.3 Einsatz von Dashcams

Die datenschutzrechtliche Problematik von Dashcams haben wir zuletzt 2013 thematisiert.[192] Seitdem hat der Einsatz dieser Kameras stetig zugenommen, was vermutlich auf das vielfältige und zunehmend preisgünstige Angebot solcher Produkte im Einzelhandel zurückzuführen ist.

Diese Entwicklung hat uns 2014 dazu veranlasst, gemeinsam mit den anderen Datenschutzaufsichtsbehörden des Bundes und der Länder einen Beschluss zu verabschieden.[193] Danach ist der Dauerbetrieb solcher Kameras grundsätzlich unzulässig. Das informationelle Selbstbestimmungsrecht umfasst das Recht des Einzelnen, sich in der Öffentlichkeit frei zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Dashcams zeichnen den Verkehr sowie Personen, die sich in der Nähe einer Straße aufhalten, ohne Anlass und permanent auf. Damit ist eine Vielzahl von Verkehrsteilnehmern betroffen, die sämtlich unter Generalverdacht gestellt werden, ohne dass sie von der Überwachung Kenntnis erlangen oder sich dieser entziehen können.

Dieser Beschluss betont, dass das Filmen im öffentlichen Straßenland nur bei einem berechtigten Interesse zulässig ist und daher ein konkreter Anlass für eine Videoüberwachung vorliegen muss.[194] Auch muss der Umstand der

191 Dokumentenband 2013, S. 180
192 JB 2013, 4.3.2
193 Beschluss des Düsseldorfer Kreises vom 25./26. Februar 2014: Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams), Dokumentenband 2014, S. 46
194 § 6b Abs. 1 Nr. 3 BDSG bzw. § 28 Abs. 1 Satz 1 Nr. 2 BDSG

Beobachtung erkennbar gemacht werden.[195] In einem unserer Fälle versuchte ein Sicherheitsunternehmen diesen Anforderungen gerecht zu werden, indem auf der Heckscheibe des Firmenfahrzeugs der deutlich sichtbare Schriftzug „Videofahrzeug“ angebracht wurde. Dennoch war die Videoüberwachung unzulässig, da die Betroffenen durch die Aufschrift zu spät und nicht ausreichend informiert wurden. Außerdem war die Kamera anlasslos in ständigem Betrieb, sodass auch kein berechtigtes Interesse des Kamerabetreibers angenommen werden konnte. Auf die Verhängung eines Bußgelds haben wir in diesem Fall verzichtet, da der Betreiber die Videoüberwachung freiwillig eingestellt hat.

Andere Fahrzeughalter nennen häufig als Begründung für den Einsatz von Dashcams, im Falle eines Unfalls den Hergang nachzuvollziehen und das Video ggf. als Nachweis bei der Regulierung von Schadensfällen und der Klärung von Haftungsfragen heranziehen zu können. Das Interesse des Autofahrers, für den eher seltenen Verkehrsunfall Videoaufnahmen als Beweismittel zur Hand zu haben, kann den Eingriff in die Persönlichkeitsrechte einer Vielzahl von Verkehrsteilnehmenden aber nicht rechtfertigen. In der Rechtsprechung ist ohnehin umstritten, ob solche Videoaufnahmen, die rechtswidrig erstellt wurden, als Beweismittel in einem Zivilprozess verwendet werden dürfen.[196]

Schon aus Rücksicht auf die Privatsphäre der anderen Verkehrsteilnehmenden sollte auf den Einsatz von Dashcams verzichtet werden. Ohnehin ist zweifelhaft, ob die gewonnenen Bilder bei einem Verkehrsunfall zur Klärung beitragen können und vor Gericht als Beweismittel zugelassen werden. Der Betrieb von Dashcams ist unzulässig und kann mit einem Bußgeld geahndet werden.

195 § 6b Abs. 2 BDSG bzw. § 28 Abs. 1 Satz 1 Nr. 2 BDSG

196 Ablehnend z. B. LG Heilbronn, Urteil vom 17. Februar 2015, I 3 S 19/14; AG München, Urteil vom 13. August 2014, 345 C 5551/14; bejahend z. B. AG Nürnberg, Urteil vom 18. Mai 2015, 18 C 8938/14

12 Politische Parteien

12.1 E-Mail-Werbung an Rechtsanwältinnen und Rechtsanwälte

Aus der Praxis

Ein Rechtsanwalt erhielt vom CDU-Kreisverband Charlottenburg-Wilmersdorf per E-Mail Werbung für eine öffentliche Diskussionsveranstaltung, an der auch der Senator für Justiz und Verbraucherschutz teilnahm. Dem Rechtsanwalt war nicht klar, wie der CDU-Kreisverband an seine E-Mail-Adresse gekommen war. Eine Einwilligung zur Nutzung für Werbezwecke hatte er nicht erteilt.

In einer ersten Stellungnahme informierte uns die CDU darüber, dass dem Anwalt die Werbung wegen seiner beruflichen Eigenschaft als in Berlin zugelassener Rechtsanwalt zugegangen sei. Die Anschrift sei über das bundesweite Anwaltsverzeichnis der Bundesrechtsanwaltskammer ermittelt worden. Die Einladung diene der politischen Willensbildung in der Bundesrepublik Deutschland. Man habe dem Rechtsanwalt darüber hinaus die Möglichkeit geben wollen, im Rahmen einer fachbezogenen Veranstaltung Gelegenheit zur Aussprache mit dem Justizsenator zu haben. Mit der Einladung seien keine Werbeabsichten verbunden gewesen.

Auch die Information zu einer Diskussionsveranstaltung ist eine Werbemaßnahme. Eine Datenübermittlung oder -nutzung zu Werbezwecken ist auch bei listenmäßig zusammengefassten Daten wie derjenigen der Bundesrechtsanwaltskammer mit schutzwürdigen Interessen der Betroffenen abzuwägen.[197] Die E-Mail-Adresse gehört allerdings ohnehin nicht zu den Daten, deren Nutzung zu Werbezwecken vom Gesetz privilegiert sind.[198]

Bei der infrage stehenden E-Mail hätte zudem in Betracht gezogen werden müssen, dass das allgemeine Persönlichkeitsrecht auch vor unerwünschter politischer Werbung schützt. Ein Rechtsanwalt ist darüber hinaus ein unabhängiges

197 § 28 Abs. 3 Satz 6 Bundesdatenschutzgesetz (BDSG)
198 § 28 Abs. 3 Satz 2 BDSG

Organ der Rechtspflege. Parteipolitische Bewerbung oder Information ist daher nicht selbstverständlich. Er ist zu sorgfältiger Lektüre seiner Posteingänge verpflichtet und kann diese demnach nicht einfach überlesen.

Die Verzeichnisse der Rechtsanwaltskammern dienen der Information der Behörden und Gerichte, der Rechtssuchenden sowie anderer am Rechtsverkehr Beteiligter.[199] Eine Nutzung für Werbe- und Informationsvorhaben lässt sich aus diesen Speicherzwecken nicht ableiten.

Der CDU-Kreisverband Charlottenburg-Wilmersdorf hat uns versichert, ein derartiges Vorgehen nicht zu wiederholen. Außerdem hat er ein für ihn negatives zivilgerichtliches Urteil des Beschwerdeführers in dieser Sache, ohne weitere Rechtsmittel einzulegen, akzeptiert.

Auch Parteiwerbung ist nur in den vom BDSG festgelegten Grenzen zulässig.

12.2 Alternative für Deutschland (AfD) versus Weckruf

Im Frühjahr wurde in der Partei AfD ein Richtungsstreit geführt. Eines der drei Bundesvorstandsmitglieder verschickte über den Mitgliederverteiler der Partei eine E-Mail, der Informationen eines anderen Mitglieds zu einem neu gegründeten Verein „Weckruf 2015“ beigefügt waren. Viele Mitglieder beschwerten sich bei uns, das Vorstandsmitglied habe den Verteiler zu parteifremden Werbezwecken missbraucht.

Ein Vorstandsbeschluss berechtigte alle drei Bundesvorstandsmitglieder, für ihre Arbeit und zur Erfüllung ihrer Aufgaben unter Berücksichtigung des Zwecks und des Interesses der Partei auf die Mitgliederdatenbank zuzugreifen. Auf diesen Beschluss berief sich das Vorstandsmitglied. Die E-Mail wurde über den E-Mail-Account des Vorstandsmitglieds versandt. Sie informierte über den Verein „Weckruf 2015“, der sowohl AfD-Mitgliedern als auch Externen zum Beitritt offenstand. Die zum damaligen Zeitpunkt vielfältig formulierten Ziele bezogen sich alle auf einen Richtungswechsel innerhalb der AfD. Es wurde

199 § 31 Abs. 1 Satz 3 BRAO

diskutiert, ob „Weckruf 2015“ als Konkurrenz für die AfD zu verstehen ist. Erst später trat das handelnde Vorstandsmitglied aus der AfD aus und in eine neue Partei ein.

Der Bundesvorstand teilte uns auf Nachfrage mit, er habe per Beschluss die Gründung des Weckruf-Vereins politisch missbilligt. Allerdings habe er auch bestimmt, eventuelle Beschlüsse oder Forderungen nach einer Unvereinbarkeit zwischen AfD und Weckruf-Verein ebenfalls zu missbilligen. Daher verstoße die Bewerbung des Weckruf-Vereins unter Nutzung der Mitgliederdaten nicht gegen die Satzung oder die politischen Intentionen der AfD.

Diese politische Interpretation ist im Rahmen unserer Untersuchung berücksichtigt worden. Danach kann nicht ausgeschlossen werden, dass es sich um eine erforderliche Information für die Parteiarbeit gehandelt hat.[200] Für die Nutzung sensitiver personenbezogener Daten durch Parteien wird verlangt, dass die Verwendung der Daten für die Parteiarbeit erforderlich war, sie mit schutzwürdigen Interessen der Betroffenen abgewogen wurde und die Nutzung organisationsintern erfolgte. Aufgrund der Beschlüsse des Vorstands verstößt die Versendung nicht gegen die Satzung oder Intentionen der AfD. Als entscheidendes Umsetzungsgremium muss dem Vorstand der AfD ein gewisser Ermessensspielraum zugestanden werden. Er entscheidet, was für die Arbeit der Partei notwendig ist.

Eine Parteimitgliedschaft ist ein sensitives Datum, da sie auf politische Motivationen schließen lässt. Die Verwendung einer privaten E-Mail-Adresse durch eine Partei ist nur erlaubt, wenn dies für die Tätigkeit der Partei erforderlich ist. Ein solcher Grund kann z. B. die parteiinterne Meinungsfindung sein. Dies gilt insbesondere, wenn eine E-Mail mit Informationen keine dem Parteizweck zuwiderlaufenden Interessen verfolgt.

200 Die spezielle Rechtsgrundlage hierfür ist § 28 Abs. 9 Satz 1 BDSG.

12.3 Veröffentlichung der Beitragspraxis als politisches Druckmittel

In vielen politischen Parteien legen Beitrags- und Kassenordnungen fest, dass Mandatsträgerinnen und Mandatsträger Beiträge, die sie für diese Arbeit erhalten, anteilig an die Partei abführen. Die Beitrags- und Kassenordnungen erlauben auch die Veröffentlichung dieser tatsächlich geleisteten Beiträge auf einer öffentlichen Versammlung unter namentlicher Nennung der Leistenden. Dies soll einerseits der Kontrolle der Mandatsträgerinnen und Mandatsträger durch die Parteibasis dienen, andererseits die Finanzierung der Parteien sicherstellen. Ein Bezirksverordneter von Bündnis 90/DIE GRÜNEN wandte sich gegen die Veröffentlichung wegen datenschutzrechtlicher Bedenken. Daraufhin wurde seine Beitragspraxis als einzige von dieser Darstellung ausgenommen.

Eine Veröffentlichung tatsächlich gezahlter Beiträge von Mandatsträgerinnen und Mandatsträgern ist rechtswidrig, denn es gibt hierfür keine Rechtsgrundlage und eine Einwilligung ist aufgrund der Einschränkung der Freiheit des Mandats nicht wirksam.[201]

Die Beitrags- und Kassenordnungen der Parteien haben keine Rechtsnormqualität. Sie kommen daher nicht als Rechtsgrundlagen für eine namentliche Veröffentlichung im Sinne des BDSG in Betracht. Auch im Parteiengesetz (PartG) findet sich keine bereichsspezifische Rechtsvorschrift zur Veröffentlichung der Höhe der Beiträge. Nur der aus einzelnen Rechenschaftsberichten zusammengefügte Gesamtrechenschaftsbericht ist vom Vorstand der Partei zu veröffentlichen.[202] Alle anderen Zuwendungen sind dem einzelnen Rechenschaftsbericht nur beizufügen[203] und daher kein Bestandteil desselben. Darüber hinaus sind ausschließlich Spenden und Mandatsträgerbeiträge im Rechenschaftsbericht zu verzeichnen, deren Gesamtwert in einem Kalenderjahr 10.000 € übersteigt.[204] Auch die für Parteien spezielle Rechtsgrundlage[205] zur organisationsinternen

201 § 4 Abs. 1 BDSG
202 § 23 Abs. 1 Satz 1 PartG
203 § 24 Abs. 3 Satz 2 PartG
204 § 25 Abs. 3 Satz 1 PartG
205 § 28 Abs. 9 BDSG

Verwendung personenbezogener Daten ist nicht anwendbar, da es nicht um die Mandatsträgereigenschaft, sondern eine grundsätzliche Zahlungsfähigkeit oder -bereitschaft geht.

Im Gegensatz zum Mitglieds- ist der Mandatsträgerbeitrag rechtlich gesehen eine Spende. Eine Parteienfinanzierung dieser Art ist legitim. Allerdings legt der Begriff nahe, dass eine Spende stets freiwillig erfolgt und ihre Höhe nicht entsprechend einem Mitgliedsbeitrag vorgeschrieben werden kann. Wird der Mandatsträgerbeitrag personenbezogen veröffentlicht, kann öffentlicher Druck erzeugt werden, eine eigentlich freiwillige Zahlung leisten zu müssen. Mittelbar wäre so auch Druck auf die politische Arbeit der Abgeordneten möglich. Es entsteht der Eindruck, hier wird über die Zahlungsfähigkeit und -bereitschaft Einfluss darauf genommen, ob die- oder derjenige zukünftig wieder zur Wahl aufgestellt und durch die Anwesenden gewählt wird. Ein Verzicht auf die Entschädigung ist für Mandatsträgerinnen und Mandatsträger unzulässig.[206] Auch ein Zwang zur Spende ist damit unzulässig. Darüber hinaus ist geregelt, dass staatliche Zuschüsse an die Fraktionen für ihren personellen und sachlichen Aufwand gezahlt werden, sodass eine Notwendigkeit der Parteienfinanzierung durch eine Pflichtabgabe und erst recht der durch eine Veröffentlichung ausgeübte Zwang nicht legitim sind.[207] Allgemein ist der Kontrollanspruch einer Partei gegenüber Mandatsträgerinnen und Mandatsträgern wegen der Freiheit des Mandats[208] in einer demokratischen Partei kein geeigneter Rechtfertigungsgrund.

Geht aus der Veröffentlichung hervor, dass jemand nicht in der vereinbarten Höhe geleistet hat, entsteht so eine unnötige Stigmatisierung. Dies gilt auch für den Fall, dass ein Mandatsträger Zweifel an der Veröffentlichung anmeldet und aus diesem Grund die Benennung seiner geleisteten Zahlung bei der Veröffentlichung ausgespart wird. Diejenigen, die das betrifft, würden sich einem öffentlichen Rechtfertigungsdruck ausgesetzt sehen. Die dadurch eingeschränkte Freiwilligkeit ermöglicht auch keine Veröffentlichung auf Einwilligungsbasis.

Eine Veröffentlichung der Parteibeiträge von Mandatsträgerinnen und Mandatsträgern ist rechtswidrig.

206 § 8 Abs. 2 Gesetz über die Entschädigung der Mitglieder der Bezirksverordnetenversammlung, der Bürgerdeputierten und sonstiger ehrenamtlich tätiger Personen
207 ebenda, § 8a
208 Art. 38 Abs. 1 i.V. m. Art. 28 Grundgesetz und Art. 38 Abs. 4 Satz 2 Verfassung von Berlin

14 Europäischer und internationaler Datenschutz

14.1 Erneut wegweisende Entscheidungen des Europäischen Gerichtshofs

Nach den spektakulären Urteilen zur Vorratsdatenspeicherung und zum Recht auf Vergessen im letzten Jahr[231] hat der Europäische Gerichtshof (EuGH) weitere drei für den Datenschutz wegweisende Entscheidungen gefällt. Diese Rechtsprechung des EuGH hat teilweise unmittelbare Auswirkungen für Deutschland und Berlin.

In einem Vorlageverfahren des Berufungsgerichts in Rumänien ging es um die Frage, unter welchen Bedingungen personenbezogene Daten zwischen zwei Verwaltungsbehörden eines Mitgliedstaats übermittelt werden dürfen.[232] Die Kläger im Ausgangsverfahren waren der rumänischen Steuerverwaltung als selbstständig Tätige bekannt. Sie übermittelte die von ihnen erklärten Einkünfte der Nationalen Kasse der Krankenversicherungen, die dann die Zahlung rückständiger Beiträge verlangte. Der Gerichtshof gelangte zu dem Ergebnis, dass die Europäische Datenschutzrichtlinie 95/46/EG der Übermittlung personenbezogener Daten an eine Verwaltungsbehörde desselben Mitgliedstaats zur dortigen Datenverarbeitung für andere Zwecke entgegensteht, wenn die betroffene Person hierüber nicht vorab unterrichtet wurde.

Eine weitere Entscheidung des EuGH betraf die Frage des anwendbaren Rechts in einem Vorlageverfahren des Obersten Gerichtshofs Ungarns.[233] Eine in der Slowakei eingetragene Gesellschaft betrieb eine Webseite zur Vermittlung von in Ungarn belegenen Immobilien. Die Inserate waren einen Monat lang kostenlos. Inserenten verlangten am Ende des Monats die Löschung ihrer Inserate und der sie betreffenden personenbezogenen Daten. Dies wurde abgelehnt

231 JB 2014, 11.2 und 11.3
232 EuGH, Urteil vom 1. Oktober 2015, C-201/14 (Rs. Bara u. a.)
233 EuGH, Urteil vom 1. Oktober 2015, C-230/14 (Rs. Weltimmo)

und darüber hinaus den Inserenten die Inserierungsleistung in Rechnung gestellt. Mangels Zahlung übermittelte der Immobilienvermittler die personenbezogenen Daten der Inserenten an Inkassounternehmen. Nachdem die ungarische Datenschutzbehörde deswegen ein Bußgeld von umgerechnet ca. 32.000 € verhängt hatte, hat der Immobilienvermittler diese Entscheidung bei den ungarischen Gerichten angefochten. Der EuGH hatte im Vorlageverfahren die Frage zu entscheiden, ob die Europäische Datenschutzrichtlinie 95/46/EG der ungarischen Datenschutzbehörde erlaubt, das ungarische Recht auf eine in einem anderen EU-Mitgliedstaat ansässige Firma anzuwenden und ein Bußgeld zu verhängen. Der EuGH hat dies für den Fall bejaht, dass der slowakische Immobilienvermittler über eine „Niederlassung" in Ungarn verfügt. Dieser Begriff umfasse jede tatsächliche und effektive Tätigkeit, die mittels einer festen Einrichtung ausgeübt wird, selbst wenn sie nur geringfügig ist. Dazu könne auch ein Vertreter mit einer Adresse in Ungarn gehören, was von dem vorlegenden Gericht zu überprüfen sei. Mit diesem Urteil hat der EuGH indirekt klargestellt, dass sich ausländische Internet-Unternehmen, die in Deutschland eine „Niederlassung" im weiteren Sinne haben, an deutsches Datenschutzrecht halten müssen. Das gilt allerdings nur bis zum Inkrafttreten der EU-Datenschutz-Grundverordnung (voraussichtlich 2018), die das nationale Datenschutzrecht harmonisieren wird.[234]

Ein wahres Erdbeben hat das Urteil des EuGH zum Safe Harbor-Abkommen der EU mit den USA verursacht, das gekippt wurde.[235]

Das Abkommen, das seit 2000 auch vielen kleinen und mittelständischen Unternehmen in der EU als Rechtsgrundlage für Datenübermittlungen in die USA diente, wurde für ungültig erklärt.[236] Zuletzt hatten sich mehr als 5000 US-Unternehmen als Empfänger von personenbezogenen Daten aus der EU zur Einhaltung der Safe Harbor-Grundsätze verpflichtet. Der Gerichtshof war den Schlussanträgen des Generalanwalts beim EuGH gefolgt, der das Abkommen für unvereinbar mit dem europäischen Datenschutzrecht gehalten hatte.[237]

234 Siehe 2.1.1

235 EuGH, Urteil vom 6. Oktober 2015, C-362/14 (Rs. Schrems), in: EuGRZ 2015, S. 562 ff.

236 Strenggenommen handelte es sich nicht um ein Abkommen, sondern um eine Entscheidung der EU-Kommission, die nach Verhandlungen mit den USA getroffen wurde; JB 2000, 4.7

237 Schlussanträge des Generalanwalts beim EuGH vom 23. September 2015

Dem Verfahren lag die Klage eines österreichischen Jurastudenten zugrunde. Er hatte vor dem irischen High Court den für die Europazentrale von Facebook zuständigen irischen Datenschutzbeauftragten verklagt, weil dieser trotz seiner Beschwerde gegen die Datenverarbeitung von Facebook nicht tätig geworden ist: Der irische Datenschutzbeauftragte sah sich durch das Safe Harbor-Abkommen gebunden, das ein Einschreiten gegen ein Unternehmen wie Facebook, das sich den Safe Harbor-Grundsätzen unterworfen hatte, nicht zulasse. Der irische High Court hat daraufhin das Verfahren ausgesetzt und die entscheidungsrelevanten Fragen dem EuGH zur Vorabentscheidung vorgelegt.

Der EuGH hat die Unwirksamkeit des Safe Harbor-Abkommens im Wesentlichen damit begründet, dass US-Unternehmen nach US-Recht den Geheimdiensten massenhaft Zugriff auf personenbezogene Informationen gewährten, sodass die USA eben kein „sicherer Hafen" für europäische Daten seien. Das habe die Europäische Kommission vor zwei Jahren nach den NSA-Enthüllungen von Edward Snowden selbst festgestellt.[238] Auch hat der Gerichtshof bemängelt, dass europäische Bürger in den USA bisher keinen Rechtsschutz haben, um z. B. die Löschung oder Berichtigung ihrer Daten durchzusetzen. Schließlich hätte die Europäische Kommission die Befugnis der nationalen Datenschutzbehörden, Datenflüsse in die USA zu kontrollieren, im Abkommen nicht einschränken dürfen. Dadurch sei die Unabhängigkeit der Datenschutzbehörden verletzt worden. Die Entscheidung bedeutet für den konkreten Fall, dass der irische Datenschutzbeauftragte nun klären muss, ob Facebook durch die Datenübermittlungen in die USA gegen europäisches Datenschutzrecht verstößt.

Das Urteil wird über den konkreten Fall hinaus allerdings auch Auswirkungen auf andere Entscheidungen der Europäischen Kommission haben, mit denen die Angemessenheit des Datenschutzniveaus in Drittländern festgestellt worden war. Das könnte z. B. Kanada und Neuseeland betreffen, die wie die USA zum informellen Geheimdienstverbund der sog. „Five Eyes" gehören.[239] Daneben dürften die weiteren Instrumente zur Legitimierung von Datentransfers in Drittländer ohne angemessenen Datenschutz auf dem Prüfstand stehen: Weder die Standardvertragsklauseln der Europäischen Kommission von 2001 für die

238 Umfassend hierzu JB 2013, 2.2

239 Australien und Großbritannien zählen ebenfalls dazu.

Eigenverarbeitung noch die von 2010 für Auftragsdatenverarbeitungen sehen Regelungen vor, die es dem US-Datenimporteur gestatten, sich der Datenanforderung von US-Geheimdiensten ggf. zu widersetzen. Das gilt auch für verbindliche Unternehmensregelungen, die den konzerninternen Datenaustausch weltweit legitimieren können.[240]

Als Reaktion auf das Urteil hat die Europäische Kommission den baldigen Abschluss eines neuen „Safe Harbor-Abkommens 2.0" versprochen, das jedoch schon seit mehr als zwei Jahren mit den USA verhandelt wird. Der EuGH hat dem Prinzip der Selbstverpflichtung keine Absage erteilt, sodass eine solche politische Neuregelung möglich und wünschenswert erscheint. Der für die digitale Wirtschaft zuständige EU-Kommissar hat bereits eine „europäische Cloud für das sichere Speichern von Firmendaten" angekündigt.[241] Ob dies angesichts der erst im Sommer novellierten Geheimdienstgesetze in Frankreich und Großbritannien ausreicht, darf allerdings bezweifelt werden; denn sie räumen den Sicherheitsbehörden die wohl weitreichendsten Befugnisse in der EU ein. Möglicherweise haben deshalb einzelne Konzerne schon die Umstellung auf deutsche Clouds angekündigt. So plant der US-Konzern Microsoft, künftig personenbezogene Daten auf Servern in Deutschland unter Einschaltung eines Treuhänders so zu verarbeiten, dass ein Zugriff von US-Behörden ausgeschlossen ist; zwei neue Rechenzentren würden im zweiten Halbjahr 2016 in Magdeburg und Frankfurt am Main zunächst für Unternehmen und Behörden etabliert.[242] Damit wäre immerhin ein Teil des Datenexportproblems beim Cloud-Produkt „MS Office 365" gelöst.[243] Soweit Unternehmenskunden dieses Produkt allerdings dazu nutzen, um Daten in Drittländer zu exportieren, bleiben sie in der Pflicht, sich von der Gleichwertigkeit des dortigen Datenschutzniveaus zu überzeugen.

240 § 4c Abs. 2 Satz 1 BDSG
241 Die Welt vom 27. Oktober 2015, S. 10: „EU plant Initiative für europäische Datenwolke"
242 Berliner Zeitung vom 12. November 2015, S. 9: „Microsoft entdeckt Datenschutz als Geldquelle"
243 Umfassend hierzu JB 2014, 2.2

14.2 Rahmenabkommen zum transatlantischen Datenverkehr

Nach jahrelangen Verhandlungen hat sich die EU-Kommission mit den USA offenbar über ein Datenschutzrahmenabkommen („Umbrella Agreement“) geeinigt, das für die Kooperation der Strafverfolgungsbehörden gelten soll. Nach Auffassung der EU-Justizkommissarin wird das Abkommen ein hohes Datenschutzniveau für alle personenbezogenen Daten garantieren, die von den Strafverfolgungsbehörden über den Atlantik gesandt werden. Insbesondere werde es garantieren, dass alle Menschen in der EU das Recht haben, den Schutz ihrer Daten bei US-Gerichten durchzusetzen. Voraussetzung für die Unterzeichnung der Vereinbarung sei jedoch, dass der US-Kongress möglichst bald die erforderlichen Gesetzesänderungen („Judicial Redress Bill“) beschließe. Damit würden erstmals Menschen in der EU vor US-Gerichten einklagbare Datenschutzrechte erhalten – im umgekehrten Fall bereits eine Selbstverständlichkeit. Das Bürgerrecht des Einzelnen muss seinen Daten folgen, wenn diese von den empfangenden Behörden nicht datenschutzkonform verarbeitet werden. Ob die „Judicial Redress Bill“ das sicherstellen wird, bleibt abzuwarten. Der zuletzt bekannt gewordene Gesetzentwurf bleibt hinter dem europäischen Schutzniveau zurück.

Die EU-Mitgliedstaaten und das Europäische Parlament müssen das Abkommen ebenfalls billigen, bevor es in Kraft treten kann. Dabei werden sie auch die Feststellung des EuGH zu berücksichtigen haben, dass eine „Regelung, die generell die Speicherung aller personenbezogenen Daten sämtlicher Personen, deren Daten aus der Union in die Vereinigten Staaten übermittelt wurden, gestattet, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme“ vorzunehmen, mit der EU-Grundrechtecharta nicht zu vereinbaren ist.[244]

244 EuGH (Rs. Schrems), a. a. O., Rn. 93

14.3 Wie wird der Datenexport in Drittländer künftig behandelt?

Selten gab es in so kurzer zeitlicher Abfolge so viele Koordinationssitzungen auf nationaler und europäischer Ebene bei den Datenschutzbehörden wie nach der zu Recht als Meilenstein bezeichneten Entscheidung des EuGH zum Safe Harbor-Abkommen. In einem ersten Statement hat die **Art. 29-Datenschutzgruppe** darauf hingewiesen, dass in jedem Fall Übermittlungen, die nach dem EuGH-Urteil auf der Grundlage von Safe Harbor erfolgen, rechtswidrig sind. Sie hat eine Frist bis Ende Januar 2016 gesetzt, innerhalb der die Europäische Kommission ein neues zwischenstaatliches Abkommen mit den USA ausgehandelt haben müsse; auch die anderen Übermittlungsinstrumente wie die Standardvertragsklauseln der Europäischen Kommission sowie die verbindlichen Unternehmensregelungen seien auf mögliche Auswirkungen durch das EuGH-Urteil zu überprüfen. Je nachdem, wie die Ergebnisse hierzu aussähen, seien die EU-Datenschutzbehörden verpflichtet, alle notwendigen und angemessenen Durchsetzungsmaßnahmen möglichst koordiniert zu ergreifen. Die Art. 29-Gruppe geht bis Ende Januar 2016 davon aus, dass die bisherigen Standardvertragsklauseln und verbindlichen Unternehmensregelungen weiter verwendet werden können. Gleichwohl seien die Datenschutzbehörden in Europa nicht gehindert, bestimmte Fälle auf der Grundlage von Beschwerden zu untersuchen. Nach der EuGH-Entscheidung sind sie hierzu sogar verpflichtet.

Die **Konferenz der Datenschutzbeauftragten des Bundes und der Länder** hat ein Positionspapier mit 14 Punkten verfasst.[245] Hervorzuheben ist hierbei insbesondere, dass die Datenschutzbehörden derzeit keine neuen Genehmigungen für Datenübermittlungen in die USA auf Grundlage von verbindlichen Unternehmensregelungen (BCR) oder Datenexportverträgen (also bei abgewandelten Standardverträgen) erteilen. Die Aufsichtsbehörden können sogar von ihrer Befugnis Gebrauch machen, die Datenübermittlung an einen in den USA oder in einem anderen Drittland ohne angemessenes Datenschutzniveau befindlichen Datenempfänger auszusetzen.[246] Das gilt unter zwei Voraussetzungen:

245 Positionspapier vom 21. Oktober 2015, Dokumentenband 2015, S. 38
246 Jeweils Art. 4 der EU-Standardvertragsklauseln von 2001 und 2010

1. Der Datenimporteur ist rechtlich in einem Maß zur Weitergabe der Daten von Unionsbürgern an Behörden seines Staates verpflichtet, das über das in einer demokratischen Gesellschaft erforderliche Maß hinausgeht. Dies ist nach dem EuGH-Urteil auch der Fall, wenn die ausländische Rechtsordnung die Betroffenenrechte gegenüber den Vertragsparteien im Vergleich zur Rechtslage in der Europäischen Union unverhältnismäßig einschränkt oder insoweit den Betroffenen kein gleichwertiger Rechtsschutz im Drittstaat gewährt wird.

2. Diese Weitergabepflichten wirken sich wahrscheinlich sehr nachteilig auf die Garantien aus, die die Standardvertragsklauseln bieten sollen.

Gegen eine Aussetzung könnte z. B. sprechen, dass der Datenexporteur bestimmte technisch-organisatorische Maßnahmen zusichert und umsetzt, die einen unverhältnismäßigen Zugriff von Sicherheitsbehörden praktisch ausschließen. Gleiches gilt, wenn ein weiterentwickelter **Datenexportvertrag** abgeschlossen wird, der zusätzliche Garantien wie effektive Transparenzpflichten beider Vertragsparteien, spürbare Vertragsstrafen für die Unterschreitung europäischen Datenschutzniveaus oder die partielle Verlagerung der Datenverarbeitung nach Europa enthalten sollte. Solche Garantien können auch in Betriebsvereinbarungen für die Übermittlung von Beschäftigtendaten enthalten sein. Diese Faktoren führen jedoch weder im Einzelnen noch in Kombination dazu, dass Aufsichtsbehörden Genehmigungen erteilen müssen. Vielmehr handelt es sich stets um eine Ermessensentscheidung im Einzelfall.

Verbindliche Unternehmensregelungen rechtfertigen ebenfalls keinen Datentransfer in Staaten mit grundrechtswidriger Massenüberwachung. Sie müssen Bestimmungen darüber enthalten, wie die Mitglieder des Konzerns mit Offenlegungsforderungen von Behörden umgehen, die über das in Europa („in einer demokratischen Gesellschaft") als erforderlich anerkannte Maß hinausgehen. Das betrifft insbesondere die Pflicht zur Information der Unternehmenszentrale, wenn die Drittstaatsbehörden auf Geheimhaltung bestehen können (National Security Letters, Gagging Orders). Rechtsschutzmöglichkeiten gegen Geheimhaltungsanordnungen sollte der Datenimporteur ausschöpfen. Zudem sollten Unternehmensregelungen Bestimmungen zu technisch-organisatorischen Maßnahmen wie Verschlüsselung unter Einschaltung von Treuhändern enthalten. Soweit einzelne Datenübermittlungen auf der Grundlage von

BCR genehmigungspflichtig sind, können die Aufsichtsbehörden die Genehmigungen entsprechend der Urteilsgründe des EuGH versagen.[247] Falls solche Übermittlungen nicht als genehmigungsbedürftig angesehen werden, können Datenübermittlungen in unsichere Drittstaaten ggf. nach vorangegangener Anordnung untersagt werden.[248]

Unternehmen, die ihre Datenverarbeitung nicht nach Europa verlagern können, sollten zunächst den Versuch unternehmen, Datenübermittlugen in Drittländer ohne angemessenes Datenschutzniveau auf die **Ausnahmetatbestände des § 4c Abs. 1 BDSG** zu stützen. Sie sind restriktiv und grundrechtskonform auszulegen; die Ausnahme darf nicht zur Regel werden. Das betrifft auch die Einwilligung. Sie scheidet als Rechtsgrundlage für massenhafte, wiederholte oder routinemäßige Datenübermittlungen aus praktischen Gründen in der Regel aus, weil die Einwilligung eindeutig sein muss und jederzeit widerruflich ist. Unter welchen engen Bedingungen Einwilligungen Datenübermittlungen in Drittstaaten ohne gleichwertiges Datenschutzniveau rechtfertigen können, muss noch festgelegt werden. So wäre daran zu denken, dass sowohl die Einwilligung als auch andere Ausnahmetatbestände (z. B. zur Wahrung lebenswichtiger Interessen der Betroffenen) unter bestimmten Voraussetzungen Datenübermittlungen legitimieren können, wenn der Wesensgehalt von Grundrechten [249] und die Menschenwürde nicht verletzt werden. Bei einer Abwägung sind die Interessen der Betroffenen an der Datenübermittlung in das Drittland zu berücksichtigen. Soweit unter diesen Voraussetzungen die Einwilligung eine tragfähige Rechtsgrundlage für eine Datenübermittlung sein kann, muss die betroffene Person vorab hinreichend deutlich darüber aufgeklärt werden, dass in einem bestimmten Drittstaat kein gleichwertiges Datenschutzniveau herrscht.

Wir werden auf international agierende Unternehmen in unserem Zuständigkeitsbereich zugehen und mindestens in Bezug auf die USA um Darlegung bitten, wie Datenübermittlungen dorthin vor dem Hintergrund des EuGH-Urteils legitimiert werden. Falls keine hinreichende Rechtsgrundlage genannt wird, werden wir von unseren Durchsetzungsbefugnissen nach dem BDSG Gebrauch machen: Ordnungswidrigkeiten können wir mit einer Geldbuße von

247 § 4c Abs. 2 BDSG
248 § 38 Abs. 5 BDSG
249 Im Wesensgehalt der Grundrechte sieht der EuGH eine Grenze der Datenverarbeitung auch im Drittland, siehe EuGH (Rs. Schrems), a. a. O., Rn. 94 f.

bis zu 300.000 € pro Datenschutzverstoß ahnden.[250] Im Übrigen können wir Beseitigungsanordnungen und Untersagungsverfügungen erlassen.[251]

Die Rechtsprechung des EuGH hat den Datenschutz in Europa wesentlich gestärkt. Die Datenschutzbehörden haben jetzt die Aufgabe, insbesondere beim Datenexport in Drittstaaten sicherzustellen, dass Unionsbürgerinnen und -bürger im Zielland einen gleichwertigen Schutz genießen.

250 § 43 Abs. 2 Nr. 1 i.V. m. Abs. 3 Satz 1, 2. Hbs. BDSG
251 § 38 Abs. 5 Satz 1 und 2 BDSG

13 Aus der Arbeit der Sanktionsstelle

13.1 Entwicklung von Anordnungen

Im Berichtszeitraum haben wir verstärkt das gesetzlich vorgeschriebene Mittel der Anordnung eingesetzt. In zwei Fällen forderten wir die verantwortlichen Stellen auf, unsere Fragen zu Datenerhebungen und -verarbeitungen unter Androhung von Zwangsgeldern zu beantworten (sog. Heranziehungsbescheide).[209]

In einem dritten Fall haben wir bei einem Unternehmen aufgrund zahlreicher Beschwerden ein Anordnungsverfahren eingeleitet, weil die Erhebung, Verarbeitung und Nutzung von E-Mail-Adressen zu Werbezwecken ohne Rechtsgrundlage vorgenommen werden. Auf der Internetseite des Unternehmens können Interessentinnen und Interessenten ihr Auto vom Unternehmen kostenlos und nach Angaben des Unternehmens „ohne Anmeldung“ bewerten und sich den durchschnittlichen Marktwert zur Orientierung anzeigen lassen. Neben Angaben zum Fahrzeug müssen sie ihre E-Mail-Adresse in eine Eingabemaske eingeben. Ein Double-Opt-In-Verfahren, bei dem die tatsächliche Inhaberin bzw. der tatsächliche Inhaber der E-Mail-Adresse bestätigt, dass die Angaben zum Fahrzeug und zur E-Mail-Adresse von ihr oder ihm stammen, setzt das Unternehmen nicht ein. Die E-Mail-Adresse nutzt das Unternehmen, um die Betroffenen daran zu erinnern, dass es an einem Ankauf des bewerteten Gebrauchtwagens interessiert ist. Da diese Erinnerungsmails als Werbung einzustufen sind, bedarf es hierfür einer Einwilligung der Betroffenen. Die über die allgemeinen Geschäftsbedingungen eingeholte Einwilligungserklärung entspricht jedoch nicht den gesetzlichen Vorgaben[210]. Sollte das Unternehmen unseren Forderungen nicht nachkommen, werden wir eine Anordnung erlassen.[211]

209 § 38 Abs. 3 Satz 1 BDSG
210 § 4a BDSG
211 § 38 Abs. 5 BDSG

Die Erfahrungen zeigen, dass bereits nach einer Anhörung, in der wir detailliert unsere rechtliche Bewertung darlegen, die Unternehmen ihre Position überdenken. So wurden bei einer Videoüberwachungsanlage an einem Wohngebäude in der Nähe des Görlitzer Parks, mit der die aufgenommenen Bilder direkt per Live-Stream ins Internet eingestellt worden waren, die Videokamera und der Live-Stream nach Einleitung des Anordnungsverfahrens abgeschaltet.

13.2 Keine Telefonwerbung unter dem Vorwand der Zufriedenheitsabfrage

2012 haben wir der Axel Springer SE mit einer Anordnung untersagt, telefonische Zufriedenheitsabfragen zur Qualität des Zustellservices bei ihren Zeitungsabonnentinnen und -abonnenten dazu zu nutzen, von den Angerufenen eine Einwilligung in Werbung per Telefon, E-Mail oder SMS zu anderen Angeboten des Verlagshauses zu erhalten, soweit die Betroffenen nicht bereits bei Abschluss der Abonnements in die Nutzung ihrer Telefonnummern zu diesen Zwecken eingewilligt hatten.[212]

Nachdem das Unternehmen erfolglos vor dem Verwaltungsgericht gegen diese Anordnung geklagt hatte,[213] beantragte es die Zulassung der Berufung gegen das klageabweisende Urteil. Das Oberverwaltungsgericht Berlin-Brandenburg lehnte diesen Antrag mangels Zulassungsgründen mit einem unanfechtbaren Beschluss ab.[214] Es bestätigte unseren Standpunkt, dass der Begriff der Werbung sowohl die unmittelbare als auch die mittelbare Absatzförderung erfasst und somit bereits die Frage nach einer Einwilligung in Werbung eine werbende Maßnahme darstellt. Das Gericht stellte zudem nochmals klar, dass die Nutzung der Telefonnummern der Abonnenten zu unerwünschten Werbezwecken nicht dadurch gerechtfertigt ist, dass mit dem Telefonat auch ein datenschutzrechtlich zulässiger Zweck – die Zufriedenheitsabfrage hinsichtlich der Vertragsleistungen – verfolgt wird, da die Daten von vornherein in zweifacher Hinsicht genutzt werden.

212 JB 2012, 13.6
213 JB 2014, 10.2
214 Beschluss vom 31. Juli 2015, OVG 12 N 71.14

Werbeanrufe sind nur mit vorheriger Einwilligung der Betroffenen erlaubt. Telefonnummern, die ein Unternehmen zur Abwicklung von vertraglichen Pflichten von Betroffenen erhalten hat, dürfen nicht zu Werbezwecken genutzt werden.

13.3 Entwicklung von Ordnungswidrigkeitenverfahren

Insgesamt haben wir 37 Bußgeld- oder Verwarnungsbescheide erlassen und Geldbußen von insgesamt 40.685 € festgesetzt.[215] In 22 Fällen haben wir einen Strafantrag gestellt.[216]

Wir haben festgestellt, dass wir mit der letzten Änderung der Verordnung über sachliche Zuständigkeiten für die Verfolgung und Ahndung von Ordnungswidrigkeiten (ZuStVO-OWiG)[217] nicht mehr für die Verfolgung von datenschutzrechtlichen Verstößen nach dem Telemediengesetz zuständig sind. Dies obliegt nunmehr den Bezirksämtern. Eine Nachfrage bei der Senatsverwaltung für Inneres und Sport ergab, dass diese Änderung der Zuständigkeit unbeabsichtigt war. Mit der nächsten Änderung der Verordnung soll unsere Zuständigkeit wiederhergestellt werden. Für Verstöße gegen die Impressumspflicht von Rundfunkanstalten bleibt die Medienanstalt Berlin-Brandenburg zuständig.[218]

13.4 Beispiele

Mit einer Änderung des Ordnungswidrigkeitengesetzes (OWiG) im Jahr 2013 wurde eine Rechtsgrundlage für die Festsetzung von Geldbußen gegen Rechtsnachfolger von juristischen Personen geschaffen. Im Falle von **Unternehmensfusionen** konnten Bußgelder bisher nur unter engen, von der Rechtsprechung entwickelten Voraussetzungen gegen das übernehmende Unternehmen verhängt werden. Diese Lücke konnten insbesondere konzerngebundene

215 § 43 Abs. 3 BDSG
216 § 44 Abs. 2 BDSG, § 32 Abs. 3 BlnDSG
217 § 1 Nr. 1d ZuStVO-OWiG
218 §§ 55, 49 Abs. 1 Satz 2 Nr. 13 i.V. m. § 49 Abs. 3 Rundfunkstaatsvertrag

Unternehmen in der Vergangenheit nutzen, um durch kurzfristige Unternehmensumwandlungen die Ahndung betriebsbezogener Ordnungswidrigkeiten gegen sie zu umgehen. Die neue Regelung im OWiG[219] ermöglicht es nun in vielen Fällen, eine Geldbuße auch gegen das übernehmende Unternehmen (den Rechtsnachfolger) festzusetzen. Die Buße darf den Wert des übernommenen Vermögens sowie die Höhe der gegenüber dem Rechtsvorgänger angemessenen Geldbuße nicht übersteigen. Wir haben nun erstmals von dieser neuen Regelung Gebrauch gemacht. Ein Unternehmen aus dem Bereich Adresshandel, dessen Geschäftsführer eine betriebsbezogene datenschutzrechtliche Ordnungswidrigkeit[220] begangen hatte, war im Verlauf des eingeleiteten Bußgeldverfahrens mit einem anderen Unternehmen verschmolzen. Der gegen den Rechtsnachfolger festgesetzte Bußgeldbescheid wurde rechtskräftig.

In zwei Fällen haben wir Bußgelder gegen Unternehmen festgesetzt, die ihrer **Meldepflicht**[221] nicht nachgekommen waren (§ 43 Abs. 1 Nr. 1 BDSG). Diese Pflicht dient einer präventiven Kontrolle für risikoträchtige Datenverarbeitungsvorgänge. Durch diese Vorschrift erhalten wir frühzeitig Kenntnis von per Gesetz als besonders riskant eingestuften Verfahren, um bei Bedarf die Einhaltung datenschutzrechtlicher Anforderungen noch vor Inbetriebnahme solcher Verfahren zu überprüfen und ggf. durchzusetzen. Bei beiden Unternehmen handelte es sich um Betreiber von **Online-Branchenportalen**. Auf solchen Seiten werden regelmäßig nicht nur die Daten von juristischen Personen, sondern auch solche von Gewerbetreibenden und Freiberuflern verarbeitet, auf die das BDSG anzuwenden ist.

Gegen einen dieser Betreiber setzten wir weitere Bußgelder fest, weil das Unternehmen bei der schriftlichen Kundenakquise in einer Vielzahl von Fällen keine **Werbewiderspruchshinweise** in die Schreiben aufgenommen hatte.[222] Es hatte Gewerbetreibende und Freiberufler massenhaft schriftlich aufgefordert, ihre beruflichen Daten in ein behördlich erscheinendes Formular einzutragen, damit diese in ihr Branchenportal aufgenommen würden. Das Unternehmen hatte die Werbewiderspruchshinweise offenbar absichtlich nicht in die Schreiben aufgenommen, um der „Abo-Falle“ größtmögliche Wirkung zu verleihen.

219 § 30 Abs. 2a OWiG
220 § 43 Abs. 1 Nr. 1 BDSG
221 § 4d Abs. 1 BDSG
222 § 43 Abs. 1 Nr. 3 BDSG

Lediglich dem „Kleingedruckten“ war zu entnehmen, dass es sich um ein entgeltliches Vertragsangebot mit einer Laufzeit von zwei Jahren handelte.

Ein vierstelliges Bußgeld setzten wir gegen einen Arbeitgeber fest, der bei einer Auskunftei eine **Bonitätsabfrage** für eine Bewerberin eingeholt hatte.[223] Diese beschwerte sich bei uns, weil ein von ihr gestelltes Selbstauskunftsersuchen bei einer großen Auskunftei zu der Information führte, dass ihr ehemaliger Arbeitgeber eine Abfrage zu ihrer Person getätigt hatte. Auf unsere Nachfrage gab das Unternehmen zunächst an, die Abfrage sei erfolgt, weil die Petentin als vormalige Kundin des Unternehmens mehrere Produkte auf Rechnung gekauft hätte. Dieser Vorwand war auch gegenüber der Auskunftei genutzt worden, um die Datenübermittlung zu erschleichen. Tatsächlich konnte das Unternehmen jedoch keine Rechnungskäufe der Petentin nachweisen. Darüber hinaus war die Abfrage nur einen Tag, nachdem die Petentin ein Bewerbungsgespräch bei dem Unternehmen absolviert hatte, erfolgt, was den Schluss nahelegte, dass die Abfrage mit der Bewerbung in Zusammenhang stand. Aus einer Zeugenbefragung ergab sich im Verlauf der Ermittlungen, dass das Unternehmen im Bewerbungsprozess regelmäßig Bonitätsauskünfte eingeholt hatte.[224]

Ein weiteres Bußgeld setzten wir gegen einen Verantwortlichen einer Internetplattform fest, der unsere Auskunftsersuchen nicht beantwortet hatte.[225] Obwohl der Betroffene im Impressum der Internetseite aufgeführt war, hatte er vorgetragen, nicht im datenschutzrechtlichen Sinne für die Seite verantwortlich zu sein. Er legte dar, die Seite werde von einer Reihe ehrenamtlicher Redakteure betrieben. Er habe lediglich eine koordinierende Funktion und könne keinen Einfluss auf die Inhalte – und damit auf die Verarbeitung personenbezogener Daten – nehmen. Diese Argumentation untermauerte er mit dem Hinweis, er sei beim deutschen Domainverwalter DENIC nur als sog. Admin-C und nicht als Domainbetreiber registriert. Das Amtsgericht Tiergarten bestätigte im Einspruchsverfahren unsere Rechtsauffassung, dass die Angaben im Impressum aufgrund der gesetzlichen **Impressumspflicht**[226] für eine Aufsichtsbehörde maßgeblich und Daten der DENIC nachrangig heranzuziehen sind. Datenschutzrechtliche Verantwortlichkeiten können nicht durch die

223 § 43 Abs. 2 Nr. 4 BDSG
224 Siehe 9.1
225 § 43 Abs. 1 Nr. 10 BDSG
226 § 5 TMG

Angabe Dritter im Impressum „verwischt“ werden. Zudem kann die verantwortliche Stelle im datenschutzrechtlichen Sinne aus mehreren Personen bestehen.[227] Diese können gleichrangig von der Aufsichtsbehörde zur Erteilung von Auskünften herangezogen werden.[228]

Gegen ein Verlagsunternehmen setzten wir zwei vierstellige Bußgelder fest, weil es Kunden mehrfach und in hartnäckiger Weise postalisch beworben hatte, obwohl sie der Nutzung ihrer Daten für Werbezwecke widersprochen hatten.[229] In einem Fall hatte das Unternehmen vorgebracht, dass der **Werbewiderspruch** zwar bearbeitet worden sei, jedoch aufgrund einer Namensdopplung im Kundenstamm und damit verbundener technischer Mängel im System nicht richtig umgesetzt wurde. In einem anderen Fall wären die Daten bereits für eine Werbeaktion mit längerem Vorlauf an ein anderes Unternehmen vermietet worden, weshalb die Datennutzung nicht mehr rechtzeitig gestoppt werden konnte. Diese Vorwände veranlassten uns nicht, von der Verhängung des Bußgelds abzusehen. Insbesondere rechtfertigt die Tatsache, dass großangelegte Marketingaktionen einen langen Planungsvorlauf haben, nicht, dass Daten noch Monate nach Eingang des Widerspruchs für Werbezwecke genutzt werden. Unternehmen haben vielmehr alle erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um sicherzustellen, dass Werbewidersprüche unverzüglich umgesetzt werden.[230]

Die datenschutzrechtlichen Vorgaben sind zu beachten. Bei Verstößen stellen wir Strafanträge oder verhängen Bußgelder.

227 § 3 Abs. 7 BDSG
228 Siehe 11.8.2
229 § 43 Abs. 2 Nr. 5b BDSG
230 § 9 BDSG

15 Telekommunikation und Medien

15.1 Datenschutz bei Smart-TV/HbbTV

15.1.1 Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste

Der Düsseldorfer Kreis hat eine Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste verabschiedet.[252] Sie gibt einen Überblick über die Bewertung der jeweiligen Angebote durch die Aufsichtsbehörden und richtet sich an Anbieter von Smart-TV-Diensten und -Produkten. Hierzu zählen insbesondere Gerätehersteller, Portalbetreiber, App-Anbieter und Anbieter von HbbTV[253]-Angeboten.

In der Orientierungshilfe bewerten die Aufsichtsbehörden insbesondere die von Rundfunkveranstaltern bei HbbTV-Angeboten geübte Praxis, über eine mit dem Rundfunksignal versandte URL bereits bei der Auswahl eines Senders unmittelbar und ohne weiteres Zutun der Nutzenden eine Internetverbindung zu dem Server des HbbTV-Anbieters auszulösen. Dabei verwendet der Anbieter zumindest die IP-Adresse der Betroffenen als personenbezogenes Datum, ohne dass für diesen datenverarbeitenden Schritt eine Rechtsgrundlage erkennbar ist.

Der Aufruf der Web-Dienste im Rahmen von HbbTV und die damit einhergehende wechselseitige Kommunikation mit dem Anbieter darf erst dann stattfinden, wenn dies durch die Nutzenden selbst initiiert wird. Dies kann z. B. durch die aktive Entscheidung erfolgen, den „Red-Button“ bei HbbTV zu betätigen und damit den Abruf eines Telemediendienstes bewusst zu veranlassen.

252 Stand: September 2015, abrufbar unter http://www.datenschutz-berlin.de/attachment/1153/2015-Orientierungshilfe_SmartTV.pdf

253 Hybrid broadcast broadband TV, ein dem jeweiligen TV-Sender zugeordnetes Internetangebot, das über internetfähige Fernsehgeräte („Smart-TV“) abgerufen werden kann.

Das Einschalten eines bestimmten Programms allein stellt dagegen keine bewusste Inanspruchnahme von Telemedien dar. Auch das bloße Verbinden des Gerätes mit dem Internet kann – anders als von einigen Anbietern propagiert – nicht als Einwilligung verstanden werden, schon weil es dabei an der notwendigen Bestimmtheit fehlt: Eine solche „Einwilligung" würde ansonsten alle Telemediendienste des Herstellers, der Portale und Empfehlungsdienste, aller potenziell empfangbaren Fernsehsender sowie aller installierbaren Apps umfassen.

Bei den im Vorfeld der Verabschiedung der Orientierungshilfe mit verschiedenen Rundfunkanbietern geführten Gespräche hat sich herausgestellt, dass dort die Umgestaltung der bereits im Betrieb befindlichen HbbTV-Dienste auf eine datenschutzkonforme Lösung auf erhebliche Schwierigkeiten stößt, die teilweise von den Rundfunkanbietern allein nicht behoben werden können.

Die Aufsichtsbehörden erwarten von den Rundfunkanbietern, dass sie die Hindernisse, die in ihrem eigenen Verantwortungsbereich liegen, beseitigen. Darüber hinaus werden die Rundfunkanbieter aufgefordert, auf die übrigen beteiligten Instanzen (z. B. Standardisierungsgremien, Anbieter von Übertragungswegen und Gerätehersteller) einzuwirken, damit diese ihrerseits die notwendigen Voraussetzungen schaffen, um den Aufbau einer Internetverbindung vor Inanspruchnahme des interaktiven Teils eines HbbTV-Angebots zukünftig zu unterbinden und damit die Möglichkeit zum anonymen Fernsehen zu erhalten.

Für eine Übergangszeit ist ein beanstandungsfreier Betrieb von bestehenden HbbTV-Angeboten möglich, wenn dabei folgende Mindestanforderungen erfüllt werden:

- Vor dem Drücken des „Red-Button" im Zusammenhang mit dem Einschalten eines HbbTV-Senders übertragene Nutzungsdaten werden nicht für Nutzungsprofile verwendet.
- Nach dem Drücken des „Red-Button" werden den Nutzenden leicht zugängliche, allgemeinverständliche Informationen über die Verarbeitung ihrer Nutzungsdaten zur Verfügung gestellt, in deren Rahmen sie auch über ihr Widerspruchsrecht gegen die Erstellung von Nutzungsprofilen informiert werden.

- Die Bildung von Nutzungsprofilen nach § 15 Abs. 3 Telemediengesetz (TMG) erfolgt frühestens nach einer Interaktion der Nutzenden mit dem interaktiven Teil des HbbTV-Angebots (Drücken des „Red-Button“).
- Nutzende können der Profilbildung, wie in § 15 Abs. 3 TMG vorgesehen, in einfacher Form widersprechen. Durch Nutzende erklärte Widersprüche werden von den Anbietern unverzüglich umgesetzt.

15.1.2 Verarbeitung von Nutzungsdaten bei HbbTV-Angeboten durch den Rundfunk Berlin-Brandenburg

Der Rundfunk Berlin-Brandenburg (rbb) betreibt in Potsdam-Babelsberg ein „Playout-Center“, über das das gesamte digitale Angebot der ARD technisch abgewickelt wird. In diesem „Playout-Center“ laufen auch die bei der Nutzung der HbbTV-Angebote aller ARD-Sender anfallenden Nutzungsdaten auf.

Die gegenwärtige Praxis des rbb bei der Ausstrahlung von HbbTV-Angeboten ermöglicht keine vollständig anonyme Nutzung dieser Angebote, wenn das Smart-TV-Gerät mit dem Internet verbunden ist. Vielmehr wird – wie oben beschrieben[254] – bereits bei der Anwahl des Senders durch die mit dem Sendesignal übertragene URL eine Verbindung über das Internet zu den entsprechenden Servern des „Playout-Centers“ aufgebaut. Dabei werden Nutzungsdaten (insbesondere die IP-Adresse) an diesen Server übertragen. Die darauffolgende Verarbeitung dieser Nutzungsdaten entspricht den oben dargestellten Mindestanforderungen. Auch die Art der Verwendung von Cookies für die „Startleiste“[255] entspricht den Angaben in der Datenschutzerklärung. Davon haben wir uns im Rahmen einer technischen Überprüfung überzeugen können.

Reichweitenmessungen erfolgen sowohl im Zusammenhang mit der Nutzung der Startleiste als auch mit der Nutzung der interaktiven Angebote der einzelnen ARD-Sender. Wenig nutzerfreundlich ist die Tatsache, dass Widersprüche gegen diese verschiedenen Verfahren jeweils getrennt erklärt werden müssen.

254 Siehe 15.1.1

255 Die nach dem Drücken des „Red-Button“ am unteren Bildschirmrand eingeblendete Startleiste enthält Informationen zum laufenden Programm und Links zu anderen Online-Angeboten des jeweiligen Senders.

Ein Widerspruch gegen eine Reichweitenmessung führt dazu, dass künftig ein Tracking durch das jeweilige (Teil-)Verfahren unterbleibt.

Die gegenwärtige Praxis des rbb und der übrigen in der ARD zusammengeschlossenen Senderanstalten hat zur Folge, dass ein technisch anonymes Fernsehen auch für diejenigen Nutzerinnen und Nutzer unmöglich wird, die den interaktiven Teil der Angebote gar nicht nutzen. Diese Situation ist unbefriedigend. Bereits 2014 hatten der Düsseldorfer Kreis und die Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten in einer gemeinsamen Position gefordert, die anonyme Nutzung von Fernsehangeboten auch bei Smart-TV-Nutzung zu gewährleisten.[256]

Gerade die öffentlich-rechtlichen Rundfunkanstalten, die aus den Gebührenbeiträgen der Bürgerinnen und Bürger finanziert werden, sollten bei der datenarmen Gestaltung ihrer elektronischen Dienste mit gutem Beispiel vorangehen. Wir erwarten, dass rbb und ARD weitere Verbesserungen vornehmen, die eine anonyme Nutzung ihrer HbbTV-Angebote jedenfalls denjenigen ermöglichen, die ihr Smart-TV-Gerät nur „normal“ ohne den interaktiven Teil des HbbTV-Angebots nutzen.

Viele HbbTV-Angebote ermöglichen derzeit keine technisch anonyme Nutzung auch in den Fällen, in denen auf den interaktiven Teil des HbbTV-Angebots nicht zugegriffen wird. Die Rundfunkanbieter bleiben aufgefordert, hier für Abhilfe zu sorgen. Wer gegenwärtig die Angebote mit einem Smart-TV-Gerät vollständig anonym nutzen möchte, muss entweder am Gerät HbbTV deaktivieren oder darf das Gerät nicht mit dem Internet verbinden.

15.2 Datenschutz bei „Wearable Computing“

Bei „Wearable Computing“ handelt es sich um Informationstechnologie, die klein genug ist, um am Körper der Nutzerin oder des Nutzers getragen zu werden. Diese Geräte enthalten meist Sensoren, die laufend Informationen

256 „Smartes Fernsehen nur mit smartem Datenschutz“ vom 20. Mai 2014, Dokumentenband 2014, S. 49; siehe auch JB 2014, 13.1

über den Körper der Betroffenen (Stimmung, Gewohnheiten, körperliche Aktivitäten, Gesundheitszustand, Geschwindigkeit, Mobilität) und/oder über die Umgebung (Bilder, Geräusche, Temperatur, Feuchtigkeit, Aufenthaltsort, soziale Umgebung) erfassen und in verschiedener Weise weiterverarbeiten.

Viele „Wearables" enthalten eine Kamera. Die Kamerafunktion wurde bereits in den letzten Jahren kritisiert wegen der technischen Möglichkeit, permanent und heimlich Bilder von Personen aufzuzeichnen.

Darüber hinaus ist die Nutzung der Geräte vielfach mit der Verpflichtung verbunden, mit dem Hersteller der Hardware, des mobilen Betriebssystems oder mit Anbietern von Cloud-Diensten Verbindung aufzunehmen. Eine lokale Speicherung nur auf dem Endgerät des Nutzers ist häufig nicht möglich. Dieser Zwang zur Vernetzung kann dazu führen, dass die Betroffenen die Kontrolle über die gesammelten personenbezogenen Daten verlieren und die Fitnessbänder und Wearables wie elektronische Fesseln wirken.

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (sog. Berlin Group) hat unter unserem Vorsitz eine Reihe von Empfehlungen zum Schutz der Privatsphäre beim Einsatz von „Wearable Computing"-Technologien verabschiedet.[257] Dabei fordert die Arbeitsgruppe in erster Linie, eine größtmögliche Transparenz der Datenverarbeitung für die Nutzenden zu gewährleisten. Als Grundeinstellung sollten personenbezogene Daten zudem unter der Kontrolle der Person verarbeitet werden, die das Gerät trägt. Es sollte keine Verpflichtung zur Herstellung einer Verbindung mit den Servern der Hard- oder Software-Hersteller, zu Plattformen oder Cloud-Diensteanbietern geben.

Der Trend zu „Wearable Computing" führt zu neuen datenschutzrechtlichen Herausforderungen. Häufig fehlt es an ausreichender Transparenz sowohl für die Nutzenden als auch für Dritte. Zudem führt der verbreitete Zwang zur Vernetzung zum Verlust der Kontrolle über die eigenen Daten. Fitnessbänder und andere tragbare Geräte können – wenn sie nicht datenschutzgerecht gestaltet werden – wie elektronische Fesseln wirken.

257 Arbeitspapier zum Datenschutz bei tragbaren Endgeräten („Wearables") vom 27./28. April 2015, Dokumentenband 2015, S. 79

15.3 Reichweitenmessung im Internet

Viele Anbieter von Telemedien setzen auf ihren Webseiten Verfahren zur Reichweitenmessung ein, um sich darüber zu informieren, wie ihre Angebote genutzt werden. Eine solche Messung ist grundsätzlich möglich, solange die in § 15 Abs. 3 TMG genannten Bedingungen eingehalten werden. Dazu gehören insbesondere

- die Informationen der Betroffenen im Rahmen der Unterrichtung nach § 13 Abs. 1 TMG – diese kann z. B. in der Datenschutzerklärung erfolgen,
- der Hinweis auf das gesetzlich festgelegte Widerspruchsrecht der Betroffenen gegen eine Reichweitenmessung,
- die Umsetzung der von den Betroffenen erklärten Widersprüche (dies erfolgt je nach eingesetztem Produkt entweder durch den Einsatz von Cookies oder von Plugins für die verwendeten Browser) und
- die Beachtung des Verbots der Zusammenführung der unter Pseudonym gespeicherten Profildaten mit Daten über den Träger des Pseudonyms.[258]

Insbesondere ist zu beachten, dass die IP-Adresse kein Pseudonym im Sinne des Telemediengesetzes ist. Sie darf daher für Zwecke der Reichweitenmessung nicht dauerhaft gespeichert werden und ist nach Ende der Verbindung unverzüglich wirksam zu anonymisieren bzw. zu löschen.

Wir haben aufgrund von Eingaben oder im Rahmen von Überprüfungen von Amts wegen den Einsatz von Reichweitenmessungsverfahren bei über 50 Anbietern von Telemedien überprüft. Diese Anbieter setzten bis auf wenige Ausnahmen das von der Google Ireland Ltd. im Wege der Auftragsdatenverarbeitung angebotene Produkt „Google Analytics“ ein. Über die vor dem Einsatz von Google Analytics notwendigen Maßnahmen haben wir bereits 2011 ausführlich berichtet.[259] Bei unseren Überprüfungen haben wir in zahlreichen Fällen Mängel festgestellt. Zu den gravierendsten zählte die Verwendung des Produkts ohne die vorgeschriebene Kürzung der IP-Adresse. Diese ist in dem von

258 Ein Verstoß gegen diese Bestimmung kann nach § 16 Abs. 2 Nr. 5, Abs. 3 TMG mit einer Geldbuße bis zu 50.000 € geahndet werden.

259 JB 2011, 12.2

Google standardmäßig angebotenen JavaScript-Code nicht enthalten, sondern muss durch den Anwender „nachgerüstet" werden. In einigen Fällen haben wir den Einsatz von Google Analytics auf Webseiten angetroffen, deren Datenschutzerklärung überhaupt keine Hinweise dazu enthielt. In diesen Fällen war es den Betroffenen auch nicht möglich, ihr Widerspruchsrecht aus § 15 Abs. 3 TMG auszuüben.

Wir haben die Anbieter zur Behebung der Mängel aufgefordert und werden uns in einer angemessenen Frist davon überzeugen, ob die erforderlichen Änderungen in den Angeboten vorgenommen worden sind. Soweit dies nicht der Fall ist, werden wir die Einleitung aufsichtsbehördlicher Maßnahmen prüfen.

Zu den erforderlichen Maßnahmen zum datenschutzkonformen Einsatz von Google Analytics haben wir ein Merkblatt mit Hinweisen für Telemedienanbieter, die das Produkt einsetzen, veröffentlicht.[260]

Bei der Auftragsdatenverarbeitung durch die Google Ireland Ltd. bedient sich diese der technischen Einrichtungen der in den USA ansässigen Muttergesellschaft Google Inc. Diese Einbeziehung war bisher unter den Bedingungen des Safe Harbor-Abkommens mit den USA möglich. Nach der hierzu ergangenen Entscheidung des EuGH[261] muss auch der Einsatz von Google Analytics auf eine neue Rechtsgrundlage gestellt werden.

Beim Einsatz von Reichweitenmessungsverfahren müssen Angebote Dritter u. U. an die Bestimmungen des in Deutschland geltenden Rechts angepasst werden. Die Verantwortung dafür trägt der Anbieter des jeweiligen Telemediums.

15.4 Änderung des Rundfunkbeitragsstaatsvertrages

Das Finanzierungssystem des öffentlich-rechtlichen Rundfunks ist vor drei Jahren grundlegend umgestellt worden. Wurden zuvor Gebühren gerätebe-

260 http://www.datenschutz-berlin.de/attachments/1159/2015-Hinweise_Google_Analytics.pdf
261 Siehe 14.1

zogen erhoben, dienen seit 2013 Raumeinheiten, d. h. die Wohnung, die Betriebsstätte und das Kfz, als Anknüpfungspunkte für die Erhebung des Rundfunkbeitrags.[262] Die mit der Reform beschlossene Evaluierung der neuen Rundfunkfinanzierung hatte zur Folge, dass der Rundfunkbeitragsstaatsvertrag geändert werden soll, u.a. um einen weiteren vollständigen Meldedatenabgleich zu ermöglichen.

Für den Datenschutz hatte die Umstellung des Finanzierungssystems Folgen: Die Adressdaten aller gemeldeten Volljährigen wurden durch die Meldestellen an den Beitragsservice übermittelt. Dieser sog. Meldedatenabgleich wurde von den Datenschutzbeauftragten des Bundes und der Länder kritisch gesehen.[263] Ihre Bedenken konnten – wenn überhaupt – nur deshalb zurückgestellt werden, weil im Rundfunkbeitragsstaatsvertrag explizit geregelt wurde, dass es sich um einen einmaligen Abgleich handeln soll.[264] Demgegenüber sieht die Neufassung des Staatsvertrags einen „weiteren Abgleich" der Meldedaten vor und stößt damit auf tiefgreifende verfassungsrechtliche Bedenken. Durch die Datenübermittlung „auf Vorrat" wird in das Grundrecht auf informationelle Selbstbestimmung nicht nur geringfügig eingegriffen. Dieser Eingriff kann nicht beliebig wiederholt werden. Die Rundfunkanstalten haben nicht überzeugend dargelegt, warum eine Wiederholung des vollständigen Meldedatenabgleichs erforderlich ist. Sie haben zudem die Möglichkeit, anlassbezogen Meldedaten anzufordern. Damit bestehen ausreichende Mechanismen, die Aktualität des Datenbestandes des Beitragsservice zu überprüfen, ohne dass es eines regelmäßigen Totalabgleichs bedarf.

Entgegen unserer Empfehlung hat der Regierende Bürgermeister dem Änderungsentwurf zwischenzeitlich zugestimmt. Geplant ist, dass der 19. Rundfunkänderungsstaatsvertrag in den einzelnen Bundesländern 2016 ratifiziert und im Oktober bzw. Januar 2017 in Kraft tritt. Es bleibt zu hoffen, dass die Landesparlamente die Kritik der Datenschutzbeauftragten ernst nehmen und die Änderungen des Rundfunkbeitragsstaatsvertrages nur verabschieden, wenn auf den erneuten Meldedatenabgleich verzichtet wird.

262 JB 2010, 13.4

263 Siehe Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2010: Rundfunkfinanzierung: Systemwechsel nutzen für mehr statt weniger Datenschutz!, Dokumentenband 2010, S. 17

264 Bayerischer VerfGH, Urteil vom 15. Mai 2014, Vf. 8-VII-12, Vf. 24-VII-12

Mit der Änderung des Rundfunkbeitragsstaatsvertrags wird der Weg geebnet, den einmaligen Totalabgleich mit den Meldedaten aller meldepflichtigen Personen in Deutschland zu einem regelmäßigen Verfahren auszubauen. Damit würde beim Beitragsservice ein zentrales „Schattenmelderegister" entstehen, das mit dem Recht der Betroffenen auf informationelle Selbstbestimmung nicht zu vereinbaren ist.

15.5 Internet Sweep Day 2015

Wie in den vergangenen Jahren haben wir uns am **Internet Sweep Day 2015** beteiligt. Die international koordinierte Datenschutzprüfung befasste sich diesmal mit an Kinder und Jugendliche gerichtete bzw. vorwiegend von Jugendlichen genutzten Webangeboten und Apps. Hierbei wurde insbesondere überprüft, ob umfassend und in altersgerechter Sprache über die Verarbeitung personenbezogener Daten informiert wird und ob unnötige Daten z. B. für Werbezwecke erhoben werden. An der Prüfung beteiligten sich weltweit 29 Aufsichtsbehörden. Von den geprüften 1494 Angeboten gaben 41 % Grund zur Beanstandung, häufig weil Daten an Dritte weitergegeben wurden. Die geprüften Berliner Angebote konnten sich im internationalen Vergleich behaupten: 80 % waren im Rahmen des Prüfumfanges beanstandungsfrei. Bei einzelnen Angeboten war insbesondere die Abfrage des genauen Geburtsdatums, bei Gewinnspielen auch der Postadresse zu hinterfragen. Für eine Altersfeststellung genügt z. B. das Geburtsjahr, die Postadresse muss nur von den Gewinnern erfragt werden.

Die geprüften Berliner Angebote konnten sich im internationalen Vergleich durchaus sehen lassen.

15.6 Aus der Arbeit der „Berlin Group"

Die internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (sog. Berlin Group) hat unter unserem Vorsitz in ihren Sitzungen am 27.-28. April in Seoul (Republik Korea) und am 13.-14. Oktober in Berlin vier Arbeitspapiere verabschiedet:

Neben dem **Arbeitspapier zum Datenschutz bei tragbaren Endgeräten („Wearables“)**[265] hat die Arbeitsgruppe in dem **Arbeitspapier zu Transparenzberichten** den Nutzen der Erstellung von Transparenzberichten durch Telekommunikationsunternehmen und Anbieter von Internet-Dienstleistungen für den Datenschutz und die Privatsphäre untersucht. Das Papier enthält Grundsätze zur Gestaltung solcher Transparenzberichte und Empfehlungen zur Umsetzung dieser Grundsätze für Unternehmen, Gesetzgeber, Behörden, Datenschutzbehörden, internationale Regierungsorganisationen, Regulierungsbehörden für Telekommunikation, Branchenverbände und die Zivilgesellschaft.[266]

Das **Arbeitspapier zur intelligenten Video-Analytik** analysiert den zunehmenden Einsatz von Videotechnologien zum Auffinden und Verfolgen von Einzelpersonen, der Verbesserung der Sicherheit und im Rahmen des Kundenmanagements im öffentlichen wie auch im privaten Sektor. Damit können je nach Art des Einsatzes dieser Technologien unterschiedliche Risiken für die Privatsphäre der Betroffenen verbunden sein. Auch greifen die verschiedenen Technologien unterschiedlich tief in die Privatsphäre der Betroffenen ein. Das Arbeitspapier gibt anhand von drei verschiedenen Einsatzszenarien Empfehlungen für Maßnahmen, die zum Schutz der Privatsphäre der Betroffenen beim Einsatz dieser Technologien umgesetzt werden müssen.[267]

Das **Arbeitspapier zur Verfolgung des Aufenthaltsorts auf der Basis von Meldungen von Mobilfunkgeräten** diskutiert die immer populärer werdenden Methoden zur Messung des Kundenverhaltens auch außerhalb des Internets. Dazu werden vielfach die insbesondere von Smartphones bei deren Nutzung ausgesandten Signale zum Betrieb von Bluetooth und zum Auffinden drahtloser Netzwerke (WiFi) genutzt, um auf Flughäfen, in Kaufhäusern oder Einkaufszentren die Wege von Nutzenden dieser Einrichtungen nachzuvollziehen. Das Papier analysiert die damit verbundenen Risiken für die Privatsphäre der Betroffenen und gibt Empfehlungen, wie diese Verfahren unter Beachtung der Grundsätze zum Schutz der Privatsphäre auszugestalten sind.[268]

265 Siehe 15.2, Dokumentenband 2015, S. 79
266 Dokumentenband 2015, S. 88
267 Dokumentenband 2015, S. 115
268 Dokumentenband 2015, S. 105

16 Informationsfreiheit

16.1 Informationsfreiheit in Deutschland

16.1.1 Mehr Transparenz in den Parlamenten

Das Bundesverwaltungsgericht hat in zwei Verfahren entschieden, dass die Bundestagsverwaltung Zugang zu den Ausarbeitungen der Wissenschaftlichen Dienste auf der Grundlage des Informationsfreiheitsgesetzes des Bundes gewähren muss. Der Kläger des ersten Verfahrens[269] begehrte Ablichtungen von Dokumenten der Wissenschaftlichen Dienste und des Sprachendienstes des Deutschen Bundestages, die auf Anforderung des früheren Bundestagsabgeordneten Karl-Theodor zu Guttenberg erstellt und von diesem für seine Dissertation genutzt wurden. Der Kläger im zweiten Verfahren[270] verlangte Einsicht in die auf Anforderung eines Bundestagsabgeordneten von den Wissenschaftlichen Diensten erstellte Ausarbeitung, die sich mit der Beobachtung „unidentifizierter Flugobjekte“ (Ufo) befasste. Der Bundestag lehnte beide Anträge mit der Begründung ab, dass das Informationsfreiheitsgesetz nicht anwendbar sei auf Unterlagen, die der Mandatsausübung der Abgeordneten zugerechnet werden. Das Bundesverwaltungsgericht folgte dem nicht: Der Deutsche Bundestag sei im Hinblick auf Zuarbeiten seiner Wissenschaftlichen Dienste informationspflichtig, denn er nehme insofern Verwaltungsaufgaben wahr. Dass die Abgeordneten die Unterlagen für ihre parlamentarische Tätigkeit nutzen, auf die das IFG nicht anwendbar ist, stehe dem nicht entgegen.

Die Geheimniskrämerei im Bundestag hat zu einer weiteren obergerichtlichen Entscheidung geführt. Das Oberverwaltungsgericht Berlin-Brandenburg[271] hat entschieden, dass ein Pressevertreter Auskunft darüber erhalten muss, an welche Organisationen aufgrund der Befürwortung von Fraktionen Hausausweise erteilt worden sind. Der Auskunftsanspruch stehe den Interessen des freien Bundestagsmandats nicht entgegen. Denn die begehrten Auskünfte ließen

269 BVerwG, Urteil vom 25. Juni 2015, 7 C 1.14
270 BVerwG, Urteil vom 25. Juni 2015, 7 C 2.14
271 OVG Berlin-Brandenburg, Beschluss vom 20. November 2015, OVG 6 S 45.15

keine Rückschlüsse darauf zu, ob und wie häufig einzelne Abgeordnete mit Interessenvertretern, die Inhaber von Hausausweisen sind, zu Gesprächen im Bundestag zusammenkommen. Inwiefern durch die Auskunft das Recht der Interessenvertreter auf informationelle Selbstbestimmung verletzt sein könnte, sei nicht zu erkennen.

Dass ausgerechnet das Gesetzgebungsorgan des Bundes zehn Jahre nach Inkrafttreten des IFG Probleme mit der Umsetzung des Gesetzes im eigenen Verwaltungsbereich hat, ist erstaunlich. Die Gerichtsentscheidungen dürften auch Auswirkungen auf Informationszugangsanträge bei den Landtagsverwaltungen haben.

16.1.2 Ergebnisse der Konferenz der Informationsfreiheitsbeauftragten in Deutschland

Seit langem werden die geheimen Verhandlungen der EU mit den USA zum Transatlantischen Freihandelsabkommen (TTIP) bemängelt.[272] Deshalb hat die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) mehr Transparenz gefordert, die auch eine Offenlegung der Positionen und Forderungen der USA sowie von Lobbyisten umfassen muss.[273] Vor dem Hintergrund „geleakter" Verhandlungsdokumente hat die EU-Kommission den Zugang zu Dokumenten sogar für Parlamente eingeschränkt: Abgeordnete sollen nur noch in Leseräumen in Brüssel Zugang zu den Verhandlungsprotokollen erhalten.[274] Außerdem hat die IFK die berufsständischen Kammern aufgefordert, ihren Transparenzpflichten nachzukommen.[275] Hintergrund ist die zunehmende Tendenz, dass sich Kammern den Informationszugangsgesetzen von Bund und Ländern z. B. unter Berufung auf schutzwürdige Betriebs- und Geschäftsgeheimnisse entziehen. Schließlich hat die IFK angesichts des gesetzgeberischen Flickenteppichs die Gesetzgeber in Bund und Ländern aufgefordert, moderne

272 JB 2014, 14.1

273 Entschließung vom 30. Juni 2015: Mehr Transparenz bei den Verhandlungen über das Transatlantische Freihandelsabkommen (TTIP)!, Dokumentenband 2015, S. 127

274 Der Tagesspiegel vom 13. August 2015, S. 1: „TTIP wird noch geheimer"

275 Entschließung vom 30. Juni 2015: Auch Kammern sind zur Transparenz verpflichtet!, Dokumentenband 2015, S. 128

Transparenzgesetze zu schaffen und die Einheitlichkeit der Lebensbedingungen auch im Bereich der Verwaltungstransparenz herzustellen.[276]

16.1.3 Gesetzgebung in anderen Bundesländern

Inzwischen besteht in 12 Bundesländern ein Recht auf Zugang zu Verwaltungsinformationen, ohne dass die antragstellende Person ihr Einsichtsinteresse begründen muss.[277] Lange erwartet wurde das Landesinformationsfreiheitsgesetz in Baden-Württemberg.[278] Wider Erwarten enthält es viele überflüssige Einschränkungen, wie die Konferenz der Informationsfreiheitsbeauftragten in Deutschland in ihrer Stellungnahme gegenüber der baden-württembergischen Landesregierung kritisiert hat.[279] Die Leuchttürme in Sachen Informationsfreiheit stehen in Bremen und in Rheinland-Pfalz. Die Hansestadt war bereits seit 2006 ein Vorreiter in Sachen Transparenz, weil mit dem Informationsfreiheitsgesetz erstmalig eine proaktive Veröffentlichungspflicht eingeführt worden war. Auch wurde ein Informationsfreiheitsregister eingerichtet, in dem die Verwaltung bestimmte Dokumente, Gutachten und insbesondere Verträge anlasslos veröffentlichen musste. Das jetzt novellierte IFG sieht eine Zusammenführung des Informationsfreiheitsregisters mit dem Open-Data-Portal in einem neuen Transparenzportal vor.[280] Im November ist das neue Transparenzgesetz für Rheinland-Pfalz in Kraft getreten. Es löste damit das noch relativ junge IFG von 2012 ab. Auch hier steht die proaktive Bereitstellung von Verwaltungsinformationen im Internet im Vordergrund. Ein Transparenzportal nach Bremer und Hamburger Vorbild soll bereits 2016 online sein.

276 Entschließung vom 4. Dezember 2015: Informationsfreiheit 2.0 – endlich gleiches Recht in Bund und Ländern!, Dokumentenband 2015, S. 129

277 Die vier Bundesländer ohne anspruchsbegründende Gesetze sind Bayern, Hessen, Niedersachsen und Sachsen.

278 Art. 1 des Gesetzes zur Einführung der Informationsfreiheit vom 17. Dezember 2015, GBl. S. 1201

279 Stellungnahme der Konferenz der Informationsfreiheitsbeauftragten in Deutschland zum Entwurf eines Gesetzes zur Einführung der Informationsfreiheit in Baden-Württemberg vom 18. September 2015, abrufbar unter www.datenschutz-berlin.de/news/datenschutz-nachrichten .

280 www.transparenz.bremen.de

Es ist bedauerlich, dass das Land Berlin als ehemaliges Vorbild in Sachen Informationsfreiheit mit dem Gesetz von 1999 auch – aber nicht nur – im Vergleich zu den anderen Stadtstaaten immer weiter ins Hintertreffen gerät, weil es offenbar die Zeichen der Zeit nicht erkennt.

16.2 Informationsfreiheit in Berlin

16.2.1 Veröffentlichung von Ergebnissen der Lebensmittelüberwachung

Wir haben in der Vergangenheit kontinuierlich über das sog. Smiley-System in Berlin (speziell im Bezirk Pankow) berichtet,[281] das sich noch nicht durchgesetzt hat. Es gilt als der deutsche Vorreiter des auf der Grundlage des Verbraucherinformationsgesetzes entwickelten Transparenzmodells, das die Verbraucherinnen und Verbrauchern vor dem Betreten einer Gaststätte über die dort amtlich festgestellten hygienischen Zustände informieren soll. Allerdings haben das Verwaltungsgericht Berlin und das Oberverwaltungsgerichts Berlin-Brandenburg die Veröffentlichung der Ergebnisse von Lebensmittelkontrollen im Internet durch Einstufung in „Benotungen“ und Vergabe von „Minuspunkten“ mangels erforderlicher Rechtsgrundlage untersagt. Zwar sieht der Referentenentwurf des Bundesministeriums für Ernährung und Landwirtschaft in § 40a Lebensmittel- und Futtermittelgesetzbuch (LFGB) eine neue Regelung zur „Information der Öffentlichkeit“ vor. Jedoch fehlt eine umfassende Transparenzregelung durch eine Ermächtigung zur einschränkungslosen Veröffentlichung von Lebensmittelkontrollberichten.

Da eine bundesrechtliche Regelung zeitnah nicht zu erwarten war, hat das Land Berlin eine begrüßenswerte Bundesratsinitiative für mehr Transparenz durch die Veröffentlichung der Ergebnisse amtlicher Überwachungs- und Kontrollmaßnahmen von Lebens- und Futtermittelunternehmen gestartet.[282] Damit soll für die Länder eine sichere Grundlage zum Erlass eigener Regelungen geschaffen werden, die es auch ermöglichen, dass die amtlichen

281 Zuletzt JB 2011, 13.2 (S. 190)
282 BR-Drs. 410/15 vom 15. September 2015

Kontrollberichte zu den jeweiligen Gaststätten durch Aushang veröffentlicht werden.

16.2.2 Elektronische Antragstellung per (einfacher) E-Mail

Nach der derzeitigen Rechtslage ist ein Antrag auf Akteneinsicht oder Aktenauskunft nach dem IFG schriftlich oder mündlich zu stellen.[283] Eine elektronische Antragstellung ist daher nur in bestimmten Fällen zulässig, in denen die Schriftform durch die elektronische Form ersetzt werden kann.[284] So kann ein Antrag per E-Mail oder De-Mail gestellt werden, wenn diese mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz[285] bzw. nach dem De-Mail-Gesetz[286] versehen ist. Die elektronische Antragstellung ist daher für antragstellende Personen nur mit erheblichen Hürden möglich, da in den genannten Fällen entweder ein qualifiziertes Zertifikat[287] oder ein De-Mail-Konto[288] erforderlich ist. Ferner muss auch die öffentliche Stelle über die Möglichkeit verfügen, qualifiziert elektronisch signierte E-Mails bzw. De-Mails zu empfangen und die Signatur rechtssicher zu prüfen.

Bereits 2013 wandte sich der Petitionsausschuss des Abgeordnetenhauses an uns, da ein Bürger dort vorgeschlagen hatte, das Formerfordernis bei der Antragstellung zu streichen. Wir hatten dem Petitionsausschuss daraufhin mitgeteilt, dass einerseits in fast allen Bundesländern mit Informationsfreiheits- bzw. Transparenzgesetzen eine elektronische Antragstellung auch per einfacher, d. h. nicht qualifiziert elektronisch signierter E-Mail möglich ist, andererseits – trotz der anderslautenden Regelung im IFG – die elektronische Antragstellung per einfacher E-Mail in Berlin bereits die Regel darstellt und weiter zunehmen wird. Wir schlugen dem Petitionsausschuss daher vor, den Vorschlag des Petenten zu unterstützen.

283 § 13 Abs. 1 Satz 1 IFG
284 § 3a Abs. 2 Satz 1 VwVfG Bund
285 § 3a Abs. 2 Satz 2 VwVfG Bund
286 § 3a Abs. 2 Satz 4 Nr. 2 VwVfG Bund
287 § 2 Nr. 7 SigG
288 § 5 Abs. 1 De-Mail-G

Mit dem Berliner E-Government-Gesetz[289] soll nun das Antragserfordernis nach dem IFG dahingehend erweitert werden, dass die Antragstellung zukünftig mündlich, schriftlich oder elektronisch möglich ist, d. h. auch per einfacher, nicht qualifiziert elektronisch signierter E-Mail. Dies ist ein erster wichtiger Schritt, das IFG von 1999 an das digitale Zeitalter anzupassen.

16.2.3 Weiterverwendung von Informationen zu gewerblichen Zwecken

Bislang war es unzulässig, die durch Akteneinsichten oder -auskünfte nach dem IFG erhaltenen Informationen zu gewerblichen Zwecken zu veröffentlichen, zu speichern oder zu sammeln.[290] Der Verstoß gegen dieses Verbot konnte als Ordnungswidrigkeit mit einer Geldbuße bis zu 5.000 € geahndet werden.[291]

Dass die entsprechenden Vorschriften im IFG der europäischen Richtlinie über die Weiterverwendung von Informationen des öffentlichen Sektors von 2003[292] widersprechen, hatten wir seinerzeit im Gesetzgebungsverfahren zum Informationsweiterverwendungsgesetz des Bundes (IWG) vorgebracht.[293] In der Richtlinie war nämlich die Weiterverwendung von Informationen im Sinne einer wirtschaftlichen Nutzung ausdrücklich vorgesehen. Unsere Anregung zur Streichung der entgegenstehenden Vorschriften im IFG wurde jedoch nicht aufgegriffen.

Diese Richtlinie wurde 2013 geändert.[294] Die Umsetzung der Änderung erfolgte 2015 dadurch, dass in das IWG ausdrücklich der Grundsatz der Weiterverwendung von Informationen aufgenommen wurde, sofern sie in den Anwendungsbereich dieses Gesetzes fallen.[295]

289 Abghs.-Drs. 17/2513 vom 27. Oktober 2015
290 § 13 Abs. 7 IFG a. F.
291 § 22 IFG a. F.
292 Richtlinie 2003/98/EG
293 JB 2006, 6.1
294 Richtlinie 2013/37/EU
295 § 2a Satz 1 IWG

Aus diesem Anlass wurden das Verwendungsverbot und die Bußgeldvorschrift im IFG aufgehoben.[296] Daher ist nun auch die Weiterverwendung von nach dem IFG erlangten Informationen zu gewerblichen Zwecken nach Maßgabe des IWG zulässig.

16.2.4 Unzulässige Verwendungsbeschränkung

Aus der Praxis

Ein Petent bat das Landesverwaltungsamt (LVwA) um Übersendung des mit dem Kulturbuch-Verlag geschlossenen Konzessionsvertrags über die Herstellung und den Vertrieb des Amtsblatts für Berlin sowie von Informationen, welche datenschutzrechtlichen Gründe einer vollständigen maschinenlesbaren Veröffentlichung des Amtsblattes entgegenstehen. Das LVwA übersandte ihm daraufhin den Kooperationsvertrag sowie eine Antwort auf eine Kleine Anfrage im Abgeordnetenhaus, aus der sich die Gründe gegen eine vollständig maschinenlesbare Online-Veröffentlichung des Amtsblatts ergaben. Die Übersendung erfolgte jedoch mit dem ausdrücklichen Hinweis, dass die Vervielfältigung, Weitergabe und Veröffentlichung in gedruckten oder elektronischen Medien nicht gestattet sei.

Durch Akteneinsichten oder -auskünfte nach dem IFG erhaltene Informationen dürfen grundsätzlich frei weiterverwendet und insbesondere auch vervielfältigt, weitergegeben und veröffentlicht werden. Weder enthält das Gesetz Verwendungsbeschränkungen, noch sind öffentliche Stellen selbst dazu berechtigt, eine Weiterverwendung der durch Akteneinsichten oder -auskünfte erhaltenen Informationen zu beschränken oder zu untersagen. Zum damaligen Zeitpunkt enthielt das IFG zwar noch das (zwischenzeitlich aufgehobene) Verwendungsverbot bei gewerblichen Zwecken, zu denen etwa die Nutzung für kommerzielle Datenbanken gehörte.[297] Der Petent verfolgte jedoch solche Zwecke nicht, sodass eine Veröffentlichung auch nach damaliger Rechtslage zulässig gewesen wäre. Wir teilten dem LVwA daher mit, dass der Petent den Konzessionsvertrag frei weiterverwenden und im Internet veröffentlichen darf, was der Petent später auch tat.

296 Drittes Gesetz zur Änderung des Berliner Informationsfreiheitsgesetzes, GVBl. 2015, S. 285
297 Zu den Einzelheiten siehe 16.2.3

Die Weiterverwendung der durch Informationszugang nach dem IFG erhaltenen Informationen unterliegt keinen gesetzlichen Beschränkungen und darf auch von öffentlichen Stellen nicht untersagt werden.

16.2.5 Unzulässiger Einsatz von Antragsformularen

Ein Petent bat beim Bezirksamt Pankow um Akteneinsicht in die Bauantragsunterlagen für zwei geplante Gebäude des Max-Delbrück-Centrums für Molekulare Medizin. Anstatt der erwarteten Unterlagen erhielt er jedoch ein Schreiben des Bezirksamts, dem ein Formular „Antrag auf Gewährung von Akteneinsicht / Auskunft nach dem Informationsfreiheitsgesetz (IFG)“ mit dem Hinweis beigefügt war, dass nach Eingang des Antrags und Rücksprache mit den Betroffenen telefonisch ein Termin vereinbart werden könne. Neben der zwingenden Festlegung auf die Rechtsgrundlage IFG war in dem Formular ein Pflichtfeld für eine Begründung des Antrags vorgesehen.

Antragstellende Personen sind nicht verpflichtet, ein Formular für einen Antrag auf Gewährung von Akteneinsicht bzw. -auskunft nach dem IFG auszufüllen. Insbesondere ist es nicht zulässig, die Vergabe von Terminen für die Akteneinsicht davon abhängig zu machen, dass die antragstellende Person ein solches Formular ausfüllt. Der Antrag auf Informationszugang kann sowohl mündlich als auch schriftlich gestellt werden und bedarf keiner besonderen Form.[298] Darüber hinaus handelt es sich um einen voraussetzungslosen Anspruch, der nicht begründet werden muss. Zudem müssen sich antragstellende Personen nicht bei der Akteneinsicht in das Bauaktenarchiv auf die Anspruchsgrundlage IFG festlegen, was zur Zahlung einer Verwaltungsgebühr führen würde. Denn womöglich kommen andere – gebührenfreie – Anspruchsgrundlagen[299] in Betracht, die zwar der Verwaltung, aber nicht dem durchschnittlichen Bürger bekannt sein dürften.

298 Zu der anstehenden Gesetzesänderung für die elektronische Antragstellung siehe 16.2.2

299 Vor allem § 16 Abs. 4 Satz 1 BlnDSG, § 4a Abs. 1 Satz 1 VwVfG Berlin und § 18a Abs. 1 und Abs. 4 Satz 3 Nr. 1 IFG i.V. m. § 3 Abs. 1 Satz 1 UIG

Der Einsatz dieses Formulars erstaunte vor allem deswegen, weil wir bereits 2011 ein identisches Formular gerügt und auf die geltende Rechtslage hinsichtlich der Antragstellung, und erst zwei Monate zuvor anlässlich eines ähnlichen vom Bezirksamt eingesetzten Formulars auf die Problematik der Festlegung auf die gebührenpflichtige Anspruchsgrundlage „IFG“ hingewiesen hatten. Wir wandten uns daher an den Bezirksbürgermeister mit der Bitte, dafür zu sorgen, dass zukünftig bei entsprechenden Anträgen auf Akteneinsicht oder -auskunft einerseits auf Antragsformulare verzichtet, andererseits von antragstellenden Personen weder eine Begründung des Antrags noch eine verbindliche Festlegung auf eine gebührenpflichtige Anspruchsgrundlage verlangt wird. Der Bezirksbürgermeister teilte uns mit, dass das Antragsformular künftig nicht mehr verwendet werde und die Beschäftigten nochmals hinsichtlich anderer in Betracht kommender Rechtsgrundlagen sensibilisiert worden seien. Der Petent hat schließlich die begehrte Akteneinsicht gebührenfrei erhalten.

Antragstellende Personen sind weder dazu verpflichtet, ein Antragsformular auszufüllen oder ihren Antrag zu begründen, noch sich auf eine gebührenpflichtige Anspruchsgrundlage festzulegen.

16.2.6 Vollmacht zur Akteneinsicht in Bauakten?

Aus der Praxis

Eine Petentin begehrte beim Bezirksamt Pankow Akteneinsicht in Unterlagen zu Schallmessungen und Begehungen einer Gaststätte. Das Bezirksamt teilte ihr daraufhin einen Termin für die Akteneinsicht mit verbunden mit dem Hinweis, dass hierfür eine schriftliche Vollmacht des Eigentümers vorzulegen und je angefangene halbe Stunde eine Gebühr i. H. v. 41,58 € zu entrichten sei.

Die Gewährung der Akteneinsicht hängt jedoch nicht von der Genehmigung oder Zustimmung der Betroffenen ab, sodass die Vorlage einer entsprechenden Vollmacht nicht verlangt werden darf. Auch ist die Gebührenhöhe nach dem Umfang der Amtshandlung und den Schwierigkeiten, die sich bei der Durchführung der Amtshandlung ergeben, zu bemessen,[300] sodass nur der

300 § 5 Nr. 2 VGebO

tatsächlich entstandene Zeitaufwand angesetzt werden darf, nicht jedoch ein (aufgerundeter) Zeitaufwand für jede angefangene halbe Stunde.

Dies teilten wir dem Bezirksamt mit und baten darum, unter Beachtung dieser Ausführungen erneut über den Antrag der Petentin zu entscheiden.

Erst nach Einschaltung des Bezirksbürgermeisters teilte uns der zuständige Bezirksstadtrat mit, dass er unsere Einschätzung vollumfänglich teile und die Formulierungen hinsichtlich der Vollmacht und der Gebührenhöhe überarbeitet werden. Im vorliegenden Fall sei zur Beschleunigung des Verfahrens um eine Vollmacht gebeten worden, was jedoch dem Schreiben an die Petentin nicht zu entnehmen gewesen sei. Der zuständige Mitarbeiter sei angewiesen worden, sich wegen der erbetenen Akteneinsicht mit der Petentin in Verbindung zu setzen.

Kurz darauf erhielt die Petentin zwar ein entsprechendes Schreiben. Dieses war jedoch – abgesehen vom Datum und vom angebotenen Termin für die Akteneinsicht – inhaltsgleich zu dem ursprünglichen Schreiben, das sie nahezu sechs Monate zuvor erhalten hatte. Wir baten daher den Bezirksstadtrat, darauf hinzuwirken, dass der Petentin die begehrte Akteneinsicht nunmehr unverzüglich ohne diese unzulässigen Bedingungen gewährt wird, und regten angesichts der überlangen Verfahrensdauer von mehr als sieben Monaten an, die Akteneinsicht durch Übersendung von Fotokopien der begehrten Unterlagen zu gewähren. Rund einen Monat später – insgesamt beinahe zehn Monate nach Antragstellung – erhielt die Petentin endlich die begehrten Unterlagen.

Die Gewährung des Informationszugangs hängt nicht von der Zustimmung der Betroffenen ab. Bei der Bemessung der Gebühren für Informationszugang darf zudem nur der tatsächlich entstandene Verwaltungsaufwand berücksichtigt werden.

16.2.7 Akteneinsicht bei der Berliner Sparkasse

Eine Petentin – eine GmbH – begehrte bei der Berliner Sparkasse Akteneinsicht in Schriftverkehr zu einer sie betreffenden Darlehensvermittlung. Die Sparkasse lehnte dies mit der Begründung ab, in der Angelegenheit nicht hoheitlich-behördlich, sondern privatrechtlich auf vertraglicher Gleichordnungsebene tätig gewesen zu sein. Die Petentin teilte der Sparkasse daraufhin mit, dass das IFG auch dann Anwendung finde, wenn eine öffentliche Stelle in der Form des Privatrechts tätig werde. Die Sparkasse lehnte die Akteneinsicht daraufhin mit dem Argument ab, dass sie ausgehend vom Gesetzeszweck[301] schon nicht in den Anwendungsbereich des IFG[302] falle.

Das IFG regelt die Informationsrechte gegenüber allen Behörden und sonstigen öffentlichen Stellen des Landes Berlin.[303] Die Sparkasse ist eine teilrechtsfähige Anstalt des öffentlichen Rechts[304] und unterliegt somit als öffentliche Stelle des Landes Berlin dem Anwendungsbereich des IFG. Somit besteht ein Anspruch auf Einsicht in oder Auskunft über den Inhalt der von der Sparkasse geführten Akten.[305] Akten in diesem Sinne sind u. a. alle schriftlich, elektronisch oder auf andere Weise festgehaltenen Gedankenverkörperungen und sonstige Aufzeichnungen, soweit sie amtlichen Zwecken dienen.[306] Amtlichen Zwecken dient eine Aufzeichnung dann, wenn sie die öffentliche Stelle betrifft, bei einer amtlichen Tätigkeit stattfindet oder die in anderer Weise im Zusammenhang mit der amtlichen Tätigkeit steht. Insbesondere wird dabei keine Unterscheidung getroffen, ob die öffentliche Stelle öffentlich-rechtlich oder privatrechtlich handelt, sodass das IFG auch bei fiskalischem Handeln öffentlicher Stellen uneingeschränkt anwendbar ist.

Dies teilten wir der Sparkasse mit und baten, unter Berücksichtigung dieser Rechtslage erneut über den Antrag der Petentin zu entscheiden. Die Sparkasse blieb bei ihrer Auffassung, dass nach dem IFG zwar auch sonstige öffentliche Stellen des Landes Berlin sowie landesunmittelbare Anstalten des öffentlichen

301 § 1 IFG
302 § 2 Abs. 1 IFG
303 § 2 Abs. 1 Satz 1 IFG
304 § 3 Abs. 1 SpkG
305 § 3 Abs. 1 Satz 1 IFG
306 § 3 Abs. 2 IFG

Rechts informationspflichtig seien.[307] Bei der Sparkasse handle es sich jedoch nur um eine teilrechtsfähige Anstalt des öffentlichen Rechts, die vollständig im Eigentum der Landesbank Berlin AG stehe, die wiederum vollständig im Eigentum der Sparkassen-Finanzgruppe stehe, weshalb das Land Berlin weder unmittelbar noch mittelbar an der Sparkasse beteiligt sei. Daher handle es sich bei der Sparkasse weder um eine sonstige öffentliche Stelle des Landes Berlin noch um eine landesunmittelbare Anstalt des öffentlichen Rechts.

Diese Argumentation vermochte nicht zu überzeugen, da sie im Gesetz keine Stütze findet. Zwar mag es zutreffen, dass die Sparkasse keine landesunmittelbare Anstalt des öffentlichen Rechts ist. Dies ändert jedoch nichts daran, dass es sich bei der Sparkasse um eine sonstige öffentliche Stelle im Sinne des IFG handelt. Hierzu gehören insbesondere – jedoch nicht abschließend – nicht rechtsfähige Anstalten, Krankenhausbetriebe, Eigenbetriebe und Gerichte.[308] Es sind keine Anhaltspunkte dafür ersichtlich, dass nach dem Willen des Gesetzgebers zwar die vollrechtsfähigen und sogar die nicht rechtsfähigen Anstalten dem IFG unterliegen sollen, nicht jedoch die teilrechtsfähigen Anstalten. Wir baten die Sparkasse daher letztmalig, unter Berücksichtigung der Rechtslage erneut über den Antrag der Petentin zu entscheiden, und drohten für den Fall weiterer Weigerung eine förmliche Beanstandung[309] an. Die Sparkasse übersandte der Petentin nach über fünf Monaten schließlich die begehrten Unterlagen.

Ein Unternehmen mit öffentlich-rechtlicher Rechtsform unterliegt dem Anwendungsbereich des IFG selbst dann, wenn es nicht öffentlich-rechtlich, sondern rein privatrechtlich tätig ist.

307 § 2 Abs. 1 Satz 1 IFG
308 § 2 Abs. 1 Satz 1, 1. Fall IFG
309 § 26 BlnDSG

17 Wo wir den Menschen sonst noch helfen konnten …

Eine **Schwangere** beschwerte sich darüber, dass sie für die außerordentliche Kündigung ihres Vertrages im **Fitnessstudio** neben der ärztlich attestierten Sportuntauglichkeit auch eine Kopie ihres Mutterpasses vorlegen sollte oder ein ärztliches Attest, aus dem der genaue Entbindungstermin hervorgeht. Auf ihre Weigerung zur Vorlage einer ungeschwärzten Kopie des Mutterpasses hat das Fitnessstudio zunächst nur eine ordentliche Kündigung akzeptiert. Die Angabe, schwanger zu sein, ist ein sensitives Datum.[310] Das Erheben, Verarbeiten und Nutzen dieses Datums für eigene Geschäftszwecke ist nur zulässig, wenn dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und die schutzwürdigen Interessen der Betroffenen nicht überwiegen.[311] Um einen Missbrauch des Kündigungsrechtes auszuschließen, durfte das Fitnessstudio nach der Rechtsprechung des Bundesgerichtshofes einen Nachweis zur Aktualität der Schwangerschaft verlangen.[312] Hierfür war aber nicht die Vorlage einer ungeschwärzten Kopie des gesamten Mutterpasses notwendig. Der Mutterpass enthält nämlich neben der Feststellung der Schwangerschaft weitere Anamnese-Daten, deren Mitteilung für eine Kündigung im Fitnessstudio nicht relevant ist und den Interessen der Schwangeren zuwiderläuft. Nachdem wir das Fitnessstudio über diese Tatsache aufgeklärt hatten, wurden die genutzten Vordrucke im Fitnessstudio geändert und die Beschäftigten hinsichtlich solcher Fälle entsprechend belehrt. Die außerordentliche Kündigung der Petentin wurde akzeptiert.

Ein Bürger beschwerte sich über eine Klinik, da sie auf der vom Petenten mitgebrachten CD einer Magnetresonanztomografie (MRT) einen **nicht mehr entfernbaren Aufdruck** angebracht hat, der den Namen der Klinik enthielt. Durch den Aufdruck war für Dritte erkennbar, dass der Patient in diesem

310 § 3 Abs. 9 BDSG
311 § 28 Abs. 6 Nr. 3 BDSG
312 BGH, Urteil vom 8. Februar 2012, XII ZR 42/10, Rn. 33

Krankenhaus untersucht wurde. Diese unter die Schweigepflicht fallende Tatsache würde einer später behandelnden Einrichtung bekannt gegeben. Wir konnten die Änderung des Verfahrens im Krankenhaus erreichen. So wurde festgelegt, dass grundsätzlich nur die CD-Hüllen mit dem entsprechenden Aufdruck versehen werden. Dadurch wird zukünftig gewährleistet, dass Patienten die Möglichkeit haben, die Behandlung bei dem betreffenden Krankenhaus gegenüber nachbehandelnden Ärzten nicht zu offenbaren.

Eine Bürgerin bat um Unterstützung, da ein an sie gerichtetes Schreiben eines Gesundheitsamtes im Adressfeld den **Zusatz „früher männlich"** enthielt. Durch diesen Textzusatz im offenen Adressfeld, der für eine Zustellbarkeit des Briefes in keinem Fall erforderlich war, konnten unbefugte Dritte diese besonders sensitive Information zur Kenntnis nehmen. Dies wurde gegenüber dem Gesundheitsamt beanstandet, da neben dem Verstoß gegen **die ärztliche Schweigepflicht** auch das Gebot der Vertraulichkeit verletzt wurde, wonach Behörden dazu verpflichtet sind, Daten vor der Kenntnisnahme durch Unbefugte zu schützen. Das Gesundheitsamt konnte glaubhaft darstellen, dass es sich bei dem festgestellten Datenschutzverstoß um einen bedauerlichen Einzelfall gehandelt hat. Unverzüglich wurden Maßnahmen ergriffen, um solche Datenschutzverletzungen in Zukunft ausschließen zu können. Es wurden sowohl der Datensatz korrigiert als auch die Beschäftigten noch einmal explizit auf deren Sorgfaltspflicht hingewiesen.

Mehrfach erhielten wir Eingaben zu dem Berliner Hörbuch-Streaming-Anbieter „**Audible**". Das Unternehmen hat die **Löschung der Accounts von Kunden** verweigert, die sich – meist nach einer offensiv beworbenen kostenlosen Nutzungsphase – gegen eine Weiterführung der Vertragsbeziehung entschieden haben. Begründet wurde die Weigerung damit, dass das Unternehmen zu Amazon gehöre und die Löschung nur möglich wäre, wenn gleichzeitig der Amazon-Account gelöscht werde. Nach unserer Intervention stellte das Unternehmen klar, dass tatsächlich die Kundendaten ausschließlich bei Amazon geführt würden, das Amazon-Konto jedoch über eine Kennzeichnung verfüge, ob die betreffenden Nutzer auch Audible-Kunden sind oder nicht. Nur im ersten Fall könne das Unternehmen auf die notwendigen Kundendaten zugreifen. Die Bearbeitung von Löschaufforderungen wird von dem Unternehmen nun mit einer verständlicheren Information beantwortet, und die Verknüpfung der Amazon-Accounts mit „Audible" wird entfernt.

Eine Bürgerin bat uns um Prüfung, weshalb auf den **Pensionärsausweisen** des Landesverwaltungsamtes (LVwA) der **Zahlungsgrund der Versorgungsbezüge** nach beamtenrechtlichen Vorschriften (z. B. Ruhegehalt, Unterhaltsbeitrag oder Hinterbliebenenbezüge) enthalten sei. Ferner bestehe die Möglichkeit anzukreuzen, soweit die Versetzung in den Ruhestand wegen Dienstunfähigkeit erfolgt sei. Aufgrund unserer Intervention stellte das LVwA fest, dass die Angabe der Gründe nicht erforderlich ist. Die inhaltliche Gestaltung des Pensionärsausweises wurde daraufhin geändert.

Ein Petent begehrte vom **Polizeipräsidenten in Berlin** gestützt auf das IFG die Übersendung der **Errichtungsanordnung** für die Datei „Sportgewalt Berlin". Der Polizeipräsident lehnte das ab: Die Errichtungsanordnung sei nicht zur Einsichtnahme bestimmt,[313] da eine solche mit der Erfüllung der Aufgaben der Gefahrenabwehr und Strafverfolgung für unvereinbar erklärt worden sei. Nach Erörterung der Rechtslage teilte uns der Polizeipräsident mit, dass die für die Errichtungsanordnung zuständige Dienststelle die Einstufung aufheben werde und der Herausgabe von Kopien an den Petenten dann nichts mehr entgegenstehe. Der nach dem IFG gebührenpflichtige[314] Antrag des Petenten wurde in einen gebührenfreien Antrag nach dem BlnDSG[315] umgedeutet. Lediglich die Kopierkosten in Höhe von 2 € musste der Petent tragen.

Ein Petent bat beim **Bezirksamt Mitte** um Auskunft, ob für ein bestimmtes Grundstück ein **Bauantrag** oder Ähnliches vorliegt. Das Bezirksamt teilte ihm mit, dass er als Mieter nicht Beteiligter am Verfahren sei und Unbeteiligten aus Datenschutzgründen keine Auskünfte zu Verfahren gegeben werden können. Wir wiesen das Bezirksamt unter Verweis auf unser Rundschreiben[316] darauf hin, dass diese Auffassung unzutreffend ist und der Petent einen Anspruch auf die Erteilung der begehrten Auskunft hat. Das Bezirksamt teilte dem Petenten daraufhin mit, dass für das Grundstück derzeit keine aktuellen Anträge vorlägen, wies jedoch unter Beifügung eines Gebührenbescheids darauf hin, dass diese Auskunft gebührenpflichtig sei. Wir teilten dem Bezirksamt daraufhin mit, dass Aktenauskünfte zwar grundsätzlich gebührenpflichtig sind,[317] die

313 § 19a Abs. 1 Satz 7 BlnDSG
314 § 16 IFG
315 § 19a Abs. 1 Satz 5 BlnDSG
316 Rundschreiben vom 21. Mai 2014, Geschäftszeichen 50.651.17
317 § 16 IFG

„Negativauskunft", dass für ein Grundstück kein Bauantrag oder Ähnliches vorliegt, jedoch keine gebührenpflichtige Auskunft in diesem Sinne darstellt.[318] Wir baten um Überprüfung der Gebührenentscheidung. Das Bezirksamt nahm daraufhin den Bescheid zurück und erstattete dem Petenten die bereits entrichtete Gebühr.

Ein Petent bat das **Bezirksamt Spandau** um Einsicht in den **Genehmigungsbescheid eines Zaunes**. Das Bezirksamt lehnte den Antrag mit der Begründung ab, dass der Petent das Vorliegen eines berechtigten Interesses an einer Kopie der entsprechenden Genehmigung nicht vorgetragen habe. Wir wiesen das Bezirksamt darauf hin, dass das Recht auf Akteneinsicht nach dem IFG voraussetzungslos ist und der Antragsteller den Antrag weder begründen noch sein Informationsinteresse dartun muss. Das Recht auf Akteneinsicht ist auch nicht von einem berechtigten Interesse des Antragstellers abhängig. Die Akteneinsicht ist in dem beantragten Umfang zu gewähren, wenn keine der im IFG geregelten Ausnahmen greift.[319] Das Bezirksamt übersandte dem Petenten daraufhin die begehrten Unterlagen.

318 Zu den Einzelheiten siehe JB 2014, 14.3.1
319 § 4 Abs. 1 IFG

18 Aus der Dienststelle

18.1 Entwicklungen

Die Dienststelle konnte im April in die Friedrichstraße 219 (Besuchereingang: Puttkamerstr. 16-18) in Kreuzberg umziehen, nachdem das Abgeordnetenhaus von Berlin und das Berliner Immobilienmanagement hierfür die Voraussetzungen geschaffen hatten. Damit ging eine längere Phase der Unsicherheit für die Beschäftigten angesichts möglicher gesundheitlicher Belastungen im alten Dienstgebäude An der Urania 4-10 zu Ende.

Der Haushaltsgesetzgeber hat den Wünschen des Berliner Beauftragten für Datenschutz und Informationsfreiheit für den Doppelhaushalt 2016/2017 in großen Teilen entsprochen und damit die Voraussetzung dafür geschaffen, dass neben der Bearbeitung der steigenden Zahl von Eingaben wenigstens ein Mindestmaß an Prüfungen von Amts wegen wird durchgeführt werden können.

Allerdings ist bereits jetzt abzusehen, dass mit der Verabschiedung der EU-Datenschutz-Grundverordnung und im Vorgriff auf ihr Inkrafttreten 2018 neue umfangreiche Aufgaben auf die Dienststelle zukommen. Die Beratung der Behörden und Unternehmen sowie die Notwendigkeit der verstärkten Kooperation mit den deutschen Datenschutzbehörden und mit dem Europäischen Datenschutzausschuss, der an die Stelle der Art. 29-Gruppe treten wird, werden zu einem erheblichen Mehraufwand führen, zumal die Entscheidungsprozesse auf europäischer Ebene künftig mit engen Fristen für die Stellungnahmen der nationalen Datenschutzbehörden verbunden sein werden. Dies führt in Zukunft zu einem erhöhten Personalbedarf, der befriedigt werden muss, um die Rechte der Berlinerinnen und Berliner nach dem künftig einheitlichen europäischen Recht zu schützen.

18.2 Zusammenarbeit mit dem Abgeordnetenhaus von Berlin

Der Ausschuss für Digitale Verwaltung, Datenschutz und Informationsfreiheit hat den Jahresbericht 2014 und die Stellungnahme des Senats in einer Sitzung am 23. November abschließend behandelt. Die Empfehlungen des Berliner Beauftragten für Datenschutz und Informationsfreiheit wurden dabei zum Teil aufgegriffen, und die zuständigen Verwaltungen wurden zur datenschutzgerechten Gestaltung ihrer Verfahren aufgefordert. Anders als in früheren Jahren hat das Abgeordnetenhaus aufgrund der Beratungen über den Jahresbericht und die Senatsstellungnahme keine inhaltlichen Beschlüsse zu Datenschutz oder Informationsfreiheit gefasst.

Der Ausschuss vertagte im Übrigen die Beratungen über einen Vorschlag des Berliner Beauftragten für Datenschutz und Informationsfreiheit zu den Konsequenzen des Urteils des Europäischen Gerichtshofs vom 6. Oktober zum Safe Harbor-Abkommen[320] für die Berliner Verwaltung. Zunächst hatte der Vertreter der Senatsverwaltung für Inneres und Sport im Ausschuss die Auffassung vertreten, das Urteil betreffe die öffentliche Verwaltung nicht. Nach dem Hinweis des Berliner Beauftragten für Datenschutz und Informationsfreiheit auf zahlreiche Fälle, in denen z. B. Schulen Dienste von amerikanischen IT-Dienstleistern (sog. Cloud-Dienste) in Anspruch nehmen wollen, ohne dass sie die Frage des gleichwertigen Datenschutzniveaus im Zielland überblicken könnten, sagte der Vertreter der Senatsverwaltung eine erneute Prüfung zu. Deren Ergebnis steht noch aus.

18.3 Zusammenarbeit mit anderen Stellen

Die **Konferenz der Datenschutzbeauftragten des Bundes und der Länder** tagte am 18./19. März in Wiesbaden und am 30. September/1. Oktober in Darmstadt unter dem Vorsitz des Hessischen Datenschutzbeauftragten

320 Siehe 14.1

und fasste zahlreiche Entschließungen zu aktuellen Fragen des Datenschutzes.[321] Zusätzlich fanden drei Sondersitzungen dieser Konferenz in Kassel und in Frankfurt am Main statt; in der letzten dieser Sondersitzungen am 21. Oktober wurde das Positionspapier zu den Auswirkungen des EuGH-Urteils zum Safe Harbor-Abkommen beschlossen.[322] Für 2016 hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern den Vorsitz in der Konferenz übernommen. Der **Düsseldorfer Kreis**, in dem unter dem Vorsitz der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen die **Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich** zusammenarbeiten, fasste Entschließungen zur Videoüberwachung im öffentlichen Personennahverkehr, in Schwimmbädern und zur Nutzung von Kameradrohnen durch Private.[323]

Die **Konferenz der Informationsfreiheitsbeauftragten in Deutschland** tagte am 30. Juni in Schwerin und fasste dort sowie anschließend mehrere Entschließungen zum Transatlantischen Freihandelsabkommen, zur Transparenz bei Kammern und zur Vereinheitlichung des Informationsfreiheitsrechts in Bund und Ländern.[324] 2016 wird die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen den Vorsitz in dieser Konferenz übernehmen.

Berlin hat seit 1996 die Bundesländer in der **Arbeitsgruppe nach Art. 29 der Europäischen Datenschutzrichtlinie** vertreten. Im März hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit auf Beschluss der Konferenz der Datenschutzbeauftragten des Bundes und der Länder diese Vertretung übernommen. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit war weiterhin in den Unterarbeitsgruppen „Border, Travel, Law Enforcement", „Cooperation" und „Future of Privacy" vertreten. Die Art. 29-Gruppe wird künftig als Europäischer Datenschutzausschuss eine wesentliche Rolle bei der Umsetzung der EU-Datenschutz-Grundverordnung spielen.

Auf Einladung der niederländischen Datenschutzbehörde fand die **37. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz**

321 Dokumentenband 2015, S. 9 ff.
322 Siehe 14.3 und Dokumentenband 2015, S. 38
323 Dokumentenband 2015, S. 51 ff.
324 Dokumentenband 2015, S..127 ff.

der Privatsphäre vom 26.-28. Oktober in Amsterdam statt. Sie befasste sich mit zentralen Fragen des Datenschutzes im weltweiten Zusammenhang und verabschiedete u. a. Entschließungen zu Transparenzberichten von Unternehmen, die sich Auskunftsersuchen staatlicher Stellen gegenübersehen, und zum Datenschutz bei humanitären Hilfsaktionen. Außerdem würdigte die Konferenz per Akklamation die Verdienste, die sich Dr. Alexander Dix in den zurückliegenden 25 Jahren insbesondere als Vorsitzender der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation (sog. Berlin Group) um den internationalen Datenschutz erworben hat. Diese Verdienste hatte bereits im April der Präsident der Ungarischen Nationalen Behörde für Datenschutz und Informationsfreiheit durch die Verleihung der Silbernen Medaille dieser Behörde an Dr. Dix gewürdigt.

Die **„Berlin Group"** tagte am 27./28. April in Seoul und beschloss dort ein Arbeitspapier zu Transparenzberichten, das später Grundlage des Beschlusses der Internationalen Konferenz in Amsterdam zum selben Thema wurde. Außerdem verabschiedete die Gruppe ein Arbeitspapier zum Datenschutz bei tragbaren Endgeräten („Wearables").[325] Bei ihrer Sitzung am 13./14. Oktober beschloss die Arbeitsgruppe außerdem Empfehlungen zur Verfolgung des Aufenthaltsorts auf der Basis von Meldungen von Mobilfunkgeräten und zu intelligenter Video-Analysetechnik.[326]

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist überdies Mitglied des Datenschutzbeirats des „Global Pulse"-Projekts der Vereinten Nationen, der am 23./24. Oktober eine Tagung zum Thema „Big Data für Zwecke der Entwicklung und humanitärer Maßnahmen" in Den Haag durchführte. Das „Global Pulse"-Projekt setzt sich für die datenschutzgerechte Nutzung von Big Data-Technologien im Rahmen von Entwicklungsprojekten und bei humanitären Hilfsmaßnahmen ein.

Erneut erhielten wir Besuch von mehreren ausländischen Delegationen, die sich in unserer Dienststelle über praktische Fragen der Datenschutzkontrolle und des Informationszugangs informierten. Dazu gehörten Vertreter der 2014

325 Siehe 15.2 und Dokumentenband 2015, S. 79 ff.
326 Siehe 15.6 und Dokumentenband 2015, S. 105 ff.

gegründeten Datenschutzkommission Japans, der marokkanischen Datenschutzbehörde und von Experten aus der Volksrepublik China.

18.4 Öffentlichkeitsarbeit

Am 28. Januar fand auf Einladung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine zentrale Veranstaltung im Abgeordnetenhaus von Berlin aus Anlass des 9. Europäischen Datenschutztages statt. Das Thema lautete „Europa: Sicherer Hafen des Datenschutzes? Zum künftigen Umgang mit dem unterschiedlichen Datenschutzniveau zwischen der EU und den USA".

Zweimal wurden dieses Jahr die berlinweiten Schülermedientage zur Förderung von Medienkompetenz unter dem Aspekt des digitalen Verbraucherschutzes durchgeführt (20.-22. Januar und 14.-16. Dezember). Im Rahmen der Projektwochen unter dem Titel „Check your Web" gestalteten wir an jeweils zwei Tagen im Januar und Dezember den Workshop „Datenschutz spielerisch erleben" und stellten zusätzlich einen Infostand zur Verfügung.

Am 5. September nahmen wir am gemeinsamen „Tag der offenen Tür" des Abgeordnetenhauses von Berlin und des Bundesrates teil und präsentierten dort einen Informationsstand.

In Kooperation mit der Verbraucherzentrale Berlin ist der Ratgeber „Schützen Sie Ihre Daten im Internet! Migranten in der digitalen Welt – Tipps zum Daten- und Verbraucherschutz" entwickelt worden. Der Ratgeber hat das Ziel, die Verbraucherinnen und Verbraucher insbesondere mit russischem und türkischem Migrationshintergrund über den Datenschutz aufzuklären und ein stärkeres Bewusstsein für den Umgang mit persönlichen Daten zu schaffen. Er gibt Hinweise u. a. zu Datenspuren im Internet, zum Umgang mit Passwörtern, zu Vertragsfallen beim Mobilfunk, zu Phishing Mails und Handlungsempfehlungen zum Selbstdatenschutz sowie zu Sicherheitseinstellungen der Mobilfunkgeräte. Den Ratgeber gibt es in deutscher, russischer und türkischer Sprache. Er ist in einem smartphone- und tabletgerechten EPUB-Format abrufbar und kann auch in Papierform als Broschüre bestellt werden.

Die Zentral- und Landesbibliothek Berlin ist mit dem besonderen Wunsch an uns herangetreten, im Zuge der Sensibilisierung der Beschäftigten für das Thema Datenschutz eine Schulung für ca. 350–400 Personen durchzuführen. Der einstündige Vortrag „Einführung in die Grundlagen des Datenschutzes" wurde im Rahmen einer Informationsveranstaltung am 2. und 10. Dezember in den Räumen der Berliner Stadtbibliothek gehalten. Insgesamt fünf Informationsveranstaltungen für jeweils 70-80 Beschäftigte fanden dort an beiden Tagen statt.

Außerdem bieten wir im Rahmen der KinderUni Lichtenberg (KUL) und der mobilen Vorlesungsreihe „KUL *unterwegs*" regelmäßige Veranstaltungen zum Thema „Soziale Netzwerke und Datenschutz – Facebook, Twitter, WhatsApp & Co." für Kinder ab acht Jahren an. Die Vorträge können jedoch auch für Jugendliche gebucht werden.[327]

Berlin, den 23. März 2016

Maja Smoltczyk
Berliner Beauftragte für Datenschutz und Informationsfreiheit

327 Nähere Informationen unter kul-unterwegs.de

Anhang

Rede des Berliner Beauftragten für Datenschutz und Informationsfreiheit am 24. September 2015 im Abgeordnetenhaus von Berlin zum Jahresbericht 2014

Sehr geehrte Frau Präsidentin,
sehr geehrte Damen und Herren,

Ihnen liegen heute der Jahresbericht 2014 zu Datenschutz und Informationsfreiheit sowie die Stellungnahme des Senats zur Beratung vor.

In den zehn Jahren, die seit meiner ersten Wahl durch dieses Hohe Haus vergangen sind, haben grundlegende Veränderungen in beiden Bereichen stattgefunden, die sich auch in dem aktuellen Bericht widerspiegeln. Ich habe immer betont, dass die Bedeutung des Datenschutzes wie auch der Informationsfreiheit zunehmen werden. Diese Erwartung sehe ich – so paradox es klingen mag – bestätigt, obwohl die Enthüllungen von **Edward Snowden** unsere schlimmsten Befürchtungen über außer Kontrolle geratene Geheimdienste nicht nur in den USA, sondern auch in Europa noch übertroffen haben. Zwar hat die Bundesregierung bisher nicht die notwendigen Konsequenzen für den Rechtsrahmen und die **Kontrolle der Geheimdienste** gezogen und hält offenbar auch keine nennenswerten Konsequenzen für nötig. Aber die Unternehmen, deren wirtschaftlicher Erfolg auf dem Vertrauen der Kunden in die Sicherheit der technisch vermittelten Kommunikation beruht, haben erste Konsequenzen gezogen. Telekommunikationsunternehmen und Anbieter von E-Mail-Diensten bieten verstärkt Verschlüsselungsmöglichkeiten an.

In Kürze wird eine Europäische Datenschutzgrundverordnung verabschiedet werden, die – so hoffe ich – den Datenschutz auf einem hohen Niveau

europaweit vereinheitlichen wird. Das ist überfällig, denn wir sind auf dem Weg in ein **„stählernes Gehäuse der Hörigkeit“**, wie Max Weber es mit Blick auf die deutsche Bürokratie bezeichnet hat. Dieses Gehäuse wird allerdings nicht – wie Weber meinte – von Bürokraten kontrolliert, sondern von großen außereuropäischen Unternehmen, die uns eine „schöne neue Welt“ versprechen, wie ein Google-Manager es formulierte, der offenbar Aldous Huxley nicht gelesen hat. Es geht auch nicht allein um marktbeherrschende US-Unternehmen wie Google, Facebook oder Apple, sondern es geht in naher Zukunft auch um chinesische Unternehmen, deren Namen noch nicht so bekannt sind, etwa AliBaba und Baidu.

Wenn wir nicht völlig in ein komfortabel wirkendes Gehäuse der Hörigkeit geraten wollen, dann müssen wir den Datenschutz und die Datenschutzaufsicht stärken. Ich teile nicht die Befürchtung der Bundeskanzlerin, dass Deutschland im weltweiten Wettbewerb ins Hintertreffen geraten könnte, wenn man die Datenschutzreform nur unter dem Blickwinkel des Datenschutzes betrachten würde. Datenschutz kann im Gegenteil zum Wettbewerbsvorteil werden. Kundenbindung und personalisierte Gesundheitsanwendungen sind wichtig und möglich, ohne die informationelle Selbstbestimmung und das Patientengeheimnis zur Disposition zu stellen. Auch die vom Senat angestrebte „Smart City“ darf nicht zu einem Gehäuse der Hörigkeit werden, sondern sie muss den Berlinerinnen und Berlinern stets auch im öffentlichen Raum die Möglichkeit bieten, sich unbeobachtet und damit frei zu bewegen. Nur in einer auf diese Weise wirklich „smarten“ Stadt wollen die Menschen leben.

Es gibt übrigens ermutigende Beispiele aus der Bundeshauptstadt dafür, dass Datenschutz auch in einer digitalisierten Umwelt ein Erfolgsfaktor ist. Berlin entwickelt sich zu einer **Metropole der Start-ups**, und immer mehr dieser Unternehmensgründer entdecken den **Datenschutz als Qualitätsmerkmal**, das ihnen **Vorteile im Wettbewerb** verschaffen kann. Ich nenne beispielhaft nur das Unternehmen Hoccer, das vor kurzem Testsieger beim Vergleichstest für Messenger-Dienste wurde, und den E-Mail-Anbieter Posteo. Beide in Berlin ansässige Unternehmen bieten sicher verschlüsselte Kommunikationsmöglichkeiten an. Es gibt also einen Markt für datenschutzfreundliche Produkte und solche Geschäftsideen sollte der Senat noch stärker als bisher fördern und selbst nutzen, um mit gutem Beispiel voranzugehen. „Datenschutz made in Berlin“ kann durchaus zum Treiber für Innovationen werden.

Meine Damen und Herren,

lassen Sie mich mit einer persönlichen Bemerkung schließen: Sie haben die Arbeit unserer Dienststelle in den zurückliegenden zehn Jahren immer wieder – auch durch Haushaltsentscheidungen - unterstützt, wofür ich Ihnen herzlich danke. Der Datenschutz und die Informationsfreiheit werden auch in Zukunft die Unterstützung des Abgeordnetenhauses brauchen, denn die Aufgaben wachsen sowohl aufgrund der technischen Entwicklung als auch durch die Europäische Datenschutzreform noch deutlich an.

Meine offizielle **Amtszeit** hat im Juni dieses Jahres geendet. Ich gehe davon aus, dass Sie in Kürze einen Nachfolger oder eine Nachfolgerin wählen werden. Eine weitere Verzögerung dieser Entscheidung würde der Bedeutung dieses Amtes nicht gerecht. Das Berliner Datenschutzgesetz sieht zwar vor, dass der Amtsinhaber auf Aufforderung des Parlamentspräsidiums bis zur Ernennung eines Nachfolgers im Amt bleibt. Ich schlage allerdings vor, dass diese gesetzliche Bestimmung bei nächster Gelegenheit in der Weise geändert wird, dass die Pflicht zur weiteren Amtsausübung auf längstens sechs Monate begrenzt wird. Das würde der Rechtslage im Land Brandenburg entsprechen.

Vielen Dank für Ihre Aufmerksamkeit.

Stichwortverzeichnis

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z

Veröffentlichungen der Berliner Beauftragten für Datenschutz und Informationsfreiheit

Tätigkeitsberichte:
Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat dem Abgeordnetenhaus und dem Senat von Berlin jährlich einen Bericht über ihre Tätigkeit vorzulegen. Neben aktuellen technischen und rechtlichen Entwicklungen wird darin über Schwerpunktthemen und Einzelfälle aus den jeweiligen Geschäftsbereichen berichtet. Der Tätigkeitsbericht wird von uns auch als Broschüre für die Bürgerinnen und Bürger veröffentlicht.

Dokumente zu Datenschutz und Informationsfreiheit:
Diese Schriftenreihe erscheint jährlich als Anlage zu unserem Tätigkeitsbericht. Sie enthält die bedeutsamen Dokumente der nationalen und internationalen Arbeitsgruppen und Konferenzen des genannten Jahres.

Berliner Informationsgesetzbuch (BlnInfGB):
In dieser Textsammlung werden von uns die wichtigsten Regelungen zum Datenschutz und zur Informationsfreiheit für das Land Berlin herausgegeben.

Ratgeber und Faltblätter zum Datenschutz:
In diesen Publikationen haben wir praktische Informationen zu einzelnen Fragen im Alltag zusammengestellt. Damit wollen wir die Menschen in die Lage versetzen, ihre Datenschutzrechte bzw. ihr Recht auf Informationszugang eigenständig wahrzunehmen.

Welche Broschüren wir im Einzelnen veröffentlicht haben, können Sie einer Übersicht auf unserer Website www.datenschutz-berlin.de entnehmen. Den überwiegenden Teil unserer Broschüren haben wir dort für Sie auch zum Download bereitgestellt. Eine Bestellung per Post ist gegen Einsendung eines an Sie selbst adressierten und mit 1,00 Euro frankierten DIN-A5-Umschlages möglich.

www.datenschutz-berlin.de

Das **Jobportal** der Berliner Verwaltung • **eVAK** – Begleitung eines neuen Verfahrens • Durchbruch zu einem neuen **Rechtsrahmen** für Europa • **Grundverordnung** • Richtlinie im Bereich von Justiz und Inneres • Große Liebe dank Big Data? • **Vernetzte Fahrzeuge** und moderne Verkehrstelematik • Risiken der Datenverarbeitung • Datenschutz made in Berlin • Risiken werden real: **Datenlecks** • Vorratsdatenspeicherung – eine unendliche Geschichte? • Projekt „Smarte Bürger“ • Parkausweise – schon auf der Gästeliste? • **Biografiefragebogen** • Videoaufnahmen in Kitas • Einführung des klinischen Krebsregisters • Reichweitenmessung im Internet • Falschparker auf dem Radar • **Videoidentifizierung** bei Banken • **Einsatz von Drohnen** • Datenschutz bei „Wearable Computing“ • Mehr **Transparenz** in den Parlamenten